

КОПИЯ



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

(МИНОБРНАУКИ РОССИИ)

П Р И К А З

« 1 » декабря 2016 г.

Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ № 1512
ЗАРЕГИСТРИРОВАНО
 Регистрационный № 44825
 от 20 декабря 2016.

Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 10.05.01 Компьютерная безопасность (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), п р и к а з ы в а ю:

1. Утвердить прилагаемый федеральный государственный образовательный стандарт высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета).

2. Признать утратившими силу:

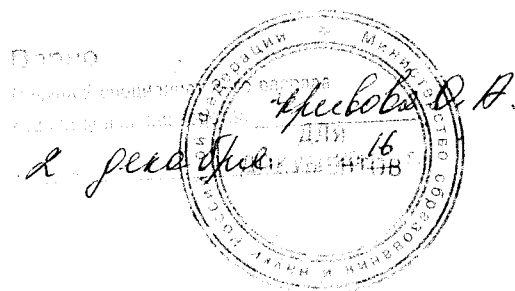
приказ Министерства образования и науки Российской Федерации от 17 января 2011 г. № 69 «Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального

образования по направлению подготовки (специальности) 090301 Компьютерная безопасность (квалификация (степень) «специалист»)» (зарегистрирован Министерством юстиции Российской Федерации 20 апреля 2011 г., регистрационный № 20544);

пункт 40 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» сентября 2016 г. № 1512

ФЕДЕРАЛЬНЫЙ ГОСУДАРСТВЕННЫЙ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ОБРАЗОВАНИЯ

по специальности

10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

(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 10.05.01 Компьютерная безопасность (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 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.

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 5,5 лет. Объем программы специалитета в очной форме обучения, реализуемый за один учебный год, составляет 60 з.е.;

при обучении по индивидуальному учебному плану вне зависимости от формы обучения 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.

В федеральных государственных организациях, находящихся в ведении федеральных государственных органов, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и

правопорядка, срок обучения по программе специалитета в связи с продолжительностью каникулярного времени обучающихся¹ составляет не менее 5 лет. При этом объем образовательной программы не изменяется, а объем программы специалитета, реализуемый за один учебный год по очной форме, составляет не более 75 з.е.

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 программы 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

¹ Пункт 1 статьи 30 Положения о порядке прохождения военной службы, утвержденного Указом Президента Российской Федерации от 16 сентября 1999 г. № 1237 «Вопросы прохождения военной службы» (Собрание законодательства Российской Федерации, 1999, № 38, ст. 4534; № 42, ст. 5008; 2000, № 16, ст. 1678; № 27, ст. 2819; 2003, № 16, ст. 1508; 2006, № 25, ст. 2697; 2007, № 11, ст. 1284; № 13, ст. 1527; № 29, ст. 3679; № 35, ст. 4289; № 38, ст. 4513; 2008, № 3, ст. 169, ст. 170; № 13, ст. 1251; № 43, ст. 4919; 2009, № 2, ст. 180; № 18, ст. 2217; № 28, ст. 3519; № 49, ст. 5918; 2010, № 27, ст. 3446; 2011, № 4, ст. 572; № 13, ст. 1741; № 40, ст. 5532; 2012, № 2, ст. 244; № 29, ст. 4075; № 47, ст. 6457; 2013, № 7, ст. 633; № 13, ст. 1526; 2014, № 8, ст. 783; № 27, ст. 3754; № 40, ст. 5413; 2015, № 1, ст. 199; № 13, ст. 1909; № 18, ст. 2691; № 25, ст. 3643; № 43, ст. 5947; 2016, № 1, ст. 216).

государственных органов, в ведении которых находятся организации, реализующие соответствующие образовательные программы².

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 разработкой и эксплуатацией средств и систем защиты информации компьютерных систем, доказательным анализом и обеспечением защищенности компьютерных систем от вредоносных программно-технических и информационных воздействий в условиях существования угроз в информационной сфере.

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

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.

² 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).

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

- научно-исследовательская;**
- проектная;**
- контрольно-аналитическая;**
- организационно-управленческая;**
- эксплуатационная.**

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

Специализации, по которым готовятся выпускники, освоившие программу специалитета:

- 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».

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, 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 учреждений 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;

проектная деятельность:

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 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;

контрольно-аналитическая деятельность:

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;

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;

организационно-управленческая деятельность:

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;

организация работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа (сведений, составляющих государственную тайну и конфиденциальной информации);

эксплуатационная деятельность:

установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения;

установка, наладка, тестирование и обслуживание программно-аппаратных 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;

в соответствии со специализациями:

специализация № 1 «Анализ безопасности компьютерных систем»:

анализ защищенности и поиск уязвимостей компьютерной системы, в том числе с использованием современных критериев и стандартов;

оценка корректности и эффективности программных реализаций алгоритмов защиты информации;

оценка корректности и эффективности программных реализаций алгоритмов защиты информации;

разработка, отладка и тестирование программного кода с использованием языков и систем программирования низкого уровня;

специализация № 2 «Математические методы защиты информации»:

разработка вычислительных алгоритмов, реализующих современные математические методы защиты информации;

разработка, анализ и обоснование адекватности математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации, а также математических моделей для оценки безопасности компьютерных систем;

оценка эффективности средств и методов защиты информации в компьютерных системах, сравнительный анализ и обоснованный выбор программно-аппаратных средств защиты информации;

специализация № 3 «Безопасность распределенных компьютерных систем»:

анализ безопасности распределенных компьютерных систем, защиты информации в них, мониторинг, аудит и контрольные проверки их работоспособности и защищенности;

разработка программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности;

организация защиты информации в распределенных компьютерных системах, включая формирование, реализацию и контроль эффективности политики их информационной безопасности;

специализация № 4 «Разработка защищенного программного обеспечения»:

разработка защищенного программного обеспечения с использованием современных технологий программирования, средств разработки программного обеспечения, новых образцов программных средств защиты в распределенных компьютерных системах и требований современных стандартов по безопасности компьютерных систем;

анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей;

разработка технической документации на программное обеспечение в соответствии с действующими стандартами;

специализация № 5 «Безопасность высокопроизводительных вычислительных систем»:

разработка и эксплуатация средств и инструментальных сред проектирования, разработки и исследования систем высокопроизводительных вычислений;

выявление и анализ атак на высокопроизводительные системы высокой доступности;

использование методов проектирования и средства обеспечения безопасности защищенных высокопроизводительных систем, средств их системного администрирования и защиты;

специализация № 6 «Безопасность программного обеспечения мобильных систем»:

анализ систем безопасности мобильных устройств и устройств беспроводной связи и разработка программных средств обеспечения их защиты;

разработка прикладного и системного программного обеспечения для мобильных устройств с учётом требований по безопасности;

реализация быстрых вычислительных алгоритмов средствами мобильных устройств;

специализация № 7 «Информационно-аналитическая и техническая экспертиза компьютерных систем»:

поиск, фиксация, анализ и документирование следов компьютерных преступлений, правонарушений и инцидентов, в том числе экспертиза вычислительной техники и носителей компьютерной информации, с учетом нормативных правовых актов и иных требований;

разработка программного обеспечения для выявления следов компьютерных преступлений и инцидентов;

специализация № 8 «Информационная безопасность объектов информатизации на базе компьютерных систем»:

разработка проектных решений и анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации,

в том числе разработка модели угроз и формирование требования к обеспечению информационной безопасности;

разработка проектов нормативных правовых актов, руководящих и методических документов предприятия, учреждения, регламентирующих деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации;

специализация № 9 «Специальные технологии противодействия компьютерным атакам»:

профессиональные задачи определяются квалификационными требованиями к военно-профессиональной, специальной профессиональной подготовке выпускников, утверждаемыми федеральными органами исполнительной власти, в ведении которых находятся федеральные государственные организации.

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, её 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 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 при решении профессиональных задач (ОПК-1);

способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);

способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);

способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);

способностью использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);

способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-6);

способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения (ОПК-7);

способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8);

способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9);

способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ОПК-10).

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

научно-исследовательская деятельность:

способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности (ПК-1);

способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований (ПК-2);

способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности (ПК-3);

способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПК-4);

проектная деятельность:

способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные

системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-5);

способностью участвовать в разработке проектной и технической документации (ПК-6);

способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем (ПК-7);

способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы (ПК-8);

контрольно-аналитическая деятельность:

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы (ПК-9);

способностью оценивать эффективность 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 (ПК-10);

способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации (ПК-11);

способностью проводить инструментальный мониторинг защищенности компьютерных систем (ПК-12);

организационно-управленческая деятельность:

способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-13);

способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа (ПК-14);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы (ПК-15);

способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем (ПК-16);

эксплуатационная деятельность:

способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение (ПК-17);

способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-18);

способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации (ПК-19);

способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций (ПК-20).

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

специализация № 1 «Анализ безопасности компьютерных систем»:

способностью проводить анализ защищенности и находить уязвимости компьютерной системы (ПСК-1.1);

способностью оценивать корректность и эффективность программных реализаций алгоритмов защиты информации (ПСК-1.2);

способностью использовать современные критерии и стандарты для анализа безопасности компьютерных систем (ПСК-1.3);

способностью разрабатывать, отлаживать и тестировать программный код с использованием языков и систем программирования низкого уровня (ПСК-1.4);

способностью учитывать в профессиональной деятельности современные тенденции развития алгоритмов кодирования и сжатия различных видов информации (ПСК-1.5);

специализация № 2 «Математические методы защиты информации»:

способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации (ПСК-2.1);

способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах (ПСК-2.2);

способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов (ПСК-2.3);

способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации (ПСК-2.4);

способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации (ПСК-2.5);

специализация № 3 «Безопасность распределенных компьютерных систем»:

способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем (ПСК-3.1);

способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем (ПСК-3.2);

способностью использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности (ПСК-3.3);

способностью организовывать защиту информации в распределенных компьютерных системах (ПСК-3.4);