МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

(РУТ (МИИТ)

ПРИКАЗ

31.05.2019 Москва № 398/а

О введении в действие образовательного стандарта высшего образования РУТ (МИИТ) по специальности 10.05.01 Компьютерная безопасность

В соответствии с п. 10 ст. 11 и п. 8 ст. 12 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Указом Президента Российской Федерации от 13.04.2018 № 156 «О внесении изменений в перечень федеральных государственных образовательных организаций высшего образования, которые вправе разрабатывать и утверждать самостоятельно образовательные стандарты по всем уровням высшего образования, утвержденный Указом Президента Российской Федерации от 09.09.2008 № 1332», поручением Министра транспорта Российской Федерации от 25.04.2018 № МС-17/68 и на основании решения ученого совета университета от 29.05.2019, протокол № 12, п р и к а з ы в а ю:

1. Ввести в действие с 31.05.2019 прилагаемый образовательный стандарт высшего образования федерального государственного автономного образовательного учреждения высшего образования «Российский университет транспорта» по специальности 10.05.01 Компьютерная безопасность.

2. Признать утратившим силу приказ от 26.02.2019 № 071/а «О введении в действие образовательного стандарта высшего образования РУТ (МИИТ) по специальности 10.05.01 Компьютерная безопасность».

3. Контроль за исполнением приказа возложить на первого проректора В.В. Виноградова.

Ректор  А.А. Климов

Андриянов Сергей Сергеевич
+7 (495) 681-19-35

Приложение
к приказу РУТ (МИИТ)
от 31.05.2019 № 398/а

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА» (РУТ (МИИТ)

УТВЕРЖДЕН
решением учёного совета
РУТ (МИИТ)
от 29.05.2019, протокол № 12

ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ОБРАЗОВАНИЯ

по специальности

10.05.01 Компьютерная безопасность

Квалификация:

Специалист по защите информации

Москва
2019

I. Общие положения

1. Образовательный стандарт высшего образования федерального государственного автономного образовательного учреждения высшего образования «Российский университет транспорта» (самостоятельно утверждаемый образовательный стандарт, далее – СУОС, СУОС ВО РУТ (МИИТ), Стандарт) по специальности 10.05.01 «Компьютерная безопасность» разработан в соответствии с Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и Указом Президента РФ от 13.04.2018 № 156, в соответствии с которым РУТ (МИИТ) предоставлено право разрабатывать и утверждать самостоятельно образовательные стандарты по всем уровням высшего образования.

2. Требования настоящего СУОС ВО РУТ (МИИТ) к условиям реализации и результатам освоения основных профессиональных образовательных программ высшего образования – программ специалитета, не ниже требований, установленных федеральным государственным образовательным стандартом высшего образования (далее ФГОС ВО) – специалитет по специальности 10.05.01 Компьютерная безопасность.

3. Настоящий СУОС ВО РУТ (МИИТ) разработан с учетом требований профессиональных стандартов, перечень которых приведен в Приложении 1.

4. Требования СУОС ВО РУТ (МИИТ) соответствуют программе развития и образовательной политике Университета и способствуют решению задач подготовки высококвалифицированных кадров, владеющих передовыми мировыми технологиями, способных решать новые комплексные профессиональные задачи и готовых вывести российскую экономику на новый уровень развития.

5. Порядок разработки, утверждения и изменения настоящего Стандарта определяется Положением о разработке и утверждении образовательных стандартов высшего образования РУТ (МИИТ) и внесении в них изменений, утвержденным Приказом РУТ (МИИТ).

6. Образовательный стандарт высшего образования, установленный РУТ (МИИТ) самостоятельно, представляет собой совокупность обязательных требований при реализации основных профессиональных образовательных программ высшего образования – программ специалитета по специальности 10.05.01 Компьютерная безопасность (далее – программа специалитета, специальность), реализуемых РУТ (МИИТ), в соответствии с лицензией на право ведения образовательной деятельности.

II. Характеристика специальности

7. Высшее образование по программе специалитета в соответствии с требованиями настоящего СУОС, может быть получено только в Университете. Получение высшего образования по программе специалитета в рамках данной специальности в форме самообразования не допускается.

8. Обучение по программе специалитета может осуществляться в очной форме обучения.

9. Содержание высшего образования по специальности определяется образовательной программой специалитета, разрабатываемой и утверждаемой Университетом в соответствии с требованиями настоящего Стандарта самостоятельно. При разработке программы специалитета Университет формирует требования к результатам ее освоения в виде универсальных, общепрофессиональных и профессиональных компетенций выпускников (далее вместе – компетенции).

10. При реализации программы специалитета Университет вправе применять электронное обучение, дистанционные образовательные технологии.

Электронное обучение, дистанционные образовательные технологии, применяемые при обучении инвалидов и лиц с ограниченными возможностями здоровья (далее – инвалиды и лица с ОВЗ), должны предусматривать возможность приема-передачи информации в доступных для них формах.

Реализация программы специалитета с применением исключительно электронного обучения, дистанционных образовательных технологий не допускается.

11. Реализация программы специалитета может осуществляется как самостоятельно, так и посредством сетевой формы обучения.

12. Программа специалитета реализуется на государственном языке Российской Федерации.

13. Срок получения образования по программе специалитета (вне зависимости от применяемых образовательных технологий):

- в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, (вне зависимости от применяемых образовательных технологий) составляет 5,5 лет;

- при обучении по индивидуальному учебному плану, вне зависимости от формы обучения, составляет не более срока получения образования, установленного для очной формы обучения, а при обучении по индивидуальному плану инвалидов и лиц с ОВЗ может быть увеличен по их

заявлению не более, чем на 1 год по сравнению со сроком получения образования для очной формы обучения.

14. 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 ускоренного обучения.

Объем программы специалитета в очной форме обучения, реализуемый за один учебный год, составляет 60 з.е.

Объем программы специалитета, реализуемый за один учебный год, составляет не более 70 з.е. при реализации программы специалитета по индивидуальному учебному плану (за исключением ускоренного обучения), а при ускоренном обучении – не более 80 з.е.

14.1. Разработчик образовательной программы самостоятельно определяет в пределах сроков и объемов, установленных пунктами 13 и 14 стандарта:

- срок получения образования по программам специалитета в очно-заочной или заочной формах обучения, а также по индивидуальному учебному плану, в том числе при ускоренном обучении;

- объем программы специалитета, реализуемый за один учебный год.

15. Программы специалитета, содержащие сведения, составляющие государственную тайну, разрабатываются и реализуются при создании условий и с соблюдением требований, предусмотренных законодательством Российской Федерации о государственной тайне, и нормативных правовых актов федеральных государственных органов, в ведении которых находятся организации, реализующие соответствующие образовательные программы.

16. Программы специалитета, содержащие научно-техническую информацию, подлежащую экспортному контролю, и в рамках которой (которых) до обучающихся доводятся сведения ограниченного доступа, и (или) в учебных целях используются секретные образцы вооружения, военной техники, их комплектующие изделия, разрабатываются и реализуются с соблюдением требований, предусмотренных законодательством Российской Федерации и нормативными правовыми актами в области экспортного контроля

III. Характеристика профессиональной деятельности выпускников, освоивших программу специалитета

17. Области профессиональной деятельности и сферы профессиональной деятельности, в которых выпускники, освоившие

программу специалитета, могут осуществлять профессиональную деятельность:

01 Образование и наука (в сфере научных исследований по вопросам защиты информации в компьютерных системах и сетях);

06 Связь, информационные и коммуникационные технологии (в сфере защиты информации, разработки, внедрения, эксплуатации, экспертизы и менеджмента средств и систем обеспечения информационной безопасности компьютерных систем и сетей);

12 Обеспечение безопасности (в сфере компьютерных систем и сетей в условиях существования угроз их информационной безопасности);

сфера обороны и безопасности;

сфера правоохранительной деятельности.

Выпускники могут осуществлять профессиональную деятельность и в других областях и (или) сферах профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

18. В рамках освоения программы специалитета выпускники могут готовиться к решению задач профессиональной деятельности следующих типов:

научно-исследовательский;

проектный;

контрольно-аналитический;

организационно-управленческий;

эксплуатационный.

При разработке и реализации программ специалитета Университет ориентируется на все типы задач профессиональной деятельности, к которым готовится специалист.

19. При разработке программы специалитета Университет устанавливает специализацию программы специалитета, которая конкретизирует содержание программы специалитета в рамках специальности путем выбора ее из следующего перечня:

Специализация № 1 «Анализ безопасности компьютерных систем».

Специализация № 2 «Математические методы защиты информации».

Специализация № 3 «Безопасность распределенных компьютерных систем».

Специализация № 4 «Разработка защищенного программного обеспечения».

Специализация № 5 «Безопасность высокопроизводительных вычислительных систем».

Специализация № 6 «Безопасность программного обеспечения мобильных систем».

Специализация № 7 «Информационно-аналитическая и техническая экспертиза компьютерных систем».

Специализация № 8 «Информационная безопасность объектов информатизации на базе компьютерных систем».

Специализация № 9 «Специальные технологии противодействия компьютерным атакам».

20. Перечень основных объектов (или областей знания) профессиональной деятельности выпускников:

защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации;

системы управления информационной безопасностью компьютерных систем;

методы и реализующие их средства защиты информации в компьютерных системах;

математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах;

методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах;

процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах.

21. Основные задачи профессиональной деятельности, которые могут решать выпускники, в зависимости от выбранных областей профессиональной деятельности и сфер профессиональной деятельности, и типов задач профессиональной деятельности, представлены в Приложении 2.

22. Перечень обобщённых трудовых функций и трудовых функций (при наличии ПС), имеющих отношение к профессиональной деятельности (далее - ПД) выпускника программ специалитета представлен в Приложении 3.

23. При разработке программы специалитета задачи профессиональной деятельности, обобщенные трудовые функции и трудовые функции (при наличии ПС), к выполнению которых должен быть готов выпускник, из числа установленных в настоящем Стандарте, разработчик выбирает самостоятельно.

IV. Требования к структуре программы специалитета

24. Структура программы специалитета включает следующие блоки:

Блок 1 «Дисциплины (модули)»;

Блок 2 «Практики, в том числе научно-исследовательская работа (НИР)»;

Блок 3 «Государственная итоговая аттестация».

Таблица 1

Структура и объем программы специалитета

Структура программы специалитета		Объем программы специалитета и ее блоков в з.е.
Блок 1	Дисциплины (модули)	не менее 285
Блок 2	Практики, в том числе научно-исследовательская работа (НИР)	не менее 33
Блок 3	Государственная итоговая аттестация	не менее 9
Объем программы специалитета		330

25. В рамках Блока 1 «Дисциплины (модули)» реализуются обязательные дисциплины (модули) по философии, истории (истории России, всеобщей истории), иностранному языку, безопасности жизнедеятельности, основам информационной безопасности, организационному и правовому обеспечению информационной безопасности, языкам программирования, операционным системам, системам управления базами данных, защите в операционных системах, технической защите информации, основам построения защищенных компьютерных сетей, основам построения защищенных баз данных, моделям безопасности компьютерных систем, криптографическим методам защиты информации, криптографическим протоколам.

Для формирования коммуникативных навыков общения в профессиональной среде и для международной академической мобильности обучающихся, изучение иностранного языка осуществляется в объеме не менее 13 з.е.

26. Дисциплины (модули) по физической культуре и спорту реализуются:

- в объеме не менее 2 з.е. в рамках Блока 1 «Дисциплины (модули)»;

- в объеме не менее 328 академических часов, которые являются обязательными для освоения, не переводятся в з.е. и не включаются в объем программы специалитета, в рамках элективных дисциплин (модулей) в очной форме обучения.

Дисциплины (модули) по физической культуре и спорту реализуются в порядке, установленном Университетом. Для инвалидов и лиц с ОВЗ устанавливается особый порядок освоения дисциплин (модулей) по физической культуре и спорту с учетом состояния их здоровья.

27. В Блок 2 «Практика» входят учебная и производственная практики (далее вместе – практики):

Типы учебной практики:

- учебно-лабораторный практикум;
- ознакомительная практика;
- экспериментально-исследовательская практика;
- научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);

Типы производственной практики:

- эксплуатационная практика;
- конструкторская практика;
- эксплуатационно-технологическая практика;
- проектно-технологическая практика;
- технологическая практика;
- научно-исследовательская работа;
- преддипломная практика.

28. При проектировании программы специалитета разработчик:

- выбирает один или несколько типов учебной практики и один или несколько типов производственной практики из перечня, указанного в пункте 27 настоящего Стандарта;
- вправе установить дополнительный тип (типы) учебной и (или) производственной практик;
- устанавливает объемы учебной и производственной практики каждого типа.

29. В Блок 3 «Государственная итоговая аттестация» входят:

- подготовка к сдаче и сдача государственного экзамена (если Организация включила государственный экзамен в состав государственной итоговой аттестации);
- выполнение и защита выпускной квалификационной работы

30. При разработке программы специалитета обучающимся обеспечивается возможность освоения элективных дисциплин (модулей) и факультативных дисциплин (модулей).

Факультативные дисциплины (модули) не включаются в объем программы специалитета. Объем и состав факультативных дисциплин (модулей) устанавливаются образовательной программой.

31. В рамках программы специалитета выделяются обязательная часть и часть, формируемая участниками образовательных отношений.

К обязательной части программы специалитета относятся дисциплины (модули) и практики, обеспечивающие формирование исключительно универсальных, общепрофессиональных компетенций, а также профессиональных компетенций, соответствующих специализации выбранной разработчиками образовательной программы, и установленных настоящим Стандартом в качестве обязательных.

В обязательную часть программы специалитета включаются, в том числе:

- дисциплины (модули), указанные в п. 25 настоящего Стандарта;
- дисциплины (модули) по физической культуре и спорту, реализуемые в рамках Блока 1 «Дисциплины (модули)».

Дисциплины (модули) и практики, обеспечивающие формирование универсальных компетенций, могут включаться в обязательную часть программы специалитета и в часть, формируемую участниками образовательных отношений.

Объем обязательной части, без учета объема государственной итоговой аттестации, должен составлять не менее 75 процентов общего объема программы специалитета.

32. Университет должен предоставлять инвалидам и лицам с ОВЗ (по их заявлению) возможность обучения по программе специалитета, учитывающей особенности их психофизического развития, индивидуальных возможностей и при необходимости, обеспечивающей коррекцию нарушений развития и социальную адаптацию указанных лиц.

V. Требования к результатам освоения программы специалитета

34. В результате освоения программы специалитета у выпускника должны быть сформированы универсальные, общепрофессиональные и профессиональные компетенции, установленные программой специалитета.

35. Программа специалитета должна устанавливать следующие универсальные компетенции (далее – УК):

Таблица 2

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника программы специалитета
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
Разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла
Командная работа и лидерство	УК-3. Способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном (ых) языке (ах), для академического и профессионального взаимодействия
Межкультурное взаимодействие	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
Самоорганизация и саморазвитие (в том числе здоровье-сбережение)	УК-6. Способен определить и реализовать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни
	УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности
Безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций
Основы правовых знаний	УК-9. Способен осуществлять социальное взаимодействие в обществе и служебном (трудовом) коллективе, профессиональную деятельность на основе требований правовых (в том числе антикоррупционных) норм, содействовать противодействию коррупции

36. Программа специалитета должна устанавливать следующие общепрофессиональные компетенции (далее - ОПК):

Таблица 3

Код и наименование общепрофессиональной компетенции выпускника

программы специалитета
ОПК-1. Способен представлять роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-2. Способен применять программные средства системного и прикладного назначения для решения профессиональных задач
ОПК-3. Способен на основании совокупности существующих математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач защиты информации
ОПК-4. Способен представлять основные черты современной естественнонаучной картины мира и физические основы функционирования электронной компонентной базы
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации (учреждения, предприятия)
ОПК-6. Способен анализировать и учитывать текущее состояние и тенденции развития методов криптографической защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, средств технической защиты информации, сетей и систем передачи информации при решении профессиональных задач
ОПК-7. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей
ОПК-8. Способен проводить анализ корректности реализации эффективных комбинаторных, теоретико-числовых и криптографических алгоритмов и протоколов применительно к конкретным условиям
ОПК-9. Способен разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации
ОПК-10. Способен администрировать подсистемы и средства защиты информации в компьютерных системах и сетях
ОПК-11. Способен проводить оценку уровня безопасности компьютерных систем и сетей
ОПК-12. Способен участвовать в разработке программно-аппаратных средств защиты информации компьютерных систем и сетей
ОПК-13. Способен производить проверки технического состояния и профилактические осмотры технических средств защиты информации
ОПК-14. Способен выполнять работы по восстановлению работоспособности подсистем защиты информации в операционных системах, программно-аппаратных средствах защиты информации, в прикладном и системном программном обеспечении
ОПК-15. Способен проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах, системах управления базами данных, компьютерных сетях
ОПК-16. Способен оценивать эффективность реализации действующих политик безопасности операционных систем и систем управления базами данных
ОПК-17. Способен контролировать корректность функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях

ОПК-18. Способен выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота с целью обеспечения защиты обрабатываемой информации
ОПК-19. Способен в процессе функционирования компьютерных систем и сетей и организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК-20. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире, в том числе для формирования гражданской позиции и развития патриотизма

37. Профессиональные компетенции, устанавливаемые программой специалитета, формируются на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников (при наличии), а также при необходимости на основе анализа требований к профессиональным компетенциям, предъявляемых к выпускникам специальности на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники в рамках специальности, иных источников (далее – иные требования, предъявляемые к выпускникам).

Профессиональные компетенции устанавливаются настоящим Стандартом в качестве обязательных и (или) рекомендуемых (далее соответственно – обязательные профессиональные компетенции (далее – ПКО), рекомендуемые профессиональные компетенции (далее – ПКР).

38. Программа специалитета должна устанавливать обязательные профессиональные компетенции, указанные в приложении 6, в зависимости от выбранных типов задач профессиональной деятельности.

39. В программе специалитета могут устанавливаться профессиональные компетенции в соответствии со специализацией программы, структурированные по типам задач профессиональной деятельности программы специалитета, указанные в приложении 7.

40. При определении профессиональных компетенций, устанавливаемых программой специалитета, разработчики:

- включают в программу специалитета все обязательные профессиональные компетенции (при наличии), в зависимости от выбранных областей профессиональной деятельности и сфер профессиональной деятельности, и типов задач профессиональной деятельности;

- вправе включить в программу специалитета одну или несколько рекомендуемых профессиональных компетенций (при наличии);

- включает определяемые самостоятельно одну или несколько профессиональных компетенций, исходя из специализации программы специалитета, на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников (при наличии), а также при необходимости на основе анализа иных требований, предъявляемых к выпускникам (Разработчик программы специалитета вправе не включать профессиональные компетенции, определяемые самостоятельно, при наличии обязательных профессиональных компетенций, а также в случае включения в программу специалитета рекомендуемых профессиональных компетенций).

При определении профессиональных компетенций на основе профессиональных стандартов осуществляется выбор профессиональных стандартов, соответствующих профессиональной деятельности выпускников из числа указанных в Приложении 1 к настоящему Стандарту и (или) иных профессиональных стандартов, соответствующих профессиональной деятельности выпускников, из реестра профессиональных стандартов, размещённого на специализированном сайте Министерства труда и социальной защиты Российской Федерации «Профессиональные стандарты» (profstandart.rosmintrud.ru) (при наличии соответствующих профессиональных стандартов).

Из каждого выбранного профессионального стандарта выделяется одна или несколько обобщённых трудовых функций (далее – ОТФ), соответствующих профессиональной деятельности выпускников, на основе установленных профессиональным стандартом для ОТФ уровня квалификации и требований раздела «Требования к образованию и обучению». ОТФ может быть выделена полностью или частично.

41. Общее число осваиваемых компетенций, включая установленные дополнительно, не может превышать 40.

42. Совокупность компетенций, установленных программой специалитета, должна обеспечивать выпускнику способность осуществлять профессиональную деятельность не менее, чем в одной области профессиональной деятельности и (или) сфере профессиональной деятельности, установленных в соответствии с пунктом 17 настоящего Стандарта, и решать задачи профессиональной деятельности не менее чем одного типа, установленных в соответствии с пунктом 18 настоящего Стандарта.

43. Индикаторы достижения универсальных, общепрофессиональных и обязательных профессиональных компетенций (при наличии) устанавливаются в Приложениях 4, 5, 6.

44. Индикаторы достижения рекомендуемых профессиональных компетенций и самостоятельно установленных профессиональных компетенций (при наличии) устанавливаются самостоятельно разработчиками образовательной программы высшего образования.

45. При проектировании программы специалитета результаты обучения по дисциплинам (модулям) и практикам должны быть соотнесены с установленными в программе специалитета индикаторами достижения компетенций.

Совокупность запланированных результатов обучения по дисциплинам (модулям) и практикам должна обеспечивать формирование у выпускника всех компетенций, установленных программой специалитета.

VI. Требования к условиям реализации программы специалитета

46. Требования к условиям реализации программы специалитета включают в себя общесистемные требования, требования к материально-техническому и учебно-методическому обеспечению, требования к кадровым и финансовым условиям реализации программы специалитета, а также требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по программе специалитета.

47. Общесистемные требования к реализации программы специалитета.

1) Университет должен располагать на праве собственности или ином законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием), обеспечивающими реализацию программы специалитета по Блоку 1 «Дисциплины (модули)» и Блоку 3 «Государственная итоговая аттестация» в соответствии с учебным планом.

2) Реализация основной образовательной программы специалитета требует формирования электронно-информационной образовательной среды (далее – ЭИОС) РУТ (МИИТ).

3) Каждый обучающийся в течение всего периода обучения должен быть обеспечен индивидуальным неограниченным доступом к ЭИОС Университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») как на территории Университета, так и вне ее.

4) ЭИОС РУТ (МИИТ) должна обеспечивать:

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

- формирование электронного портфолио обучающегося, в том числе сохранение работ и оценок на эти работы.

В случае реализации программы специалитета с применением электронного обучения, дистанционных образовательных технологий ЭИОС Университета должна дополнительно обеспечивать:

- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы специалитета;

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

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

5) Функционирование ЭИОС РУТ (МИИТ) обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование ЭИОС Университета должно соответствовать законодательству Российской Федерации.

6) При реализации программы специалитета в сетевой форме требования к реализации программы специалитета должны обеспечиваться совокупностью ресурсов материально-технического и учебно-методического обеспечения, предоставляемого организациями, участвующими в реализации программы специалитета в сетевой форме.

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

1) Помещения должны представлять собой учебные аудитории для проведения учебных занятий всех видов, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей).

Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС РУТ (МИИТ).

Допускается замена оборудования его виртуальными аналогами, позволяющими обучающимся получать запланированные результаты

обучения по модулям (дисциплинам), предусмотренным программой специалитета.

2) Университет должен быть обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства (состав определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости).

3) При использовании в образовательном процессе печатных изданий библиотечный фонд должен быть укомплектован печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочих программах дисциплин (модулей), практик, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику.

4) 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 (при необходимости).

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

6) Перечень материально-технического обеспечения, минимально необходимый для реализации программ специалитета, включает в себя:

лаборатории в области:

- физики, оснащенную учебно-лабораторными стендами по механике, электричеству и магнетизму, электродинамике, оптике;

- электроники и схемотехники, оснащенную учебно-лабораторными стендами, средствами для измерения и визуализации частотных и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов;

- сетей и систем передачи информации, оснащенную рабочими местами на базе вычислительной техники, стендами сетей передачи информации с коммутацией пакетов и коммутацией каналов;

- безопасности компьютерных сетей, оснащенную стендами для изучения проводных и беспроводных компьютерных сетей, включающих абонентские устройства, коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, системы обнаружения атак;

- технической защиты информации, оснащенную специализированным оборудованием по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам, аппаратно-программными комплексами радиомониторинга;

- программно-аппаратных средств обеспечения информационной безопасности, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, средствами анализа программных реализаций, программно-аппаратными комплексами защиты информации, включая криптографические средства защиты информации, программно-аппаратными комплексами поиска и уничтожения остаточной информации, программно-аппаратными модулями доверенной загрузки;

специально оборудованные кабинеты (классы, аудитории):

- информатики, оснащенный рабочими местами на базе вычислительной техники;

- информационных технологий, оснащенный рабочими местами на базе вычислительной техники и абонентскими устройствами, подключенными к сети«Интернет» с использованием проводных и (или) беспроводных технологий;

- научно-исследовательской работы обучающихся, курсового и дипломного проектирования, оснащенный рабочими местами на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и (или) программных средств, а также комплектом оборудования для печати;

аудиторию (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну;

специальную библиотеку (библиотеку литературы ограниченного доступа), предназначенную для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа.

Университет имеет лаборатории и (или) специально оборудованные кабинеты (классы, аудитории), обеспечивающие практическую подготовку в соответствии с теми специализациями программы специалитета, которые реализуются.

Кабинеты (классы, аудитории) для Организаций, реализующих специализации №9:

выделенное помещение (аудиторию) для проведения учебных занятий, в ходе которых до обучающихся доводятся сведения, составляющие государственную тайну;

огневой подготовки;

тактико-специальной (военно-профессиональной, специальной профессиональной) подготовки;

тиры (для стрельбы из табельного оружия).

Компьютерные (специализированные) классы и лаборатории, если в них предусмотрены рабочие места на базе вычислительной техники, должны быть оборудованы современной вычислительной техникой из расчета одно рабочее место на каждого обучаемого при проведении занятий в данных классах (лабораториях).

Допускается замена оборудования его виртуальными аналогами.

7) Лабораторные занятия/работы должны проводиться в специально оборудованных учебных и/или научно-исследовательских лабораториях Университета, а при необходимости – в производственных и/или исследовательских лабораториях организаций, участвующих в образовательном процессе РУТ (МИИТ).

8) Помещения, предназначенные для проведения лабораторных занятий/работ, а также расположенные в них лабораторные установки (стенды, лабораторное оборудование) должны соответствовать действующим санитарно-гигиеническим нормам и требованиям техники безопасности.

9) Количество лабораторных установок (стендов, лабораторное оборудование) должно быть достаточным для обеспечения эффективной самостоятельной работы обучающихся одной учебной группы (подгруппы) и для достижения целей, определяемых содержанием лабораторных работ. Исключение могут составить научные и производственные установки, системы, стенды и устройства, уникальные в техническом или в каком-либо ином отношении.

49. Требования к кадровым условиям реализации программы специалитета.

1) Реализация программы специалитета обеспечивается педагогическими работниками РУТ (МИИТ), а также лицами, привлекаемыми к реализации программы специалитета на иных условиях.

2) Квалификация педагогических работников Университета должна отвечать квалификационным требованиям, указанным в квалификационных справочниках и (или) профессиональных стандартах (при наличии).

Уровень квалификации педагогических работников определяется установленным в Университете порядком, в том числе в форме критериев и

требований, предъявляемым к кандидатам при организации конкурсного отбора на замещения должностей педагогических работников. Уровень квалификации педагогических работников и представителей работодателей, привлекаемых к реализации конкретных дисциплин и междисциплинарных модулей, устанавливается в образовательной программе с учетом содержания дисциплины (модуля) и языка, на котором реализуется данная дисциплина (модуль).

3) Не менее 80 процентов численности педагогических работников Университета, участвующих в реализации программы специалитета, и лиц, привлекаемых к реализации программы специалитета на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), должны вести научную, учебно-методическую и (или) практическую деятельность, соответствующую профилю преподаваемой дисциплины (модуля).

4) Не менее 7 процентов численности педагогических работников Организации, участвующих в реализации программы специалитета, и лиц, привлекаемых к реализации программы специалитета на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), должны являться руководителями и (или) работниками иных организаций, осуществляющими трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники программы специалитета (иметь стаж работы в данной профессиональной сфере не менее 3 лет).

5) Не менее 70 процентов численности педагогических работников Организации и лиц, привлекаемых к образовательной деятельности Организации на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), должны иметь ученую степень (в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации) и (или) ученое звание (в том числе ученое звание, полученное в иностранном государстве и признаваемое в Российской Федерации).

В реализации программы специалитета должен принимать участие минимум один педагогический работник РУТ (МИИТ), имеющий ученую степень доктора или кандидата наук по научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность», соответствующей направлениям подготовки кадров высшей квалификации по программам подготовки научно-педагогических кадров в аспирантуре (адъюнктуре), входящим в укрупненную группу специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

К педагогическим работникам и лицам, привлекаемым к образовательной деятельности Университета на иных условиях, с учеными степенями и/или учеными званиями приравниваются лица без ученых степеней и званий, имеющие государственные почетные звания, лауреаты государственных премий в сфере информационных технологий.

50. Требование к финансовым условиям реализации программы специалитета – финансовое обеспечение реализации программы специалитета должно осуществляться в объеме не ниже значений базовых нормативов затрат на оказание государственных услуг по реализации образовательных программ высшего образования – программ специалитета и значений корректирующих коэффициентов к базовым нормативам затрат, определяемых Министерством науки и высшего образования Российской Федерации.

VII. Оценка качества освоения программы специалитета

51. Ответственность за обеспечение качества подготовки обучающихся при реализации программ специалитета и получение обучающимися требуемых настоящим СУОС результатов обучения несет Университет.

52. Качество образовательной деятельности и подготовки обучающихся по программе специалитета определяется в рамках системы внутренней оценки, а также системы внешней оценки на добровольной основе.

53. В целях совершенствования программы специалитета Университета при проведении регулярной внутренней оценки качества образовательной деятельности и подготовки обучающихся по программе специалитета привлекает работодателей и (или) их объединения, иных юридических и (или) физических лиц, включая педагогических работников Университета.

54. Внешняя оценка качества образовательной деятельности по программе специалитета в рамках процедуры государственной аккредитации осуществляется с целью подтверждения соответствия образовательной деятельности по программе специалитета требованиям настоящего Стандарта.

55. Внешняя оценка качества образовательной деятельности и подготовки обучающихся по программе специалитета может осуществляться в рамках профессионально-общественной аккредитации, проводимой работодателями, их объединениями, а также уполномоченными ими организациями, в том числе иностранными организациями, либо авторизованными национальными профессионально-общественными организациями, входящими в международные структуры, с целью признания

качества и уровня подготовки выпускников, отвечающими требованиям профессиональных стандартов (при наличии), требованиям рынка труда к специалистам соответствующего профиля.

56. Обучающимся должна быть предоставлена возможность оценивания условий, содержания, организации и качества образовательного процесса в целом и отдельных дисциплин (модулей) и практик, а также работы отдельных преподавателей путем анонимного заполнения обучающимися опросных листов.

57. Оценка качества освоения программы специалитета обучающимися включает текущий контроль успеваемости, промежуточную аттестацию и государственную итоговую аттестацию.

Для осуществления процедур промежуточной аттестации и государственной итоговой аттестации обучающихся должны быть созданы соответствующие фонды оценочных средств, содержащие компетенции и индикаторы достижения компетенций, заявленные в программе специалитета, позволяющие оценить результаты обучения по отдельным дисциплинам (модулям) и практикам.

Разработчик образовательной программы самостоятельно формирует фонды оценочных средств по дисциплине (модулю) и практике, включающие требования по текущему контролю, промежуточной аттестации, государственной итоговой аттестации, используемых в программе специалитета.

Конкретные формы и процедуры текущего контроля успеваемости и промежуточной аттестации, обучающихся по каждой дисциплине (модулю) и практике устанавливаются образовательной программой (в том числе особенности процедур текущего контроля успеваемости и промежуточной аттестации при обучении инвалидов и лиц с ограниченными возможностями здоровья) и доводятся до сведения обучающихся в сроки, определяемые локальными нормативными актами РУТ (МИИТ).

58. Государственная итоговая аттестация выпускника является обязательной и осуществляется после освоения образовательной программы в полном объеме. Государственная итоговая аттестация, включает защиту выпускной квалификационной работы.

VIII. Контроль за соблюдением стандарта

59. Контроль за соблюдением обязательных требований настоящего образовательного стандарта РУТ (МИИТ) организует и осуществляет Учебно-методическое управление университета.

60 Контроль предусматривает следующие мероприятия:

- проверка соблюдения обязательных требований образовательного стандарта при утверждении образовательных программ по специальности10.05.01 «Компьютерная безопасность», разработанной по данному СУОС ВО РУТ (МИИТ);

- проверка соблюдения обязательных требований образовательного стандарта при внесении изменений в образовательную программу по данной специальности, разработанной по данному СУОС ВО РУТ (МИИТ);

- проверка соблюдения обязательных требований образовательного стандарта при реализации образовательной программы по специальности, разработанной по данному СУОС ВО РУТ (МИИТ).

IX. Список разработчиков и экспертов, принимавших участие в разработке образовательного стандарта высшего образования РУТ (МИИТ)

Разработчики:		
Российский университет транспорта (МИИТ)	Директор Института транспортной техники и систем управления(ИТТСУ)	П.Ф. Бестемьянов
Российский университет транспорта (МИИТ)	Заведующий кафедрой «Управление и защита информации» ИТТСУ	Л.А. Баранов
Российский университет транспорта (МИИТ)	Профессор кафедры «Управление и защита информации» ИТТСУ	В.М. Алексеев
Российский университет транспорта (МИИТ)	Профессор кафедры «Управление и защита информации» ИТТСУ	В.Г. Сидоренко
ОАО «Научно-исследовательский и проектно-конструкторский институт информатизации автоматизации и связи на железнодорожном транспорте» (НИИАС) – дочернее общество ОАО «РЖД»	Заместитель руководителя научно-технического комплекса	И.Б. Шубинский
Федеральное государственное унитарное предприятие «ЗащитаИнфоТранс»	Директор Центра по сертификации	А.А. Привалов

Министерства транспорта Российской Федерации		
Российский университет транспорта (МИИТ)	Инженер I категории кафедры «Управление и защита информации» ИТТСУ	А.А. Кречетова
Эксперты:		
ОАО «Научно-исследовательский и проектно-конструкторский институт информатизации автоматизации и связи на железнодорожном транспорте» (НИИАС) – дочернее общество ОАО «РЖД»	Первый заместитель Генерального директора	Е.Н. Розенберг
Федеральное государственное унитарное предприятие «ЗащитаИнфоТранс» Министерства транспорта Российской Федерации	Заместитель Генерального директора	И.А. Сидоров

Приложение 1
к образовательному стандарту высшего образования
по специальности 10.05.01 Компьютерная безопасность

ПЕРЕЧЕНЬ
профессиональных стандартов, соответствующих профессиональной деятельности выпускников, освоивших программу специалитета

№ п/п	Код профессионального стандарта	Наименование области профессиональной деятельности. Наименование профессионального стандарта
06 Связь, информационные и коммуникационные технологии		
1	**06.001**	Профессиональный стандарт «Программист», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2013 г. № 679н (зарегистрирован Министерством юстиции Российской Федерации 18 декабря 2013 г., регистрационный № 30635)
2	**06.004**	Профессиональный стандарт «Специалист по тестированию в области информационных технологий», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 11 апреля 2014 г. № 225н (зарегистрирован Министерством юстиции Российской Федерации 09 июня 2014 г., регистрационный № 32623)
3	**06.022**	Профессиональный стандарт «Системный аналитик», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от28 октября 2014 г. № 809н (зарегистрирован в Минюсте России 24 ноября 2014 г. № 34882).
4	**06.024**	Профессиональный стандарт «Специалист по технической поддержке информационно-коммуникационных систем», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от5 октября 2015 г. № 688н(зарегистрирован в Минюсте России 22 октября 2015 г. № 39412).
5	**06.027**	Профессиональный стандарт «Специалист по администрированию сетевых устройств информационно-коммуникационных систем», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от5 октября 2015 г. № 686н (зарегистрирован в Минюсте России 30 октября 2015 г. № 39568).
6	**06.028**	Профессиональный стандарт «Системный программист», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 5 октября 2015 г. № 685н (зарегистрирован Министерством юстиции Российской Федерации 20 ноября 2015г., регистрационный № 39374)
7	**06.030**	Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Министерства труда и

		социальной защиты Российской Федерации от3 ноября 2016 г. № 608н (зарегистрирован в Минюсте России 25 ноября 2016 г. № 44449).
8	**06.031**	Профессиональный стандарт «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от9 ноября 2016 г. № 611н(зарегистрировано в Минюсте России 22 ноября 2016 г. № 44398).
9	**06.032**	Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» утверждённый приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 года № 598н (зарегистрирован в Министерстве юстиции Российской Федерации 28 ноября 2016 года. № 44464).
10	**06.033**	Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от15 сентября 2016 г. № 522н (зарегистрировано в Минюсте России 28 сентября 2016 г. № 43857).
11	**06.034**	Профессиональный стандарт «Специалист по технической защите информации», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н(зарегистрирован в Минюсте России 25 ноября 2016 г. № 44443).
12	**06.037**	Профессиональный стандарт «Специалист по поддержке программно-конфигурируемых информационно-коммуникационных сетей», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от26 июня 2017 г. № 514н (зарегистрирован в Минюсте России 18 июля 2017 г. № 47441).
12 Обеспечение безопасности		
13	**12.004**	Профессиональный стандарт «Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 29 декабря 2015 г. № 1179н (зарегистрирован Министерством юстиции Российской Федерации 28 января 2016 г., регистрационный № 40858)
14	**12.005**	Профессиональный стандарт «Специалист по противодействию иностранным техническим разведкам», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 25 декабря 2015 г. № 15с (зарегистрирован Министерством юстиции Российской Федерации 22 января 2016 г., регистрационный № 40706)

Приложение 2
к образовательному стандарту высшего образования
по специальности10.05.01 Компьютерная безопасность

ПЕРЕЧЕНЬ
основных задач профессиональной деятельности выпускников

Область профессиональной деятельности	Типы задач профессиональной деятельности	Задачи профессиональной деятельности	Объекты профессиональной деятельности (или области знания)
06 Связь, информационные и коммуникационные технологии (в сфере науки, техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)	Научно-исследовательский (вид ПД)	- сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности -участие в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах - изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте - разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов	- защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; - системы управления информационной безопасностью компьютерных систем; - методы и реализующие их средства защиты информации в компьютерных системах; -математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; -методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; -процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах; -математические модели процессов, возникающих при защите информации в системах управления высокоскоростными и беспилотными транспортными средствами; -процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в системах управления высокоскоростными и беспилотными транспортными средствами.
	Проектный (вид ПД)	- разработка и конфигурирование программно-аппаратных средств защиты информации - разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов - разработка проектов систем и подсистем управления	- защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; - системы управления информационной безопасностью компьютерных систем; - методы и реализующие их средства защиты информации в компьютерных системах; - математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах;

		информационной безопасностью объекта в соответствии с техническим заданием - проектирование программных и аппаратных средств защиты информации в соответствии с техническим заданием с использованием средств автоматизации проектирования	- методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах; - математические модели процессов, возникающих при защите информации в системах управления высокоскоростными и беспилотными транспортными средствами; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в системах управления высокоскоростными и беспилотными транспортными средствами.
	Организационно-управленческий (вид ПД)	- организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ - поиск рациональных решений при разработке средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения - осуществление правового, организационного и технического обеспечения защиты информации - организация работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа (сведений, составляющих государственную тайну и конфиденциальной информации)	- защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; - системы управления информационной безопасностью компьютерных систем; - методы и реализующие их средства защиты информации в компьютерных системах; - математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; - методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах; - математические модели процессов, возникающих при защите информации в системах управления высокоскоростными и беспилотными транспортными средствами; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в системах управления высокоскоростными и беспилотными транспортными средствами.
	Контрольно-аналитический (вид ПД)	- оценивание эффективности реализации систем защиты информации и действующей политики безопасности в компьютерных системах - предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей - применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты	- защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; - системы управления информационной безопасностью компьютерных систем; - методы и реализующие их средства защиты информации в компьютерных системах; - математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах;

		- выполнение экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты и анализ результатов - проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности компьютерной системы - проведение инструментального мониторинга защищенности компьютерных систем - подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей	- методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах; - математические модели процессов, возникающих при защите информации в системах управления высокоскоростными и беспилотными транспортными средствами; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в системах управления высокоскоростными и беспилотными транспортными средствами.
	Эксплуатационный (вид ПД)	- установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения - установка, наладка, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем - проверка технического состояния и профилактические осмотры технических средств защиты информации - проведение аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты	- защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; - системы управления информационной безопасностью компьютерных систем; - методы и реализующие их средства защиты информации в компьютерных системах; - математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; - методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах; - математические модели процессов, возникающих при защите информации в системах управления высокоскоростными и беспилотными транспортными средствами; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в системах управления высокоскоростными и беспилотными транспортными средствами.

Приложение 3
к образовательному стандарту высшего образования
по специальности 10.05.01 Компьютерная безопасность

Перечень обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программы специалитета

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
06.022 Системный аналитик	D	Управление аналитическими работами и подразделением	7	Разработка методик выполнения аналитических работ	D/02.7	7
				Планирование аналитических работ в информационно-технологическом (далее - ИТ) проекте	D/03.7	7
				Организация аналитических работ в ИТ-проекте	D/04.7	7
				Контроль аналитических работ в ИТ-проекте	D/05.7	7
				Составление отчетов об аналитических работах в ИТ-проекте	D/06.7	7
				Управление процессами разработки и сопровождения требований к системам и управление качеством систем	D/08.7	7
				Управление аналитическими ресурсами и компетенциями	D/09.7	7
06.030 Специалист по защите информации в телекоммуникационных системах и сетях	D	Разработка средств защиты СССЭ (за исключением сетей связи специального назначения) от НСД	7	Анализ угроз информационной безопасности в сетях электросвязи	D/01.7	7
				Разработка средств и систем защиты СССЭ от НСД, защищенных телекоммуникационных систем (ЗТКС)	D/02.7	7
				Проведение научно-исследовательских и опытно-конструкторских работ (НИОКР) в сфере разработки средств и систем защиты СССЭ от НСД, создания ЗТКС	D/03.7	7
	F	Управление развитием средств и систем защиты СССЭ от НСД	7	Управление рисками систем защиты сетей электросвязи от НСД	F/01.7	7
				Управление отношениями с поставщиками и потребителями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД	F/02.7	7

				Управление отношениями с регуляторами в сфере защиты информации	F/03.7	7
06.032 Специалист по безопасности компьютерных систем и сетей	C	Оценивание уровня безопасности компьютерных систем и сетей	7	Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	C/01.7	7
				Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей	C/02.7	7
				Проведение анализа безопасности компьютерных систем	C/03.7	7
				Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов	C/04.7	7
				Проведение инструментального мониторинга защищенности компьютерных систем и сетей	C/05.7	7
				Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	C/06.7	7
06.033 Специалист по защите информации в автоматизированных системах	D	Разработка систем защиты информации автоматизированных систем	7	Тестирование систем защиты информации автоматизированных систем	D/01.7	7
				Разработка проектных решений по защите информации в автоматизированных системах	D/02.7	7
				Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	D/04.7	7
06.034 Специалист по технической защите информации	F	Проектирование объектов в защищенном исполнении	7	Проектирование средств и систем информатизации в защищенном исполнении	F/01.7	7
				Проектирование систем защиты информации на объектах информатизации	F/02.7	7
	G	Проведение аттестации объектов на соответствие требованиям по защите информации	7	Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации	G/01.7	7
				Проведение аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации	G/02.7	7

Приложение 4
к образовательному стандарту высшего образования
по специальности 10.05.01 Компьютерная безопасность

Универсальные компетенции выпускников и индикаторы их достижения

Категория (группа) компетенций	Специалитет	
	Компетенция	Индикаторы достижения компетенции
1	2	3
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Рассматривает возможные варианты решения задачи, оценивая их достоинства и недостатки. УК-1.2.Анализирует задачу, выделяя ее базовые составляющие, осуществляет декомпозицию задачи. УК-1.3. Выявляет естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и привлечь для их решения соответствующий физико-математический аппарат.
Разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1.Формулирует в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Определяет ожидаемые результаты решения выделенных задач. УК-2.2. Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений. УК-2.3. Решает конкретные задачи проекта заявленного качества и за установленное время. УК-2.4. Публично представляет результаты решения конкретной задачи проекта. УК-2.5 Демонстрирует уважительное отношение к праву и закону, достаточный уровень профессионального правосознания и правовой культуры для исполнения профессиональных обязанностей, обеспечивать защиту прав интеллектуальной собственности. УК-2.6 Способен разрабатывать варианты управленческих решений в сфере профессиональной деятельности, определять обоснованность их выбора на основе критериев соответствия требованиям нормативных правовых актов.

Командная работа и лидерство	УК-3. Способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1. Эффективно использует стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде. УК-3.2. Учитывает особенности поведения групп людей, с которыми работает/взаимодействует, учитывает их в своей деятельности. УК-3.3. Предвидит результаты (последствия) личных действий и планирует последовательность шагов для достижения заданного результата. УК-3.4. Эффективно взаимодействует с другими членами команды, в том числе участвует в обмене информацией, знаниями и опытом, в презентации результатов работы команды. УК-3.5. Планирует командную работу, распределяет поручения и делегирует полномочия членам команды. Организует обсуждение разных идей и мнений.
Коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном (ых) языке (ах), для академического и профессионального взаимодействия	УК-4.1. Выбирает на государственном и иностранном(-ых) языках коммуникативно приемлемые стиль делового общения, вербальные и невербальные средства взаимодействия с партнерами. УК-4.2. Использует информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном(-ых) языках. УК-4.3. Осуществляет коммуникацию на иностранном языке в ситуациях академического и профессионального общения в интернациональной среде с пониманием культурных, языковых и социально-экономических различий.
Межкультурное взаимодействие	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1. Умеет различать уровни познания, понимает, что собой представляет мировоззрение, как оно формируется и по каким основаниям может быть типологизировано, УК-5.2. Ставит философские вопросы и видеть возможные направления их решения. УК-5.3. Демонстрирует уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения.
Самоорганизация и саморазвитие (в том числе	УК-6. Способен определить и реализовать приоритеты собственной деятельности и способы ее	УК-6.1. Применяет знание о своих ресурсах и их пределах (личностных, ситуативных, временных и т.д.), для успешного выполнения порученной работы. УК-6.2. Понимает важность планирования перспективных целей собственной деятельности с учетом условий, средств, личностных возможностей, этапов карьерного

здоровье-сбережение)	совершенствования на основе самооценки и образования в течение всей жизни	роста, временной перспективы развития деятельности и требований рынка труда.
	УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1. Поддерживает должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности и соблюдает нормы здорового образа жизни.
Безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	УК-8.1 Анализирует основные природные и техносферные опасности, риск их реализации, свойства и характер воздействия вредных и опасных факторов природных и техносферных опасностей на человека и природную среду; УК-8.2 Соблюдает требования безопасности технических регламентов, законодательных актов, нормативно- правовых документов в области безопасности труда и охраны окружающей среды, реализует безопасные условия труда, в сфере своей профессиональной деятельности; УК-8.3 Применяет способы и средства защиты в чрезвычайных ситуациях, владеет приемами оказании первой помощи пострадавшим, в том числе при несчастных случаях на производстве.
Основы правовых знаний	УК-9. Способен осуществлять социальное взаимодействие в обществе и служебном (трудовом) коллективе, профессиональную деятельность на основе требований правовых (в том числе антикоррупционных) норм, содействовать противодействию коррупции	УК-9.1 Демонстрирует правильное толкование и способность применять правовые нормы в повседневной деятельности, обеспечивая соблюдение и защиту прав человека; способность осознанно исполнять требования законодательства УК-9.2 Осознаёт социальную значимость своей будущей профессии, понимает основные направления государственной антикоррупционной политики; УК-9.3 Демонстрирует нетерпимость к коррупционному поведению в жизни социума и трудовых коллективах УК-9.4 Способен давать оценку коррупционному поведению, содействовать пресечению проявлений коррупции в трудовых коллективах и в обществе

Приложение 5
к образовательному стандарту высшего образования
по специальности 10.05.01 Компьютерная безопасность

Общепрофессиональные компетенции выпускников и индикаторы их достижения

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
2	3
ОПК-1. Способен представлять роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1. Понимает значение информации и информационной безопасности в развитии современного общества, значимость своей будущей профессии.
ОПК-2. Способен применять программные средства системного и прикладного назначения для решения профессиональных задач	ОПК-2.1. Оценивает функциональные возможности аппаратных и программных средств, включая операционные системы, в составе компьютерной системы; проводит классификацию и устанавливает групповую принадлежность программного обеспечения. ПК-2.2. Выполняет работы по установке, настройке, администрированию и проверке работоспособности программно-аппаратные средства системного, прикладного и специального назначения в сфере профессиональной деятельности. ОПК-2.3. Выполняет управление инцидентами безопасности при функционировании программных средств системного, прикладного и специального назначения.
ОПК-3. Способен на основании совокупности существующих математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач защиты информации	ОПК-3.1. Применяет систему фундаментальных знаний (математических, естественнонаучных и инженерных) для формулирования и решения проблем задач защиты информации. ОПК-3.2. Применяет методы математического моделирования для формализации содержательно отчетливо сформулированных проблем.

ОПК-4. Способен представлять основные черты современной естественнонаучной картины мира и физические основы функционирования электронной компонентной базы	ОПК-4.1. Владеет основными понятиями современной естественнонаучной картины мира ОПК-4.2. Имеет представление о физических основах функционирования электронной компонентной базы систем компьютерной безопасности ОПК-4.3. Имеет применять на практике знания о современной естественнонаучной картине мира и физических основах функционирования электронной компонентной базы
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации (учреждения, предприятия)	ОПК-5.1. Использует нормативные правовые акты и нормативные методические документы, регламентирующие деятельность по информационной безопасности, в своей профессиональной деятельности. ОПК-5.2. Использует нормативные правовые акты и нормативные методические документы, регламентирующие деятельность по разработке и сопровождению современных компьютерных систем, в своей профессиональной деятельности.
ОПК-6. Способен анализировать и учитывать текущее состояние и тенденции развития методов криптографической защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, средств технической защиты информации, сетей и систем передачи информации при решении профессиональных задач	ОПК-6.1. Строит, анализирует и реализует алгоритмы, в том числе криптографические, в современных программных комплексах. ОПК-6.2. Строит, анализирует и реализует протоколы, в том числе криптографические, в современных программных комплексах. ОПК-6.3. Строит, анализирует и учитывает новые методы защиты в системах управления базами данных, сетей и систем передачи информации
ОПК-7. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ОПК-7.1. Имеет представление о различных методах научных исследований, их выборе и областях применения ОПК-7.2. Владеет навыками выбора методов научных исследований при решении конкретных задач ОПК-7.3. Умеет ставить и анализировать задачу при проведении разработок в области обеспечения безопасности компьютерных систем и сетей с точки зрения выбранного методы научных исследований
ОПК-8. Способен проводить анализ корректности реализации эффективных комбинаторных, теоретико-числовых и криптографических алгоритмов и протоколов применительно к конкретным условиям	ОПК-8.1. Строит, анализирует и реализует алгоритмы, в том числе криптографические, в современных программных комплексах. ОПК-8.2. Устанавливает причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. ОПК-8.3. Анализирует корректность комбинаторных, теоретико-числовых и криптографических алгоритмов в современных программных комплексах.

ОПК-9. Способен разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	ОПК-9.1. Владеет методами и средствами моделирования политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, угроз безопасности информации ОПК-9.2. Знает типовые модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, угроз безопасности информации ОПК-9.3. Умеет адаптировать типовые и строить оригинальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации
ОПК-10. Способен администрировать подсистемы и средства защиты информации в компьютерных системах и сетях	ОПК-10.1. Выполняет задачи по администрированию подсистем и средств защиты информации в КС ОПК-10.2. Выполняет задачи по администрированию подсистем и средств защиты информации в сетях
ОПК-11. Способен проводить оценку уровня безопасности компьютерных систем и сетей	ОПК-11.1. Знает методы, средства и нормативную базу оценки уровня безопасности компьютерных систем и сетей. ОПК-11.2. Умеет применять на практике методы, средства и нормативную базу оценки уровня безопасности компьютерных систем и сетей. ОПК-11.3. Умеет делать выводы об уровне безопасности компьютерных систем и сетей по полученным экспериментальным данным
ОПК-12. Способен участвовать в разработке программно-аппаратных средств защиты информации компьютерных систем и сетей	ОПК-12.1. Участвует в разработке программно-аппаратных средств защиты информации компьютерных систем и сетей.
ОПК-13. Способен производить проверки технического состояния и профилактические осмотры технических средств защиты информации	ОПК-13.1. Производит проверки технического состояния и профилактические осмотры технических средств защиты информации
ОПК-14. Способен выполнять работы по восстановлению работоспособности подсистем защиты информации в операционных системах, программно-аппаратных средствах защиты информации, в прикладном и системном программном обеспечении	ОПК-14.1. Владеет навыками по выявлению и дифференциации нарушений работоспособности подсистем защиты информации в операционных системах, программно-аппаратных средствах защиты информации, в прикладном и системном программном обеспечении ОПК-14.2. Знает последовательность действий по восстановлению работоспособности подсистем защиты информации в операционных системах, программно-аппаратных средствах защиты информации, в прикладном и системном программном обеспечении; умеет применять на практике эти знания

	ОПК-14.3. Умеет анализировать результаты выполненных работ по восстановлению работоспособности подсистем защиты информации в операционных системах, программно-аппаратных средствах защиты информации, в прикладном и системном программном обеспечении; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов
ОПК-15. Способен проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах, системах управления базами данных, компьютерных сетях	ОПК-15.1. Владеет методами и средствами мониторинга эффективности программно-аппаратных средств защиты информации в операционных системах, системах управления базами данных, компьютерных сетях ОПК-15.2. Умеет проводить дифференциацию и декомпозицию задач мониторинга эффективности различных программно-аппаратных средств защиты информации в операционных системах, системах управления базами данных, компьютерных сетях ОПК-15.3. Умеет анализировать полученные результаты мониторинга эффективности программно-аппаратных средств защиты информации в операционных системах, системах управления базами данных, компьютерных сетях и делать соответствующие выводы ОПК-15.4. Владеет навыками сравнительного анализа эффективности программно-аппаратных средств защиты информации в операционных системах
ОПК-16. Способен оценивать эффективность реализации действующих политик безопасности операционных систем и систем управления базами данных	ОПК-16.1. Владеет методами и средствами оценки эффективности операционных систем и систем управления базами данных ОПК-16.2. Умеет применять на практике методы и средства оценки эффективности операционных систем и систем управления базами данных ОПК-16.3. Умеет проводить дифференциацию и декомпозицию задач оценки эффективности реализации действующих политик безопасности операционных систем и систем управления базами данных ОПК-16.4. Умеет анализировать результаты оценки эффективности реализации действующих политик безопасности операционных систем и систем управления базами данных; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов
ОПК-17. Способен контролировать корректность функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях	ОПК-17.1. Владеет методами и средствами контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях ОПК-17.2. Умеет применять на практике методы и средства контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях ОПК-17.3. Умеет проводить дифференциацию и декомпозицию задач контроля

	корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях ОПК-17.4. Умеет анализировать результаты контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов
ОПК-18. Способен выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота с целью обеспечения защиты обрабатываемой информации	ОПК-18.1. Знает и умеет применять на практике методы и средства настройки параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота с целью обеспечения защиты обрабатываемой информации ОПК-18.2. Умеет определять требуемые значения параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота в зависимости от заданного уровня защиты обрабатываемой информации ОПК-18.3. Умеет ставить и решать задачи настройки параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота с целью обеспечения заданного уровня защиты обрабатываемой информации ОПК-18.4. Умеет анализировать результаты настройки параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота с целью обеспечения заданного уровня защиты обрабатываемой информации; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов
ОПК-19. Способен в процессе функционирования компьютерных систем и сетей и организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-19.1. Участвует в разработке проектной и технической документации, включая технические задания, технико-экономическое обоснование и проектную документацию на разрабатываемые программные средства. ОПК-19.2. Знает и умеет применять на практике нормативные, правовые и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем. ОПК-19.3. Разрабатывает проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем. ОПК-19.4. Разрабатывает научно-техническую документацию, готовит аналитические отчеты, научно-технические отчеты, обзоры, публикации по результатам выполненных работ.

	ОПК-19.5. Умеет применять современные программные средства для разработки и редакции проектно-конструкторской и технологической документации
ОПК-20. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-20.1. Знает основные этапы и закономерности исторического развития России, ее место и роль в современном мире ОПК-20. 2. Умеет применять на практике научно-обоснованные, философские, этические и естественнонаучные методы познания для формирования гражданской позиции и развития патриотизма

Приложение 6
к образовательному стандарту высшего образования
по специальности 10.05.01 Компьютерная безопасность

Обязательные профессиональные компетенции выпускников и индикаторы их достижения

Задача ПД	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ опыта)
1	2	3	4	5
Тип задач профессиональной деятельности – научно-исследовательский				
Анализ, разработка, внедрение, эксплуатация, экспертиза и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей, обеспечение безопасности информации в автоматизированных системах	- защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; - системы управления информационной безопасностью компьютерных систем; - методы и реализующие их средства защиты информации в компьютерных системах; - математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; - методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в	ПКО-1 Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах	ПКО-1.1. Участвует в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах. ПКО-1.2.Изучает и анализирует отечественный и зарубежный опыт по проблемам компьютерной безопасности ПКО-1.3. Участвует в проведении экспериментально-исследовательских работ при сертификации средств защиты информации.	06.030 Специалист по защите информации в телекоммуникационных системах и сетях; 06.032 Специалист по безопасности компьютерных систем и сетей; 06.033 Специалист по защите информации в автоматизированных системах; анализ опыта
		ПКО-2. Способен применять математические методы в области компьютерной безопасности	ПКО-2.1. Проводит анализ и разрабатывает под руководством квалифицированного специалиста математические модели безопасности компьютерных систем. ПКО-2.2. Применяет специальные математические методы, включая криптографические, для анализа и разработки защищенных компьютерных систем. ПКО-2.3.. Применяет решения на основе специальных математических методов для обеспечения защищенной передачи данных в современных компьютерных сетях.	

	компьютерных системах; - математические модели процессов, возникающих при защите информации в системах управления высокоскоростными и беспилотными транспортными средствами; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в системах управления высокоскоростными и беспилотными транспортными средствами.			
Тип задач профессиональной деятельности – проектный				
Анализ, разработка, внедрение, эксплуатация, экспертиза и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей, обеспечение безопасности информации в автоматизированных системах	- защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; - системы управления информационной безопасностью компьютерных систем; - методы и реализующие их средства защиты информации в компьютерных системах; - математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; - методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; - процессы (технологии) создания программного обеспечения средств и систем защиты информации,	ПКО-3. Способен проводить анализ исходных данных и формировать требования к компонентам и методам при проектировании подсистем и средств обеспечения информационной безопасности.	ПКО-3.1. Изучает и обобщает опыт работы различных учреждений, организаций и предприятий в области повышения эффективности защиты информации. ПКО-3.2. Формирует требования по защите информации, включая использование математического аппарата для решения прикладных задач. ПКО-3.3. Составляет планы этапов проведения научно-исследовательских и опытно-конструкторских работ. ПКО-3.4. Разрабатывает и анализирует структурные и функциональные схемы защищенных компьютерных систем в сфере профессиональной деятельности.	06.030 Специалист по защите информации в телекоммуникационных системах и сетях; 06.032 Специалист по безопасности компьютерных систем и сетей; 06.033 Специалист по защите информации в автоматизированных системах; 06.034 Специалист по технической защите информации; анализ опыта
		ПКО-4. Способен участвовать в разработке подсистемы информационной безопасности компьютерной (в том числе автоматизированной) системы включая разработку программно-аппаратных средств защиты информации, защищенных операционных	ПКО-4.1. Осуществляет рациональный выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности, создаваемых защищенных компьютерных систем в сфере профессиональной деятельности. ПКО-4.2. Проектирует и разрабатывает компоненты защищенных автоматизированных систем в сфере профессиональной деятельности.	

	обрабатываемой в компьютерных системах; - математические модели процессов, возникающих при защите информации в системах управления высокоскоростными и беспилотными транспортными средствами; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в системах управления высокоскоростными и беспилотными транспортными средствами.	систем, систем управления базами данных, компьютерных сетей, систем антивирусной защиты, средств криптографической защиты информации.		
		ПКО-5. Способен участвовать в работах по проектированию и реализации комплексного подхода к обеспечению информационной безопасности объекта защиты.	ПКО-5.1. Принимает участие в формировании политики информационной безопасности, ее реализации и контроле выполнения. ПКО-5.2. Формирует, организует и поддерживает комплекс мер по обеспечению информационной безопасности.	
Тип задач профессиональной деятельности – контрольно-аналитический				
Анализ, разработка, внедрение, эксплуатация, экспертиза и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей, обеспечение безопасности информации в автоматизированных системах	- защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; - системы управления информационной безопасностью компьютерных систем; - методы и реализующие их средства защиты информации в компьютерных системах; - математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; - методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; - процессы (технологии) создания программного обеспечения средств и систем	ПКО-6. Способен проводить оценку эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	ПКО-6.1. Подбирает методики и инструментарий, определяет критерии и осуществляет проверку эффективности систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	06.022 Системный аналитик; 06.030 Специалист по защите информации в телекоммуникационных системах и сетях; 06.032 Специалист по безопасности компьютерных систем и сетей; 06.033 Специалист по защите информации в автоматизированных системах; 06.034 Специалист по технической защите информации; анализ опыта
		ПКО-7. Способен проводить анализ информационной безопасности объектов и систем, принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации.	ПКО-7.1. Проводит анализ безопасности компьютерных систем, в том числе с использованием методов моделирования, на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности. ПКО-7.2. Участвует в проведении экспериментально- исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы.	

	защиты информации, обрабатываемой в компьютерных системах; - математические модели процессов, возникающих при защите информации в системах управления высокоскоростными и беспилотными транспортными средствами; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в системах управления высокоскоростными и беспилотными транспортными средствами.		ПКО-7.3. Вырабатывает рекомендации в связи с проведенным анализом безопасности, в том числе для принятия решения о повторной аттестации компьютерной системы (в том числе автоматизированных систем), предложения по устранению выявленных уязвимостей.	
		ПКО-8. Способен проводить инструментальный мониторинг защищенности компьютерных систем.	ПКО-8.1. Анализирует защищенность компьютерных систем с использованием сканеров безопасности. ПКО-8.2. Анализирует защищенность сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем.	
Тип задач профессиональной деятельности – организационно-управленческий				
Анализ, разработка, внедрение, эксплуатация, экспертиза и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей, обеспечение безопасности информации в автоматизированных системах	- защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; - системы управления информационной безопасностью компьютерных систем; - методы и реализующие их средства защиты информации в компьютерных системах; - математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; - методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; - процессы (технологии) создания программного	ПКО-9. Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию.	ПКО-9. 1. Разрабатывает и организует выполнение мероприятий в соответствии с положениями политики информационной безопасности и защиты информации ограниченного доступа. ПКО-9. 2. Разрабатывает предложения по совершенствованию системы управления информационной безопасностью компьютерной системы. ПКО-9.3. Разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	06.030 Специалист по защите информации в телекоммуникационных системах и сетях; 06.032 Специалист по безопасности компьютерных систем и сетей; 06.033 Специалист по защите информации в автоматизированных системах; 06.034 Специалист по технической защите информации; анализ опыта
		ПКО-10. Способен организовать процесс защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской	ПКО-10.1. Проверяет уровень квалификации, распределяет полномочия и контролирует выполнение инструкций в отношении персонала обслуживающего технические, программные и программно-аппаратные средства защиты информации. ПКО-10.2. Анализирует компьютерные системы в сфере профессиональной деятельности с целью	

	обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах; - математические модели процессов, возникающих при защите информации в системах управления высокоскоростными и беспилотными транспортными средствами; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в системах управления высокоскоростными и беспилотными транспортными средствами.	Федерации, Федеральной службы по техническому и экспортному контролю.	выявления условий, способствующих совершению правонарушений в отношении сведений ограниченного доступа.	
Тип задач профессиональной деятельности –эксплуатационный				
Анализ, разработка, внедрение, эксплуатация, экспертиза и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей, обеспечение безопасности информации в автоматизированных системах	- защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; - системы управления информационной безопасностью компьютерных систем; - методы и реализующие их средства защиты информации в компьютерных системах; - математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; - методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; - процессы (технологии)	ПКО-11. Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации.	ПКО-11.1. Обосновывает критерии и рассчитывает показатели эффективности защиты обрабатываемой информации. ПКО-11.2. Составляет методики тестирования, подбирает инструментарий и осуществляет проверку эффективности функционирования программных, программно-аппаратных и технических средств, подсистем защиты информации. ПКО-11.3. Выполняет работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации.	06.030 Специалист по защите информации в телекоммуникационных системах и сетях; 06.032 Специалист по безопасности компьютерных систем и сетей; 06.033 Специалист по защите информации в автоматизированных системах; 06.034 Специалист по технической защите информации; анализ опыта
		ПКО-12. Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности, проводить мониторинг и анализ эффективности реализации	ПКО-12.1. Выполняет работы, связанные с реализацией частных политик информационной безопасности автоматизированной системы. ПКО-12.2. Проводит мониторинг и аудит безопасности компьютерной системы в сфере профессиональной деятельности. ПКО-12.3. Формирует основные показатели и критерии эффективности, оценивает	

	создания программного обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах; - математические модели процессов, возникающих при защите информации в системах управления высокоскоростными и беспилотными транспортными средствами; - процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в системах управления высокоскоростными и беспилотными транспортными средствами.	систем защиты информации и действующих политик безопасности в компьютерных системах.	эффективность компьютерной системы и ее средств защиты в области профессиональной деятельности.	

Приложение 7
к образовательному стандарту высшего образования
по специальности 10.05.01 Компьютерная безопасность

Рекомендуемые профессиональные компетенции выпускников и индикаторы их достижения

Задача ПД	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ опыта)
1	2	3	4	5
Тип задач профессиональной деятельности – научно-исследовательский				
Анализ, разработка, внедрение, эксплуатация, экспертиза и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей, обеспечение безопасности информации в автоматизированных системах	– защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; – системы управления информационной безопасностью компьютерных систем; – методы и реализующие их средства защиты информации в компьютерных системах; – математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; – методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; – процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в	ПКР-1. Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов.	ПКР-1.1. Строит математические модели для оценки безопасности компьютерных систем. ПКР-1.2. Анализирует компоненты системы безопасности с использованием современных математических методов.	06.030 Специалист по защите информации в телекоммуникационных системах и сетях; 06.032 Специалист по безопасности компьютерных систем и сетей; 06.033 Специалист по защите информации в автоматизированных системах; анализ опыта
		ПКР-2. Способен проводить моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации	ПКР-2.1. Проводит моделирование автоматизированных систем с целью анализа уязвимостей ПКР-2.2. На основании проведенного моделирования определяет эффективность средств и способов защиты информации	

	компьютерных системах.			
Тип задач профессиональной деятельности – проектный				
Анализ, разработка, внедрение, эксплуатация, экспертиза и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей, обеспечение безопасности информации в автоматизированных системах	– защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; – системы управления информационной безопасностью компьютерных систем; – методы и реализующие их средства защиты информации в компьютерных системах; – математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; – методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; – процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах.	ПКР-3. Способен принимать участие в разработке проектных решений по защите информации в автоматизированных системах	ПКР-3.1. Участвует в разработке проектных решений по защите информации в автоматизированных системах высокоскоростного транспорта ПКР-3.2. Участвует в разработке проектных решений по защите информации в беспилотных автоматизированных системах	06.030 Специалист по защите информации в телекоммуникационных системах и сетях; 06.032 Специалист по безопасности компьютерных систем и сетей; 06.033 Специалист по защите информации в автоматизированных системах; 06.034 Специалист по технической защите информации; анализ опыта
		ПКР-4. Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем	ПКР-4.1. Разрабатывает программные средства для систем защиты информации автоматизированных систем высокоскоростного транспорта ПКР-4.2. Разрабатывает программные средства для систем защиты информации автоматизированных систем в беспилотных автоматизированных системах	
		ПКР-5. Способен проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.	ПКР-5.1. Проводит сравнительный анализ программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации. ПКР-5.2. Делает обоснованный выбор программно-аппаратных средств защиты информации.	
		ПКР-6. Способен принимать участие в разработке архитектуры системы защиты информации автоматизированной системы	ПКР-6.1. Участвует в разработке архитектуры системы защиты информации автоматизированных систем высокоскоростного транспорта. ПКР-6.2. Участвует в разработке архитектуры системы защиты информации беспилотных автоматизированных систем.	
Тип задач профессиональной деятельности – контрольно-аналитический				
Анализ, разработка, внедрение, эксплуатация, экспертиза и менеджмент средств и систем	– защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации; – системы управления информационной безопасностью	ПКР-7. Способен разрабатывать, анализировать и обосновывать адекватность математических моделейпроцессов, возникающих при работе	ПКР-7.1. Разрабатывает математические модели процессов, возникающих при работе программно- аппаратных средств защиты информации. ПКР-7.2. Анализирует математические модели процессов, возникающих при работе	06.030 Специалист по защите информации в телекоммуникационных системах и сетях; 06.032 Специалист по безопасности

обеспечения информационной безопасности компьютерных систем и сетей, обеспечение безопасности информации в автоматизированных системах	компьютерных систем; – методы и реализующие их средства защиты информации в компьютерных системах; – математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; – методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; – процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах.	программно-аппаратных средств защиты информации.	программно- аппаратных средств защиты информации. ПКР-7.3. Обосновывает адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.	компьютерных систем и сетей; 06.033 Специалист по защите информации в автоматизированных системах; 06.034 Специалист по технической защите информации; анализ опыта
Тип задач профессиональной деятельности – организационно-управленческий				
Обеспечение безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите	Формирование требований к защите информации в автоматизированных системах	ПКР-8. Способен подготовить обоснование необходимости защиты информации в автоматизированной системе	ПКР-8.1. Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы автоматизированных систем высокоскоростного транспорта ПКР-8.2. Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных систем	06.030 Специалист по защите информации в телекоммуникационных системах и сетях; 06.032 Специалист по безопасности компьютерных систем и сетей; 06.033 Специалист по защите информации в автоматизированных системах; 06.034 Специалист по технической защите информации; анализ опыта
Тип задач профессиональной деятельности –эксплуатационный				
Анализ, разработка, внедрение,	– защищаемые компьютерные системы и входящие в них	ПКР-9. Способен определять возможные угрозы	ПКР-9.1. Проводит анализ угроз безопасности информации, обрабатываемой	06.030 Специалист по защите информации в

эксплуатация, экспертиза и менеджмент средств и систем обеспечения информационной безопасности компьютерных систем и сетей, обеспечение безопасности информации в автоматизированных системах	средства обработки, хранения и передачи информации; – системы управления информационной безопасностью компьютерных систем; – методы и реализующие их средства защиты информации в компьютерных системах; – математические модели процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; – методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах; – процессы (технологии) создания программного обеспечения средств и систем защиты информации, обрабатываемой в компьютерных системах.	безопасности информации, обрабатываемой автоматизированной системой	автоматизированными системами высокоскоростного транспорта. ПКР-9.2. Проводит анализ угроз безопасности информации, обрабатываемой беспилотными автоматизированными системами.	телекоммуникационных системах и сетях; 06.032 Специалист по безопасности компьютерных систем и сетей; 06.033 Специалист по защите информации в автоматизированных системах; 06.034 Специалист по технической защите информации; анализ опыта
		ПКР-10. Способен проводить тестирование систем защиты информации автоматизированных систем	ПКР-10.1. Проводит индивидуальное тестирование систем защиты информации в блоке автоматизированных систем	
		ПКР-11. Способен участвовать в разработке эксплуатационной документации на системы защиты информации автоматизированных систем	ПКР-11.1. Участвует в разработке эксплуатационной документации системы защиты информации в автоматизированных системах высокоскоростного транспорта ПКР-11.2. Участвует в разработке эксплуатационной документации на системы защиты информации в беспилотных автоматизированных системах	