

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ПРИКАЗ**

**от 1 декабря 2016 г. № 1509**

**ОБ УТВЕРЖДЕНИИ**

**ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА**

**ВЫСШЕГО ОБРАЗОВАНИЯ ПО СПЕЦИАЛЬНОСТИ 10.05.03**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ**

**СИСТЕМ (УРОВЕНЬ СПЕЦИАЛИТЕТА)**

В соответствии с подпунктом 5.2.41 Положения о Министерстве образования и науки Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 3 июня 2013 г. № 466 (Собрание законодательства Российской Федерации, 2013, № 23, ст. 2923; № 33, ст. 4386; № 37, ст. 4702; 2014, № 2, ст. 126; № 6, ст. 582; № 27, ст. 3776; 2015, № 26, ст. 3898; № 43, ст. 5976; 2016, № 2, ст. 325; № 8, ст. 1121; № 28, ст. 4741), и пунктом 17 Правил разработки, утверждения федеральных государственных образовательных стандартов и внесения в них изменений, утвержденных постановлением Правительства Российской Федерации от 5 августа 2013 г. № 661 (Собрание законодательства Российской Федерации, 2013, № 33, ст. 4377; 2014, № 38, ст. 5069; 2016, № 16, ст. 2230), приказываю:

1. Утвердить прилагаемый федеральный государственный образовательный стандарт высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета).
2. Признать утратившими силу:

приказ Министерства образования и науки Российской Федерации от 17 января 2011 г. № 60 "Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки (специальности) 090303 Информационная безопасность автоматизированных систем (квалификация (степень) "специалист")" (зарегистрирован Министерством юстиции Российской Федерации 31 марта 2011 г.,

регистрационный № 20355);

пункт 42 изменений, которые вносятся в федеральные государственные образовательные стандарты высшего профессионального образования по направлениям подготовки (специальностям), подтверждаемого присвоением лицам квалификации (степени) "специалист", утвержденных приказом Министерства образования и науки Российской Федерации от 31 мая 2011 г. № 1975 (зарегистрирован Министерством юстиции Российской Федерации 28 июня 2011 г., регистрационный № 21200).

Министр

О.Ю. Васильева

Приложение

Утвержден  
приказом Министерства образования  
и науки Российской Федерации  
от 1 декабря 2016 г. № 1509

**ФЕДЕРАЛЬНЫЙ ГОСУДАРСТВЕННЫЙ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ**

**ВЫСШЕГО ОБРАЗОВАНИЯ**

**ПО СПЕЦИАЛЬНОСТИ**

**10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

**АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

**(УРОВЕНЬ СПЕЦИАЛИТЕТА)**

**I. ОБЛАСТЬ ПРИМЕНЕНИЯ**

Настоящий федеральный государственный образовательный стандарт высшего образования представляет собой совокупность требований, обязательных при реализации основных профессиональных образовательных программ высшего образования - программ специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем (далее соответственно - программа специалитета, специальность).

## II. ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

В настоящем федеральном государственном образовательном стандарте используются следующие сокращения:

ОК - общекультурные компетенции;

ОПК - общепрофессиональные компетенции;

ПК - профессиональные компетенции;

ПСК - профессионально-специализированные компетенции;

ФГОС ВО - федеральный государственный образовательный стандарт высшего образования;

сетевая форма - сетевая форма реализации образовательных программ.

## III. ХАРАКТЕРИСТИКА СПЕЦИАЛЬНОСТИ

3.1. Получение образования по программе специалитета допускается только в образовательной организации высшего образования (далее - организация).

3.2. Обучение по программе специалитета в организации осуществляется в очной форме обучения.

Объем программы специалитета составляет 300 зачетных единиц (далее - з.е.) вне зависимости от формы обучения, применяемых образовательных технологий, реализации программы специалитета с использованием сетевой формы, реализации программы специалитета по индивидуальному учебному плану, в том числе ускоренного обучения.

3.3. Срок получения образования по программе специалитета:

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

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 лиц с ограниченными возможностями здоровья может быть увеличен по их желанию не более чем на 1

год по сравнению со сроком получения образования для очной формы обучения. Объем программы специалитета за один учебный год при обучении по индивидуальному плану не может составлять более 75 з.е.

Конкретный срок получения образования и объем программы специалитета, реализуемый за один учебный год, при обучении по индивидуальному плану определяются организацией самостоятельно в пределах сроков, установленных настоящим пунктом.

3.4. При реализации программы специалитета организация вправе применять электронное обучение и дистанционные образовательные технологии.

При обучении лиц с ограниченными возможностями здоровья электронное обучение и дистанционные образовательные технологии должны предусматривать возможность приема-передачи информации в доступных для них формах.

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

3.5. Реализация программы специалитета возможна с использованием сетевой формы.

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

3.7. Программы специалитета, содержащие сведения, составляющие государственную тайну, разрабатываются и реализуются при создании условий и с соблюдением требований законодательства Российской Федерации о государственной тайне и нормативных правовых актов федеральных государственных органов, в ведении которых находятся организации, реализующие соответствующие образовательные программы [1].

[1] Часть 4 статьи 81 Федерального закона от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации" (Собрание законодательства Российской Федерации, 2012, № 53, ст. 7598; 2013, № 19, ст. 2326; № 23, ст. 2878; № 27, ст. 3462; № 30, ст. 4036; № 48, ст. 6165; 2014, № 6, ст. 562, ст. 566; № 19, ст. 2289; № 22, ст. 2769; № 23, ст. 2933; № 26, ст. 3388; № 30, ст. 4217, ст. 4257, ст. 4263; 2015, № 1, ст. 42, ст. 53, ст. 72; № 14, ст. 2008; № 27, ст. 3951, ст. 3989; № 29, ст. 4339, ст. 4364; № 51, ст. 7241; 2016, № 1, ст. 8, ст. 9, ст. 24, ст. 78; № 10, ст. 1320; № 23, ст. 3289, ст. 3290; № 27, ст. 4160, ст. 4219, ст. 4223, ст. 4238, ст. 4239, ст. 4245, ст. 4246, ст. 4292).

#### IV. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

##### ВЫПУСКНИКОВ, ОСВОИВШИХ ПРОГРАММУ СПЕЦИАЛИТЕТА

4.1. Область профессиональной деятельности выпускников, освоивших программу специалитета, включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере.

4.2. Объектами профессиональной деятельности выпускников, освоивших программу специалитета, являются:

автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;

технологии обеспечения информационной безопасности автоматизированных систем;

системы управления информационной безопасностью автоматизированных систем.

4.3. Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу специалитета:

научно-исследовательская;

проектно-конструкторская;

контрольно-аналитическая;

организационно-управленческая;

эксплуатационная.

При разработке и реализации программы специалитета организация ориентируется на все виды профессиональной деятельности, к которым готовится специалист.

Специализации, по которым готовятся выпускники, освоившие программу специалитета:

специализация № 1 "Автоматизированные информационные системы специального назначения";

специализация № 2 "Высокопроизводительные вычислительные системы специального назначения";

специализация № 3 "Информационная безопасность автоматизированных систем критически важных объектов";

специализация № 4 "Безопасность открытых информационных систем";

специализация № 5 "Информационная безопасность автоматизированных банковских систем";

специализация № 6 "Защищенные автоматизированные системы управления";

специализация № 7 "Обеспечение информационной безопасности распределенных информационных систем";

специализация № 8 "Анализ безопасности информационных систем";

специализация № 9 "Создание автоматизированных систем в защищенном исполнении";

специализация № 10 "Информационная безопасность автоматизированных систем на транспорте";

специализация № 11 "Специальные технологии информационной безопасности".

4.4. Выпускник, освоивший программу специалитета, должен быть готов решать следующие профессиональные задачи:

в соответствии с видами профессиональной деятельности:

научно-исследовательская деятельность:

сбор, обработка, анализ и систематизация научно-технической информации по проблематике информационной безопасности автоматизированных систем;

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

моделирование и исследование свойств защищенных автоматизированных систем;

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

разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;

проектно-конструкторская деятельность:

сбор и анализ исходных данных для проектирования защищенных автоматизированных систем;

разработка политик информационной безопасности автоматизированных систем;

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

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

разработка систем управления информационной безопасностью автоматизированных систем;

контрольно-аналитическая:

контроль работоспособности и эффективности применяемых средств защиты информации;

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

проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов;

организационно-управленческая деятельность:

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

организационно-методическое обеспечение информационной безопасности автоматизированных систем;

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

контроль реализации политики информационной безопасности;

эксплуатационная деятельность:

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

администрирование подсистем информационной безопасности автоматизированных систем;

мониторинг информационной безопасности автоматизированных систем;

управление информационной безопасностью автоматизированных систем;

обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций;

в соответствии со специализациями:

профессиональные задачи в соответствии со специализациями № 1 "Автоматизированные информационные системы специального назначения", № 2 "Высокопроизводительные вычислительные системы специального назначения", № 11 "Специальные технологии информационной безопасности" определяются квалификационными требованиями к военно-профессиональной, специальной профессиональной подготовке выпускников, установленными федеральными государственными органами, в ведении которых находятся федеральные государственные организации, реализующие соответствующие программы специалитета;

специализация № 3 "Информационная безопасность автоматизированных систем критически важных объектов":

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

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

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



автоматизированных систем критически важных объектов;

специализация № 4 "Безопасность открытых информационных систем":

разработка и реализация политики информационной безопасности открытых информационных систем;

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

контроль обеспечения информационной безопасности открытой информационной системы;

специализация № 5 "Информационная безопасность автоматизированных банковских систем":

разработка и реализация политики информационной безопасности автоматизированных банковских систем;

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

контроль обеспечения информационной безопасности автоматизированных банковских систем;

специализация № 6 "Защищенные автоматизированные системы управления":

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

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

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

специализация № 7 "Обеспечение информационной безопасности распределенных информационных систем":

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

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

аудит защищенности информационно-технологических ресурсов;

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

специализация № 8 "Анализ безопасности информационных систем":

использование языков, систем, инструментальных программных и аппаратных средства для моделирования информационных систем и испытаний систем защиты, в

том числе анализа безопасности программного обеспечения;

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

участие в сертификационных испытаниях по существующим требованиям;

специализация № 9 "Создание автоматизированных систем в защищенном исполнении":

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

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

специализация № 10 "Информационная безопасность автоматизированных систем на транспорте":

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

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

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

## V. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ПРОГРАММЫ СПЕЦИАЛИТЕТА

5.1. В результате освоения программы специалитета у выпускника должны быть сформированы общекультурные, общепрофессиональные, профессиональные и профессионально-специализированные компетенции.

5.2. Выпускник, освоивший программу специалитета, должен обладать следующими общекультурными компетенциями:

способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской

позиции и развития патриотизма (ОК-3);

способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);

способностью к самоорганизации и самообразованию (ОК-8);

способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

5.3. Выпускник, освоивший программу специалитета, должен обладать следующими общепрофессиональными компетенциями:

способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);

способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);

способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);

способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);

способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);

способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);

способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);

способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8).

5.4. Выпускник, освоивший программу специалитета, должен обладать следующими профессиональными компетенциями:

научно-исследовательская деятельность:

способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

способностью создавать и исследовать модели автоматизированных систем (ПК-2);

способностью проводить анализ защищенности автоматизированных систем (ПК-3);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

проектно-конструкторская деятельность:

способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);

способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

контрольно-аналитическая деятельность:

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов

по защите информации (ПК-16);

способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

организационно-управленческая деятельность:

способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

эксплуатационная деятельность:

способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

5.5. Выпускник, освоивший программу специалитета, должен обладать профессионально-специализированными компетенциями, соответствующими специализации программы специалитета:

содержание профессионально-специализированных компетенций специализаций № 1 "Автоматизированные информационные системы специального назначения", № 2 "Высокопроизводительные вычислительные системы специального назначения", № 11 "Специальные технологии информационной безопасности" определяется квалификационными требованиями к военно-профессиональной, специальной профессиональной подготовке выпускников, установленными федеральными государственными органами, в ведении которых находятся федеральные государственные организации, реализующие соответствующие программы специалитета;

специализация № 3 "Информационная безопасность автоматизированных систем критически важных объектов":

способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-3.1);

способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-3.2);

способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов (ПСК-3.3);

способностью разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов (ПСК-3.4);

способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-3.5);

специализация № 4 "Безопасность открытых информационных систем":

способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-4.1);

способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.2);

способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3);

способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы (ПСК-4.4);

способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.5);

специализация № 5 "Информационная безопасность автоматизированных банковских систем":

способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем (ПСК-5.1);

способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем (ПСК-5.2);

способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью автоматизированных банковских систем (ПСК-5.3);

способностью участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных банковских систем (ПСК-5.4);

способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы (ПСК-5.5);

специализация № 6 "Защищенные автоматизированные системы управления":

способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях (ПСК-6.1);

способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления (ПСК-6.2);

способностью планировать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью защищенных автоматизированных систем управления и организаций (ПСК-6.3);

способностью участвовать в разработке защищенных автоматизированных систем управления, применять современные технологии их проектирования (ПСК-6.4);

способностью участвовать в разработке и оценке соответствия средств защиты информации подсистем обеспечения информационной безопасности защищенных автоматизированных систем управления нормативным требованиям по защите информации (ПСК-6.5);

специализация № 7 "Обеспечение информационной безопасности распределенных информационных систем":

способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1);

способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);

способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);

способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4);

способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5);

специализация № 8 "Анализ безопасности информационных систем":

способностью использовать языки, системы, инструментальные программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты (ПСК-8.1);

способностью разрабатывать методики и тесты для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите

информации (ПСК-8.2);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности, планировать объем тестовых проверок (ПСК-8.3);

способностью применять инструментарий анализа безопасности программного обеспечения (ПСК-8.4);

способностью участвовать в сертификационных испытаниях по существующим требованиям (ПСК-8.5);

специализация № 9 "Создание автоматизированных систем в защищенном исполнении":

способностью принимать участие в моделировании, разработке, реализации и управлении процессами создания и эксплуатации автоматизированных систем в защищенном исполнении на всех стадиях и этапах их жизненного цикла (ПСК-9.1);

способностью рационально выбирать методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении (ПСК-9.2);

способностью применять современные технологии проектирования автоматизированных систем в защищенном исполнении (ПСК-9.3);

способностью применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла (ПСК-9.4);

способностью проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении (ПСК-9.5);

специализация № 10 "Информационная безопасность автоматизированных систем на транспорте":

способностью участвовать в разработке защищенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с использованием программных, программно-аппаратных и технических методов и средств защиты информации (ПСК-10.1);

способностью разрабатывать политику безопасности для совершенствования системы управления информационной безопасностью распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-10.2);

способностью осуществлять рациональный выбор средств и разрабатывать предложения по обеспечению информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-10.3);

способностью осуществлять мониторинг и аудит уровня защищенности, оценку соответствия и аттестацию распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учетом нормативных требований по защите информации (ПСК-10.4);

способностью обеспечить эффективное применение средств защиты электронного технологического документооборота и технического документооборота на транспорте (по видам) (ПСК-10.5).

5.6. При разработке программы специалитета все общекультурные, общепрофессиональные, профессиональные компетенции и профессионально-



специализированные компетенции, отнесенные к выбранной специализации, включаются в набор требуемых результатов освоения программы специалитета.

5.7. При разработке программы специалитета организация вправе дополнить набор компетенций выпускников с учетом направленности программы специалитета на конкретные области знания и (или) специализации программы.

5.8. При разработке программы специалитета требования к результатам обучения по отдельным дисциплинам (модулям), практикам организация устанавливает самостоятельно с учетом требований соответствующих примерных основных образовательных программ.

5.9. Программы специалитета, реализуемые в интересах обороны и безопасности государства, обеспечения законности и правопорядка в федеральных государственных организациях, находящихся в ведении федеральных государственных органов, указанных в части 1 статьи 81 Федерального закона от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации" (далее - федеральные государственные органы), разрабатываются на основе требований, предусмотренных указанным Федеральным законом, а также квалификационных требований к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемых федеральным государственным органом, в ведении которого находятся соответствующие организации [1].

[1] Часть 2 статьи 81 Федерального закона от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации" (Собрание законодательства Российской Федерации, 2012, № 53, ст. 7598; 2013, № 19, ст. 2326; № 23, ст. 2878; № 27, ст. 3462; № 30, ст. 4036; № 48, ст. 6165; 2014, № 6, ст. 562, ст. 566; № 19, ст. 2289; № 22, ст. 2769; № 23, ст. 2933; № 26, ст. 3388; № 30, ст. 4217, ст. 4257, ст. 4263; 2015, № 1, ст. 42, ст. 53, ст. 72; № 14, ст. 2008; № 27, ст. 3951, ст. 3989; № 29, ст. 4339, ст. 4364; № 51, ст. 7241; 2016, № 1, ст. 8, ст. 9, ст. 24, ст. 78; № 10, ст. 1320; № 23, ст. 3289, ст. 3290; № 27, ст. 4160, ст. 4219, ст. 4223, ст. 4238, ст. 4239, ст. 4245, ст. 4246, ст. 4292).

## VI. ТРЕБОВАНИЯ К СТРУКТУРЕ ПРОГРАММЫ СПЕЦИАЛИТЕТА

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

6.2. Программа специалитета состоит из следующих блоков:

Блок 1 "Дисциплины (модули)", который включает дисциплины (модули), относящиеся к базовой части программы, и дисциплины (модули), относящиеся к вариативной части программы;

Блок 2 "Практики, в том числе научно-исследовательская работа (НИР)", который в полном объеме относится к базовой части программы;

Блок 3 "Государственная итоговая аттестация", который в полном объеме относится к базовой части программы и завершается присвоением квалификации, указанной в перечне специальностей высшего образования, утвержденном Министерством образования и науки Российской Федерации [1].

[1] Перечень специальностей высшего образования - специалитета, утвержденный приказом Министерства образования и науки Российской Федерации от 12 сентября 2013 г. № 1061 (зарегистрирован Министерством юстиции Российской Федерации 14 октября 2013 г., регистрационный № 30163), с изменениями, внесенными приказами Министерства образования и науки Российской Федерации от 29 января 2014 г. № 63 (зарегистрирован Министерством юстиции Российской Федерации 28 февраля 2014 г., регистрационный № 31448), от 20 августа 2014 г. № 1033 (зарегистрирован Министерством юстиции Российской Федерации 3 сентября 2014 г., регистрационный № 33947), от 13 октября 2014 г. № 1313 (зарегистрирован Министерством юстиции Российской Федерации 13 ноября 2014 г., регистрационный № 34691), от 25 марта 2015 г. № 270 (зарегистрирован Министерством юстиции Российской Федерации 22 апреля 2015 г., регистрационный № 36994) и от 1 октября 2015 г. № 1080 (зарегистрирован Министерством юстиции Российской Федерации 19 октября 2015 г., регистрационный № 39355).

### Структура программы специалитета

Таблица

Структура программы специалитета		Объем программы специалитета в з.е.
Блок 1	Дисциплины (модули)	261 - 267
	Базовая часть,	186 - 216
	в том числе дисциплины (модули) специализации	15 - 21
	Вариативная часть	51 - 75
Блок 2	Практики, в том числе научно-исследовательская работа (НИР)	27 - 30
	Базовая часть	27 - 30
Блок 3	Государственная итоговая аттестация	6 - 9
	Базовая часть	6 - 9
Объем программы специалитета		300

6.3. Дисциплины (модули) и практики, относящиеся к базовой части программы специалитета, являются обязательными для освоения обучающимся с учетом специализации программы, которую он осваивает. Набор дисциплин (модулей) и практик, относящихся к базовой части программы специалитета, организация определяет самостоятельно в объеме, установленном настоящим ФГОС ВО, с учетом соответствующей (соответствующих) примерной (примерных) основной (основных) профессиональной (профессиональных) образовательной (образовательных) программы (программ).

6.4. Дисциплины (модули) по философии, истории, иностранному языку, безопасности жизнедеятельности, языкам программирования, технологиям и методам программирования, электронике и схемотехнике, безопасности операционных систем, безопасности сетей электронных вычислительных машин (далее - ЭВМ), безопасности систем баз данных, основам информационной безопасности, криптографическим методам защиты информации, организации ЭВМ и вычислительных систем, технической защите информации, сетям и системам передачи информации, организационному и правовому обеспечению информационной безопасности, программно-аппаратным средствам обеспечения информационной безопасности, разработке и эксплуатации защищенных автоматизированных систем, управлению информационной безопасностью реализуются в рамках базовой части Блока 1 "Дисциплины (модули)" программы специалитета. Объем, содержание и порядок

реализации указанных дисциплин (модулей) определяются организацией самостоятельно.

6.5. Дисциплины (модули) по физической культуре и спорту реализуются в рамках:

базовой части Блока 1 "Дисциплины (модули)" программы специалитета в объеме не менее 72 академических часов (2 з.е.) в очной форме обучения;

элективных дисциплин (модулей) в объеме не менее 328 академических часов. Указанные академические часы являются обязательными для освоения и в з.е. не переводятся.

Дисциплины (модули) по физической культуре и спорту реализуются в порядке, установленном организацией. Для инвалидов и лиц с ограниченными возможностями здоровья организация устанавливает особый порядок освоения дисциплин (модулей) по физической культуре и спорту с учетом состояния их здоровья.

В федеральных государственных организациях, находящихся в ведении федеральных государственных органов, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, в рамках элективных дисциплин (модулей) реализуются дисциплины (модули) по физической подготовке.

6.6. Дисциплины (модули), относящиеся к вариативной части программы специалитета, определяют в том числе направленность (профиль) и специализацию программы специалитета.

Набор дисциплин (модулей), относящихся к вариативной части программы специалитета, организация определяет самостоятельно в объеме, установленном настоящим ФГОС ВО. После выбора обучающимся специализации программы набор соответствующих выбранной специализации дисциплин (модулей) становится обязательным для освоения обучающимся.

6.7. В Блок 2 "Практики, в том числе научно-исследовательская работа (НИР)" входят учебная и производственная, в том числе преддипломная, практики.

Типы учебной практики:

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

учебно-лабораторный практикум;

ознакомительная практика;

экспериментально-исследовательская практика.

Типы производственной практики:

практика по получению профессиональных умений и опыта профессиональной деятельности;

эксплуатационная практика;

конструкторская практика;

технологическая практика;

научно-исследовательская работа.

Способы проведения учебной и производственной, в том числе преддипломной, практики:

стационарная;

выездная.

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

При разработке программ специалитета организация выбирает типы практик в зависимости от специализации программы. Организация вправе предусмотреть в программе специалитета иные типы практик дополнительно к установленным настоящим ФГОС ВО.

Учебная и (или) производственная практика может проводиться в структурных подразделениях организации, обладающих необходимым кадровым потенциалом и материально-технической базой.

Выбор мест прохождения практик для лиц с ограниченными возможностями здоровья производится с учетом состояния здоровья обучающихся и требований по доступности.

В федеральных государственных организациях, находящихся в ведении федеральных государственных органов, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, особенности организации и проведения практик определяются федеральным государственным органом, в ведении которого находится организация, в том числе за счет времени, выделяемого на проведение практик, могут проводиться комплексные учения (специальные профессиональные деловые игры).

6.8. В Блок 3 "Государственная итоговая аттестация" входит защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, а также подготовка к сдаче и сдача государственного экзамена (если организация включила государственный экзамен в состав государственной итоговой аттестации).

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

Проведение практик и государственных аттестационных испытаний, а также реализация дисциплин (модулей), на которых до обучающихся доводятся сведения ограниченного доступа и (или) в учебных целях используются секретные образцы вооружения, военной техники, их комплектующие изделия, не допускается с применением электронного обучения, дистанционных образовательных технологий.

6.10. При разработке программы специалитета обучающимся обеспечивается возможность освоения дисциплин (модулей) по выбору, в том числе специальные условия инвалидам и лицам с ограниченными возможностями здоровья, в объеме не менее 30 процентов вариативной части Блока 1 "Дисциплины (модули)".

В федеральных государственных организациях, находящихся в ведении федеральных государственных органов, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, особенности формирования вариативной части образовательных программ и освоения

дисциплин (модулей) по выбору определяются федеральным государственным органом, в ведении которого находится организация.

6.11. Количество часов, отведенных на занятия лекционного типа, в целом по Блоку 1 "Дисциплины (модули)", должно составлять не более 55 процентов от общего количества часов аудиторных занятий, отведенных на реализацию данного Блока.

## VII. ТРЕБОВАНИЯ К УСЛОВИЯМ РЕАЛИЗАЦИИ

### ПРОГРАММЫ СПЕЦИАЛИТЕТА

7.1. Общесистемные требования к реализации программы специалитета.

7.1.1. Организация должна располагать материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

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

Электронная информационно-образовательная среда организации должна обеспечивать:

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

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы;

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

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

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

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование электронной информационно-образовательной среды должно соответствовать законодательству Российской Федерации [1].

[1] Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196; 2011, № 15, ст. 2038; № 30, ст. 4600; 2012, № 31, ст. 4328; 2013, № 14, ст. 1658; № 23, ст. 2870; № 27, ст. 3479; № 52, ст. 6961, ст. 6963; 2014, № 19, ст. 2302; № 30, ст. 4223, ст. 4243, № 48, ст. 6645; 2015, № 1, ст. 84; № 27, ст. 3979; № 29, ст. 4389, ст. 4390; 2016, № 28, ст. 4558), Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; 2011, № 23, ст. 3263; № 31, ст. 4701; 2013, № 14, ст. 1651; № 30, ст. 4038; № 51, ст. 6683; 2014, № 23, ст. 2927; № 30, ст. 4217, ст. 4243).

В федеральных государственных организациях, находящихся в ведении федеральных государственных органов, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, функциональные возможности, порядок формирования, использования и эксплуатации электронной информационно-образовательной среды, особенности доступа обучающихся к электронно-библиотечной системе (электронной библиотеке) и электронной информационно-образовательной среде, а также к современным профессиональным базам данных и информационным справочным системам, к компьютерной технике, подключенной к локальным сетям и (или) сети "Интернет", определяются федеральным государственным органом, в ведении которого находится организация.

7.1.3. В случае 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.

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

7.1.5. Квалификация руководящих и научно-педагогических работников организации должна соответствовать квалификационным характеристикам, установленным в Едином квалификационном справочнике должностей руководителей, специалистов и служащих, разделе "Квалификационные характеристики должностей руководителей и специалистов высшего профессионального и дополнительного профессионального образования", утвержденном приказом Министерства здравоохранения и социального развития Российской Федерации от 11 января 2011 г. № 1н (зарегистрирован Министерством юстиции Российской Федерации 23 марта 2011 г., регистрационный № 20237), и профессиональным стандартам (при наличии).

В федеральных государственных организациях, находящихся в ведении федеральных государственных органов, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, квалификационные характеристики должностей руководителей и научно-педагогических работников высшего образования и дополнительного профессионального образования определяются в соответствии с законодательством Российской Федерации.

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

7.1.7. Реализация программы специалитета по данной специальности допускается только при наличии у организации лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну.

7.1.8. Для реализации программы специалитета организация должна определить отдельную кафедру или иное структурное подразделение, деятельность которых направлена на реализацию образовательных программ высшего образования по специальностям и направлениям подготовки, входящим в укрупненную группу специальностей и направлений подготовки 10.00.00 "Информационная безопасность".

7.2. Требования к кадровым условиям реализации программ специалитета.

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

7.2.2. Доля научно-педагогических работников (в приведенных к целочисленным значениям ставок) имеющих образование и (или) ученую степень, соответствующие профилю преподаваемой дисциплины (модуля), в общем числе научно-педагогических работников, реализующих программу специалитета, должна составлять не менее 80 процентов.

7.2.3. Доля научно-педагогических работников (в приведенных к целочисленным значениям ставок), имеющих ученую степень (в том числе ученую степень, присвоенную за рубежом и признаваемую в Российской Федерации) и (или) ученое звание (в том числе ученое звание, полученное за рубежом и признаваемое в Российской Федерации), в общем числе научно-педагогических работников, реализующих программу специалитета, должна быть не менее 60 процентов.

В федеральных государственных организациях, находящихся в ведении федеральных государственных органов, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, доля преподавателей указанных категорий определяется федеральным государственным органом, в ведении которого находится организация.

В федеральных государственных организациях, находящихся в ведении федеральных государственных органов, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, к научно-педагогическим работникам с учеными степенями и (или) учеными званиями приравниваются преподаватели военно-профессиональных и специально-профессиональных дисциплин (модулей) без ученых степеней и (или) ученых званий, имеющие профильное высшее образование, опыт военной службы (службы в правоохранительных органах) в области и с объектами профессиональной деятельности, соответствующими программе специалитета, не менее 10 лет, воинское (специальное) звание не ниже "майор" ("капитан 3 ранга"), а также имеющие боевой опыт, или государственные награды, или государственные (отраслевые) почетные звания, или государственные премии.

В числе научно-педагогических работников с ученой степенью доктора наук и (или) ученым званием профессора могут учитываться преподаватели военно-профессиональных и (или) специально-профессиональных дисциплин (модулей) с ученой степенью кандидата наук, имеющие или государственные награды, или государственные (отраслевые) почетные звания, или являющиеся лауреатами государственных премий.

7.2.4. Доля работников (в приведенных к целочисленным значениям ставок) из числа руководителей и работников организаций, деятельность которых связана со специализацией реализуемой программы специалитета (имеющих стаж работы в данной профессиональной области не менее 3 лет), в общем числе работников, реализующих программу специалитета, должна быть не менее 5 процентов.

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

7.3.1. Специальные помещения должны представлять собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового

проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Специальные помещения должны быть укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

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

Перечень материально-технического обеспечения, необходимого для реализации программы специалитета, включает в себя лаборатории и специализированные кабинеты (классы, аудитории), оснащенные лабораторным оборудованием, в зависимости от степени его сложности.

Минимально необходимый для реализации программы специалитета перечень материально-технического обеспечения должен включать в себя лаборатории в области:

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

электротехники, электроники и схемотехники, оснащенную учебно-лабораторными стендами для изучения работы компонентов узлов и блоков вычислительных устройств, рабочих мест разработчиков систем и устройств в системах автоматизированного проектирования, 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, структурированной кабельной системой, телекоммуникационным оборудованием, обучающим программным обеспечением, эмулятором активного сетевого оборудования;

безопасности сетей ЭВМ, оснащенную стендами для изучения проводных и беспроводных компьютерных сетей, включающих абонентские устройства, коммутаторы, маршрутизаторы, точки доступа, межсетевые экраны, системы обнаружения компьютерных атак, системы углубленной проверки сетевых пакетов и системы защиты от утечки данных, анализаторы кабельных сетей;

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;

программно-аппаратных средств обеспечения информационной безопасности, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, средствами сканирования защищенности компьютерных сетей, устройствами чтения смарт-карт и радиометок, программно-аппаратными комплексами защиты информации, включая криптографические средства защиты информации;

защищенных автоматизированных систем, оснащенную аппаратно-программными средствами управления доступом к данным, шифрования, средствами дублирования и восстановления данных, средствами мониторинга состояния автоматизированных систем, источниками бесперебойного и аварийного питания, средствами контроля и управления доступом в помещения, охранной и пожарной сигнализацией, климатическим контролем;

специально оборудованные кабинеты (классы, аудитории):

Интернет-технологий, оснащенный рабочими местами на базе вычислительной техники и мобильными абонентскими устройствами, подключенными к сети "Интернет" с использованием проводных и/или беспроводных технологий;



для выполнения работ в рамках курсового и дипломного проектирования, научно-исследовательской работы обучающихся, оснащенные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых для проведения исследований дополнительных аппаратных и/или программных средств, а также комплектом оборудования для печати.

Компьютерные 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), а также комплектом проекционного оборудования для преподавателя.

Организация должна иметь лаборатории и (или) специально оборудованные кабинеты (классы, аудитории), обеспечивающие практическую подготовку в соответствии с каждой специализацией программы специалитета, которые она реализует.

Выполнение требований к материально-техническому обеспечению программ специалитета должно обеспечиваться необходимыми материально-техническими ресурсами, в том числе расходными материалами и другими специализированными материальными запасами.

Конкретные требования к материально-техническому и учебно-методическому обеспечению определяются в примерных основных образовательных программах.

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

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

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

Фонд дополнительной литературы помимо учебной должен включать официальные, справочно-библиографические и специализированные отечественные и зарубежные периодические издания, правовые нормативные акты и нормативные методические документы в области информационной безопасности, в том числе ограниченного доступа, в расчете один - два экземпляра на каждые 100 обучающихся по данной специальности.

7.3.2. Организация должна быть обеспечена необходимым комплектом лицензионного программного обеспечения и сертифицированными программными и аппаратными средствами защиты информации, состав которых определяется в рабочих программах дисциплин (модулей).

7.3.3. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда должны обеспечивать одновременный доступ не менее 25 процентов обучающихся по программе специалитета.

7.3.4. 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).

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

#### 7.4. Требования к финансовым условиям реализации программы специалитета.

7.4.1. Финансовое обеспечение реализации программы специалитета должно осуществляться в объеме не ниже установленных Министерством образования и науки Российской Федерации базовых нормативных затрат на оказание государственной услуги в сфере образования для данного уровня образования и направления подготовки с учетом корректирующих коэффициентов, учитывающих специфику образовательных программ в соответствии с Методикой определения нормативных затрат на оказание государственных услуг по реализации образовательных программ высшего образования по специальностям (направлениям подготовки) и укрупненным группам специальностей (направлений подготовки), утвержденной приказом Министерства образования и науки Российской Федерации от 30 октября 2015 г. № 1272 (зарегистрирован Министерством юстиции Российской Федерации 30 ноября 2015 г., регистрационный № 39898).

7.4.2. В организации, в которой законодательством Российской Федерации предусмотрена военная или иная приравненная к ней служба, служба в правоохранительных органах, финансовое обеспечение реализации программы специалитета должно осуществляться в пределах бюджетных ассигнований федерального бюджета, выделяемых федеральным органом исполнительной власти.