Приказ Министерства образования и науки РФ от 17 января 2011 г. N 69 "Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки (специальности) 090301 Компьютерная безопасность (квалификация (степень) "специалист")"

В соответствии с пунктом 5.2.7 Положения о Министерстве образования и науки Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 15 мая 2010 г. N 337 (Собрание законодательства Российской Федерации, 2010, N 21, ст. 2603; N 26, ст. 3350), пунктом 7 Правил разработки и утверждения федеральных государственных образовательных стандартов, утвержденных постановлением Правительства Российской Федерации от 24 февраля 2009 г. N 142 (Собрание законодательства Российской Федерации, 2009, N 9, ст. 1110), приказываю:

Утвердить прилагаемый федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки (специальности) 090301 Компьютерная безопасность (квалификация (степень) "специалист") и ввести его в действие со дня вступления в силу настоящего приказа.

Министр А.А. Фурсенко

Зарегистрировано в Минюсте РФ 20 апреля 2011 г.
Регистрационный N 20544

Приложение

Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки (специальности) 090301 Компьютерная безопасность (квалификация (степень) "специалист")
(утв. приказом Министерства образования и науки РФ от 17 января 2011 г. N 69)

Комментарий ГАРАНТа
См. справку о федеральных государственных образовательных стандартах

I. Область применения

1.1. Настоящий федеральный государственный образовательный стандарт высшего профессионального образования (ФГОС ВПО) представляет собой совокупность требований, обязательных при реализации основных образовательных программ подготовки специалистов по направлению подготовки (специальности) 090301 Компьютерная безопасность образовательными учреждениями высшего профессионального образования (высшими учебными заведениями, вузами), имеющими государственную аккредитацию, на территории Российской Федерации.

1.2. Право на реализацию основных образовательных программ высшее учебное заведение имеет только при наличии соответствующей лицензии, выданной уполномоченным федеральным органом исполнительной власти.

II. Используемые сокращения

В настоящем стандарте используются следующие сокращения:

ВПО	- высшее профессиональное образование;
ООП	- основная образовательная программа;
ОК	- общекультурные компетенции;
ПК	- профессиональные компетенции;
ПСК	- профессионально-специализированные компетенции;
УЦ ООП	- учебный цикл основной образовательной программы;
ФГОС ВПО	- федеральный государственный образовательный стандарт высшего профессионального образования.

III. Характеристика направления подготовки (специальности)

Нормативный срок, общая трудоемкость освоения ООП (в зачетных единицах)* и соответствующая квалификация (степень) приведены в таблице 1.

Таблица 1

Сроки, трудоемкость освоения ООП и квалификация (степень) выпускников

Наименование ООП	Квалификация (степень)		Нормативный срок освоения ООП (для очной формы обучения), включая каникулы, предоставляемые после прохождения итоговой государственной аттестации	Трудоемкость (в зачетных единицах)
	Код в соответствии с принятой классификацией ООП	Наименование		
ООП подготовки специалиста	65	специалист	5,5 лет	330*

* Трудоемкость основной образовательной программы подготовки специалиста по очной форме обучения в среднем за учебный год равна 60 зачетным единицам.

По данной ООП подготовки специалиста обучение в форме очно-заочной (вечерней), заочной и экстерната не допускается.

IV. Характеристика профессиональной деятельности специалистов

4.1. Область профессиональной деятельности специалистов 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 специалистов 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.

4.3. Специалист по направлению подготовки (специальности) 090301 Компьютерная безопасность готовится к следующим видам профессиональной деятельности:

научно-исследовательская;

проектная;

контрольно-аналитическая;

организационно-управленческая;

эксплуатационная.

Конкретные виды профессиональной деятельности, к которым в основном готовится специалист, определяются высшим учебным заведением совместно с обучающимися, научно-педагогическими работниками высшего учебного заведения и объединениями работодателей.

По окончании обучения по направлению подготовки (специальности) 090301 Компьютерная безопасность, наряду с квалификацией (степенью) "специалист" присваивается специальное звание "специалист по защите информации".

4.4. Специалист по направлению подготовки (специальности) 090301 Компьютерная безопасность должен 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;

проведение измерений и наблюдений, составление описания проводимых исследований, подготовка данных для составления обзоров, отчетов и научных публикаций;

изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте;

разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов;

обоснование и выбор рационального решения по уровню обеспечения защищенности компьютерной системы с учетом заданных требований;

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

проектная деятельность:

сбор и анализ исходных данных для проектирования систем 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;

сопровождение разработки технического и программного обеспечения системы информационной безопасности;

контрольно-аналитическая деятельность:

проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средствах защиты информации;

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;

осуществление правового, организационного и технического обеспечения защиты информации;

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

эксплуатационная деятельность:

установка, настройка, эксплуатация и обслуживание аппаратно-программных средств защиты информации;

проверка технического состояния и остаточного ресурса оборудования защиты информации, организация профилактических проверок и текущего ремонта;

приемка и освоение программно-аппаратных средств защиты информации;

составление инструкций по эксплуатации аппаратно-программных средств защиты информации;

обеспечение эффективного функционирования средств защиты информации с учетом требований по обеспечению защищенности компьютерной системы;

администрирование подсистем информационной безопасности компьютерных систем;

обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций;

проведение аттестации технических средств, программ, алгоритмов на предмет

соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

V. Требования к результатам освоения основных образовательных программ подготовки специалиста

5.1. Выпускник должен обладать следующими общекультурными компетенциями (ОК):

способностью действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма (ОК-1);

способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики (ОК-2);

способностью анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач (ОК-3);

способностью понимать движущие силы и закономерности исторического процесса, роль личности в истории, политической организации общества, способностью уважительно и бережно относиться к историческому наследию, толерантно воспринимать социальные и культурные различия (ОК-4);

способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-5);

способностью к работе в коллективе, кооперации с коллегами, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (ОК-6);

способностью логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);

способностью к письменной и устной деловой коммуникации, к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков (ОК-8);

способностью к логически-правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания (ОК-9);

способностью самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой деятельности, развития социальных и профессиональных компетенций, изменения вида своей профессиональной деятельности (ОК-10);

способностью к осуществлению воспитательной и образовательной деятельности (ОК-11);

способностью самостоятельно применять методы физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, достижения должного уровня физической подготовленности в целях обеспечения полноценной социальной и профессиональной деятельности (ОК-12).

5.2. Выпускник должен обладать следующими профессиональными компетенциями (ПК):

общепрофессиональными:

способностью выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения (ПК-1);

способностью применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2);

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

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

способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК-5);

способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ПК-6);

способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности (ПК-7);

способностью работать с программными средствами прикладного, системного и специального назначения (ПК-8);

способностью использовать языки и системы программирования, инструментальные средства для решения различных профессиональных, исследовательских и прикладных задач (ПК-9);

способностью формулировать результат проведенных исследований в виде конкретных рекомендаций, выраженных в терминах предметной области изучавшегося явления (ПК-10);

способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах (ПК-11);

способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ПК-12);

способностью организовать антивирусную защиту информации при работе с компьютерными системами (ПК-13);

в научно-исследовательской деятельности:

способностью осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем (ПК-14);

способностью применять современные методы и средства исследований для обеспечения информационной безопасности компьютерных систем (ПК-15);

способностью проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности (ПК-16);

способностью готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-17);

способностью разрабатывать математические модели безопасности защищаемых компьютерных систем (ПК-18);

способностью проводить обоснование и выбор рационального решения по уровню защищенности компьютерной системы с учетом заданных требований (ПК-19);

способностью проводить анализ и формализацию поставленных задач в области компьютерной безопасности (ПК-20);

в проектной деятельности:

способностью проводить сбор и анализ исходных данных для проектирования систем защиты информации (ПК-21);

способностью участвовать в разработке проектной документации (ПК-22);

способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем (ПК-23);

способностью участвовать в разработке системы защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы (ПК-24);

способностью оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи (ПК-25);

в контрольно-аналитической деятельности:

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований к уровню защищенности компьютерной системы (ПК-26);

способностью к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей (ПК-27);

способностью обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения (ПК-28);

способностью оценивать эффективность систем защиты информации в компьютерных системах (ПК-29);

в организационно-управленческой деятельности:

способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-30);

способностью разрабатывать оперативные планы работы первичных подразделений (ПК-31);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы (ПК-32);

способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-33);

в эксплуатационной деятельности:

способностью производить установку, тестирование программного обеспечения и программно-аппаратных средств по обеспечению информационной безопасности

компьютерных систем (ПК-34);

способностью принимать участие в эксплуатации программного обеспечения и программно-аппаратных средств обеспечения информационной безопасности компьютерных систем (ПК-35);

способностью производить проверку технического состояния и профилактические осмотры оборудования по защите информации (ПК-36);

способностью выполнять работы по приему, настройке, регулировке, освоению и восстановлению работоспособности оборудования защиты информации (ПК-37);

способностью разрабатывать и составлять инструкции и руководства пользователей по эксплуатации средств обеспечения информационной безопасности компьютерных систем и аппаратно-программных средств защиты информации (ПК-38).

Специализация N 1 "Анализ безопасности компьютерных систем":

способностью исследовать, разрабатывать, реализовывать и применять математические модели и методы анализа и синтеза защищенных компьютерных систем (ПСК-1.1);

способностью применять системы и инструментальные среды проектирования и разработки программ (ПСК-1.2);

способностью осуществлять обоснованный выбор программно-аппаратных средств защиты информации в условиях конкретной компьютерной системы (ПСК-1.3);

способностью оценивать эффективность программных реализаций алгоритмов защиты информации (ПСК-1.4);

способностью проводить анализ защищенности и находить потенциальные уязвимости компьютерной системы (ПСК-1.5);

способностью вносить предложения и формировать комплекс мер по усилению защищенности компьютерных систем (ПСК-1.6);

способностью использовать современные критерии и стандарты для анализа безопасности компьютерных систем (ПСК-1.7).

Специализация N 2 "Математические методы защиты информации":

способностью ориентироваться в современных и перспективных математических методах защиты информации, оценивать возможность и эффективность их применения в конкретных задачах защиты информации (ПСК-2.1);

способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов (ПСК-2.2);

способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации (ПСК-2.3);

способностью моделировать алгоритмы в системах компьютерной математики, оценивать их работоспособность и эффективность (ПСК-2.4);

способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств защиты информации (ПСК-2.5);

способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации (ПСК-2.6);

способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации (ПСК-2.7).

Специализация N 3 "Безопасность распределенных компьютерных систем":

способностью организовать защиту информации в распределенных компьютерных системах (ПСК-3.1);

способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем (ПСК-3.2);

способностью проводить мониторинг и аудит информационной безопасности на объектах информатизации (ПСК-3.3);

способностью обеспечить эффективное применение информационно-технологических ресурсов распределенной компьютерной системы, с учетом требований информационной безопасности (ПСК-3.4);

способностью проводить контрольные проверки работоспособности и эффективности применяемых программных средств защиты информации в распределенных компьютерных системах (ПСК-3.5);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПСК-3.6);

способностью использовать современные среды и технологии разработки программного обеспечения в распределенных компьютерных системах (ПСК-3.7).

Специализация N 4 "Разработка защищенного программного обеспечения":

способностью использовать современные технологии программирования для разработки защищенного программного обеспечения (ПСК-4.1);

способностью проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей (ПСК-4.2);

способностью руководствоваться требованиями современных стандартов по безопасности компьютерных систем (ПСК-4.3);

способностью использовать современные технологии разработки программного обеспечения (ПСК-4.4);

способностью осуществлять внедрение и сопровождение разработанного программного обеспечения и новых образцов программно-аппаратных средств защиты в компьютерных системах (ПСК-4.5);

способностью оценивать эффективность новых образцов программных средств защиты в компьютерных системах (ПСК-4.6);

способностью разрабатывать техническую документацию на программное обеспечение в соответствии с действующими стандартами (ПСК-4.7).

Специализация N 5 "Безопасность высокопроизводительных вычислительных систем":

способностью эксплуатировать системы и инструментальные среды проектирования и разработки программ (ПСК-5.1);

способностью работать со средствами системного администрирования в высокопроизводительных системах (ПСК-5.2);

способностью использовать существующие и создавать новые инструментальные средства для решения различных профессиональных, исследовательских и прикладных задач высокопроизводительных вычислений (ПСК-5.3);

способностью участвовать в проведении анализа и моделировании систем безопасности, в испытаниях механизмов безопасности (ПСК-5.4);

способностью выявлять и анализировать атаки на высокопроизводительную систему высокой доступности (ПСК-5.5);

способностью применять методы настройки систем обнаружения вторжений в различных ситуациях (ПСК-5.6);

способностью использовать методы проектирования и средства обеспечения безопасности защищенных высокопроизводительных систем (ПСК-5.7).

Специализация N 6 "Безопасность программного обеспечения мобильных систем":

способностью разрабатывать программные средства обеспечения защиты мобильных устройств и устройств беспроводной связи (ПСК-6.1);

способностью реализовывать быстрые вычислительные алгоритмы средствами мобильных устройств (ПСК-6.2);

способностью принимать участие в исследованиях и анализе систем безопасности мобильных устройств и устройств беспроводной связи (ПСК-6.3);

способностью применять средства обеспечения и контроля информационной безопасности для мобильных систем (ПСК-6.4);

способностью разрабатывать прикладное и системное программное обеспечение для мобильных устройств с учётом требований по безопасности (ПСК-6.5);

способностью создавать программы, поддерживающие интерфейсы с мобильными устройствами (ПСК-6.6);

способностью обеспечивать взаимодействие прикладного программного обеспечения персональных компьютеров с мобильными устройствами (ПСК-6.7).

Специализация N 7 "Информационно-аналитическая и техническая экспертиза компьютерных систем":

способностью использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов (ПСК-7.1);

способностью проводить экспертизу вычислительной техники и носителей компьютерной информации (ПСК-7.2);

способностью руководствоваться в своей работе требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий (ПСК-7.3);

способностью правильно использовать в своей работе юридическую терминологию (ПСК-7.4);

способностью подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем (ПСК-7.5);

способностью разрабатывать программное обеспечение, предназначенное для выявления следов компьютерных преступлений и инцидентов (ПСК-7.6);

способностью анализировать существующие методы совершения компьютерных преступлений, правонарушений и инцидентов и прогнозировать их возможные пути развития (ПСК-7.7).

Специализация N 8 "Информационная безопасность объектов информатизации на базе компьютерных систем":

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности конкретных объектов информатизации на базе компьютерных систем в защищенном исполнении (ПСК-8.1);

способностью на основании моделей угроз и моделей нарушителя информационной безопасности формировать требования к обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении (ПСК-8.2);

способностью на основании требований к обеспечению информационной безопасности формировать перечень функций безопасности объекта информатизации на базе компьютерных систем в защищенном исполнении и выбирать рациональные способы и средства их реализации (ПСК-8.3);

способностью разрабатывать проектные решения по системам обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении (ПСК-8.4);

способностью проводить анализ систем обеспечения информационной

безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении на предмет их соответствия требованиям по обеспечению информационной безопасности (ПСК-8.5);

способностью обеспечить информационную безопасность процессов проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении (ПСК-8.6);

способностью разрабатывать проекты нормативных и правовых актов предприятия, учреждения, организации, регламентирующих деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении (ПСК-8.7).

VI. Требования к структуре основных образовательных программ подготовки специалиста

6.1. ООП подготовки специалиста предусматривает изучение следующих учебных циклов (таблица 2):

гуманитарный, социальный и экономический цикл;

математический и естественнонаучный цикл;

профессиональный цикл;

и разделов:

физическая культура;

учебная и производственная практики, научно-исследовательская работа;

итоговая государственная аттестация.

6.2. Каждый учебный цикл имеет базовую (обязательную) часть и вариативную, устанавливаемую вузом. Вариативная часть дает возможность расширения и (или) углубления знаний, умений и навыков, определяемых содержанием базовых (обязательных) дисциплин (модулей) и дисциплин специализаций, позволяет обучающемуся получить углубленные знания и навыки для успешной профессиональной деятельности и (или) для продолжения дальнейшего обучения по программам послевузовского профессионального образования (аспирантура, адъюнктура).

6.3. Базовая (обязательная) часть цикла "Гуманитарный, социальный и экономический цикл" должна предусматривать изучение следующих обязательных дисциплин: "История Отечества", "Философия", "Иностранный язык".

Базовая (обязательная) часть профессионального цикла должна предусматривать изучение всех дисциплин, указанных в структуре ООП подготовки специалиста.

Таблица 2

Структура ООП подготовки специалиста

Код УЦ ООП	Учебные циклы (разделы) и проектируемые результаты их освоения	Трудоемкость (Зачетные единицы)*	Перечень дисциплин для разработки программ (примерных), а так же учебников и учебных пособий	Коды формируемых компетенций

С.1	Гуманитарный, социальный и экономический цикл	32 - 39		
	Базовая часть В результате изучения базовой части цикла студент должен: знать: - содержание и взаимосвязь основных принципов, законов, понятий и категорий гуманитарных, социальных и экономических наук; - основные этапы развития философской мысли, основную проблематику и структуру философского знания; - основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; - лексический и грамматический минимум в объеме, необходимом для работы с текстами профессиональной направленности и осуществления коммуникации на иностранном языке; - основные экономические теории, категории и закономерности, методы анализа экономических явлений и процессов; - основы экономической и финансовой деятельности отрасли и ее структурных подразделений, методику оценки хозяйственной, деятельности (применительно к отрасли обеспечения информационной безопасности); - основы права и законодательства России, основы конституционного строя Российской Федерации, характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности	24 - 29**	Философия История Отечества Иностранный язык Экономика Правоведение Основы управленческой деятельности	ОК-1 ОК-2 ОК-3 ОК-4 ОК-5 ОК-6 ОК-7 ОК-8 ОК-9 ОК-10 ОК-11 ПК-4 ПК-5 ПК-14 ПК-22 ПК-30 ПК-31 ПК-33

	Российской Федерации; - научные основы, цели, принципы, методы и технологии управленческой деятельности; уметь: - использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач; - анализировать мировоззренческие, социально и личностно значимые философские проблемы; - анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности; - читать и переводить научно-техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи; - анализировать экономические показатели деятельности подразделения; - использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности; - уметь работать в коллективе, принимать управленческие решения и оценивать их эффективность; владеть: - основными методами научного познания; - иностранным языком в объеме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на			

	иностранном языке; - навыками письменного аргументированного изложения собственной точки зрения; - навыками публичной речи, аргументации, ведения дискуссии и полемики; - навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; - навыками выбора, обоснования, реализации и контроля результатов управленческого решения.			
	Вариативная часть (знания, умения, навыки определяются ООП вуза)	8 - 10		
С.2	Математический и естественнонаучный цикл	90 - 98		
	Базовая часть В результате изучения базовой части цикла студент должен: знать: - основные понятия и задачи векторной алгебры и аналитической геометрии; - основные свойства алгебраических структур; - основы линейной алгебры над произвольными полями; - основные положения теории пределов функций, теории рядов; - основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных; - понятие меры, измеримые функции и их свойства; - абстрактный интеграл Лебега и его основные свойства; - свойства кольца многочленов; - свойства векторных пространств; - основы теории групп и теории групп подстановок; - основные понятия и методы	74 - 78**	Математический анализ Геометрия Теория вероятностей и математическая статистика Алгебра Математическая логика и теория алгоритмов Дискретная математика Теория информации Физика Информатика	ОК-3 ОК-5 ОК-7 ОК-8 ОК-9 ОК-10 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10 ПК-11 ПК-12 ПК-16 ПК-17 ПК-18 ПК-19 ПК-20

	теории вероятностей, математической статистики и теории случайных процессов; - основные понятия математической логики и теории алгоритмов; - основные понятия и методы дискретной математики; - основные понятия и методы теории информации; - основные законы механики; - основные законы термодинамики и молекулярной физики; - основные законы электричества и магнетизма; - основы теории колебаний и волн, оптики; - основы квантовой физики и физики твёрдого тела; - физические явления и эффекты, используемые при обработке, хранении, передаче, уничтожении и защите информации; - основные понятия информатики; - формы и способы представления данных в персональном компьютере; - состав, назначение функциональных компонентов и программного обеспечения персонального компьютера; - классификацию современных компьютерных систем; - типовые структуры и принципы организации компьютерных сетей; уметь: - определять возможности применения методов математического анализа; - решать основные задачи векторной алгебры и аналитической геометрии; - решать основные задачи теории пределов функций, дифференцирования, интегрирования и разложения			

	функций в ряды; - использовать математический аппарат дискретной математики, в том числе применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач; - уметь находить представление и исследовать свойства булевых и многозначных функций формулами в различных базисах, - вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); - на основе законов механики описывать основные виды движения тел; - строить математические модели физических явлений и процессов; - решать типовые прикладные физические задачи; - применять стандартные методы и модели к решению теоретико-вероятностных и статистических задач; - использовать расчетные формулы, таблицы, графики, компьютерные программы при решении математических задач; - проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; - решать системы линейных уравнений над полями; - использовать математический аппарат дискретной математики; - вычислять теоретико-информационные характеристики источников сообщений и каналов связи			

	(энтропия, взаимная информации, пропускная способность); - строить математические модели физических явлений и процессов; - решать типовые прикладные физические задачи; - применять основные законы общей физики при решении практических задач; - применять персональные компьютеры для обработки различных видов информации; - применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, дефрагментации и очистки диска); - пользоваться сетевыми средствами и внешними носителями информации для обмена данными; владеть: - навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; - навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; - навыками пользования библиотеками прикладных программ и пакетами программ для решения прикладных математических задач; - навыками решения систем линейных уравнений над полем и кольцом вычетов; - навыками решения стандартных задач в векторных пространствах; - навыками использования языка математической логики; - навыками решения задач			

	дискретной математики; - основами построения математических моделей текстовой информации и моделей систем передачи информации; - методами теоретического исследования физических явлений и процессов; - навыками проведения физического эксперимента и обработки его результатов; - навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов); - навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией).			
	Вариативная часть (знания, умения, навыки определяются ООП вуза)	16 - 20		
С.3	Профессиональный цикл	145 - 155		
	Базовая часть В результате изучения базовой части цикла студент должен: знать: - общие принципы построения и использования современных языков программирования высокого уровня; - язык программирования высокого уровня (объектно-ориентированное программирование); - язык ассемблера персонального компьютера; - особенности взаимодействия языков высокого и низкого уровня, организации работы с памятью в скриптовых языках; - базовые структуры данных; - основные комбинаторные и теоретико-графовые алгоритмы,	117 - 123**	Языки программирования Методы программирования Аппаратные средства вычислительной техники Операционные системы Компьютерные сети Системы управления базами данных Основы	ОК-1 ОК-2 ОК-5 ОК-6 ОК-7 ОК-8 ОК-9 ОК-10 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10 ПК-11 ПК-12 ПК-13

	а также способы их эффективной реализации и оценки сложности; - современные технологии программирования; - показатели качества программного обеспечения; архитектуру основных типов современных компьютерных систем; - структуру и принципы работы современных и перспективных микропроцессоров; - основы системного программирования; - принципы построения современных операционных систем и особенности их применения; - основы Интернет-технологий; - характеристики и типы систем баз данных; - физическую организацию баз данных и принципы (основы) их защиты; - средства и методы хранения и передачи аутентификационной информации; - требования к подсистеме аудита и политике аудита; - защитные механизмы и средства обеспечения безопасности операционных систем; - механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; - основные протоколы идентификации и аутентификации абонентов сети; - защитные механизмы и средства обеспечения сетевой безопасности; - средства и методы предотвращения и обнаружения вторжений; - основные средства и методы анализа программных		информационной безопасности Модели безопасности компьютерных систем Организационное и правовое обеспечение информационной безопасности Защита в операционных системах Основы построения защищенных компьютерных сетей Основы построения защищенных баз данных Защита программ и данных Электроника и схемотехника Сети и системы передачи информации Техническая защита информации Криптографические методы защиты информации Криптографические протоколы Теоретико-числовые методы в криптографии	ПК-14 ПК-15 ПК-16 ПК-17 ПК-18 ПК-19 ПК-20 ПК-21 ПК-22 ПК-23 ПК-24 ПК-25 ПК-26 ПК-27 ПК-28 ПК-29 ПК-30 ПК-31 ПК-32 ПК-33 ПК-34 ПК-35 ПК-36 ПК-37 ПК-38

	реализаций; - сущность и понятие информации, информационной безопасности и характеристику ее составляющих; - место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; - источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; - основные виды политик управления доступом и информационными потоками в компьютерных системах; - основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; - основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;		Безопасность жизнедеятельности	

	- организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; - основы теории электрических цепей; - принципы работы элементов и функциональных узлов электронной аппаратуры; - методы анализа и синтеза электронных схем; - типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; - эталонную модель взаимодействия открытых систем; - современные виды информационного взаимодействия и обслуживания; - общие принципы проектирования современных систем и сетей телекоммуникаций, включая мультисервисные сети связи; - технические каналы утечки информации; - возможности технических средств перехвата информации; - способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - организацию защиты информации от утечки по техническим каналам на объектах информатизации; - основы физической защиты объектов информатизации;			

	- основные виды симметричных и асимметричных криптографических алгоритмов; - математические модели шифров; - криптографические стандарты; - типовые криптографические протоколы и основные требования к ним; - алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; уметь: - формализовать поставленную задачу; - работать с интегрированными средами разработки программного обеспечения; - разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями; - разрабатывать и сопровождать программные средства с учетом требований к их защищенности; - проводить оценку сложности алгоритмов; - разрабатывать эффективные алгоритмы и программы; - планировать разработку сложного программного обеспечения; - оценивать качество готового программного обеспечения; - организовывать удаленный доступ к базам данных; - осуществлять нормализацию отношений при проектировании реляционной базы данных; - применять нормативные правовые акты и нормативные методические документы в			

	области обеспечения информационной безопасности; - разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; - формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; - применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - использовать средства защиты, предоставляемые системами управления базами данных; - разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; - разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы; - применять действующую законодательную базу в области обеспечения компьютерной безопасности; - применять на практике методы			

	анализа электрических цепей; - работать с современной элементной базой электронной аппаратуры; - проводить анализ показателей качества сетей и систем связи; - читать структурные и функциональные схемы систем и сетей связи; - пользоваться нормативными документами по противодействию технической разведке; - анализировать и оценивать угрозы информационной безопасности объекта; - корректно применять симметричные и асимметричные криптографические алгоритмы; - формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям; - определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; владеть: - профессиональной терминологией в области информационной безопасности; - навыками разработки, документирования, тестирования и отладки программ; - навыками использования инструментальных средств отладки и дизассемблирования программного кода; - навыками системного программирования; - навыками разработки алгоритмов решения типовых профессиональных задач; - навыками документирования			

	программного обеспечения; - навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; - навыками конфигурирования и администрирования операционных систем; - навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; - навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; - навыками настройки межсетевых экранов; - методиками анализа сетевого трафика; - методиками анализа результатов работы средств обнаружения вторжений; - методикой составления запросов для поиска информации в базах данных; - навыками анализа программных реализаций; - профессиональной терминологией в области информационной безопасности; - методами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах; - навыками работы с нормативными правовыми актами; - навыками организации и обеспечения режима секретности;			

	- методами организации и управления деятельностью служб защиты информации на предприятии; - методами формирования требований по защите информации; - методиками использования средств защиты, предоставляемых системами управления базами данных; - навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры; - навыками работы с программными средствами схемотехнического моделирования; - навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений; - методами и средствами технической защиты информации; - методами расчета и инструментального контроля показателей технической защиты информации; - криптографической терминологией; - простейшими подходами к анализу безопасности криптографических протоколов; - навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.			
	1. Специализация "Анализ безопасности компьютерных систем". С целью получения данной специализации при изучении базовой части цикла обучающийся должен: знать: - основные алгоритмы кодирования и сжатия	15 - 19	Методы и стандарты оценки защищенности компьютерных систем Алгоритмы кодирования и сжатия информации	ПСК-1.1 ПСК-1.2 ПСК-1.3 ПСК-1.4 ПСК-1.5 ПСК-1.6

	информации; - основные стандарты оценивания защищенности компьютерных систем; уметь: - анализировать компьютерную систему с целью определения уровня защищенности и доверия; - исследовать систему защиты компьютерной сети с целью обнаружения уязвимостей; владеть: - методами анализа программного обеспечения; - основными методами верификации программ.		Методы верификации Анализ уязвимостей программного обеспечения	
	2. Специализация "Математические методы защиты информации". С целью получения данной специализации при изучении базовой части цикла обучающийся должен: знать: - принципы и методы построения быстрых алгоритмов для реализации систем защиты информации; - основные алгоритмы кодирования, сжатия и восстановления различных видов информации; - принципы построения псевдослучайных генераторов и их свойства; - принципы применения эллиптических и гиперэллиптических кривых в криптографии; уметь: - проводить предварительное оценивание временной сложности разрабатываемых алгоритмов; - разрабатывать быстрые вычислительные алгоритмы для криптографических приложений; владеть: - навыками программирования	15 - 19	Теория кодирования, сжатия и восстановления информации Теория псевдослучайных генераторов Методы алгебраической геометрии в криптографии	ПСК-2.1 ПСК-2.2 ПСК-2.3 ПСК-2.4 ПСК-2.5 ПСК-2.6 ПСК-2.7

	алгебраических операций в конечных алгебраических структурах, в том числе в группе точек эллиптических и гиперэллиптических кривых; - навыками использования систем компьютерной математики для решения профессиональных задач; - методами построения быстрых вычислительных алгоритмов алгебры и теории чисел.			
	3. Специализация "Безопасность распределенных компьютерных систем". С целью получения данной специализации при изучении базовой части цикла обучающийся должен: знать: - основные принципы построения защищенных распределенных компьютерных систем; - основные принципы построения систем обнаружения компьютерных атак; - способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; уметь: - формализовать задачу управления безопасностью информационных систем; - анализировать защищенность систем; - администрировать системы обнаружения компьютерных атак; владеть: - навыками выявления и устранения уязвимостей компьютерной сети; - навыками организации защищенного удаленного доступа к информационным ресурсам; - способами настройки стандартных систем	15 - 19	Теория управления информационной безопасностью распределенных компьютерных систем Системы обнаружения компьютерных атак Методы анализа рисков	ПСК-3.1 ПСК-3.2 ПСК-3.3 ПСК-3.4 ПСК-3.5 ПСК-3.6 ПСК-3.7

	обнаружения компьютерных атак; - навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем.			
	4. Специализация "Разработка защищенного программного обеспечения". С целью получения данной специализации при изучении базовой части цикла обучающийся должен: знать: - основные подходы к разработке защищенного программного обеспечения; - основные принципы отладки программ; - основные виды уязвимости программного кода; - основные типы вредоносных программ и способы их внедрения; уметь: - применять инструментальные средства отладки и дизассемблирования программного кода; владеть: - навыками анализа исходного и исполняемого кода программы для выявления основных уязвимостей.	15 - 19	Анализ программных реализаций Уязвимости программного обеспечения Теория передачи сигналов и сообщений	ПСК-4.1 ПСК-4.2 ПСК-4.3 ПСК-4.4 ПСК-4.5 ПСК-4.6 ПСК-4.7
	5. Специализация "Безопасность высокопроизводительных вычислительных систем". С целью получения данной специализации при изучении базовой части цикла обучающийся должен: знать: - алгоритмы синхронизации; - принципы распределения транзакций; - принципы разработки архитектуры высокопроизводительных систем: прозрачность,	15-19	Обнаружение вторжений и мониторинг функционирования высокопроизводительных систем Разработка прикладного программного обеспечения для высокопроизводительных систем Принципы построения и	ПСК-5.1 ПСК-5.2 ПСК-5.3 ПСК-5.4 ПСК-5.5 ПСК-5.6 ПСК-5.7

	открытость, масштабируемость; - гомогенные и гетерогенные мультикомпьютерные системы; - распределенные сетевые операционные системы; - распределенные файловые системы; - основные принципы построения систем обнаружения вторжений и мониторинга; - принципы распараллеливания алгоритмов; - технологии программирования для параллельных и масштабируемых платформ; уметь: - разрабатывать профили защиты и задания по безопасности; - проектировать архитектуру защищенных систем; - анализировать и оценивать безопасность защищенных информационных систем; - выявлять атаки, описывать природу атаки, ее признаки и методы обнаружения, распознавать атаки отказа в обслуживании; - создавать параллельные программы и разрабатывать прикладное программное обеспечение для высокопроизводительных систем; владеть: - методиками работы с высокопроизводительными системами; - методами построения и анализа архитектуры высокопроизводительных систем; - способами создания сигнатур обнаруженных атак; - способами настройки стандартных систем обнаружения вторжений; - навыками администрирования средств контроля доступа к		архитектура высокопроизводительных вычислительных систем	

	ресурсам высокопроизводительных систем; - технологиями создания прикладного программного обеспечения для высокопроизводительных систем.			
	6. Специализация "Безопасность программного обеспечения мобильных систем". С целью получения данной специализации при изучении базовой части цикла обучающийся должен: знать: - быстрые алгебраические и теоретико-числовые алгоритмы; - языки высокоуровневого программирования для мобильных систем; - архитектуры современных мобильных операционных систем; протоколы сетевого взаимодействия; - штатные механизмы безопасности мобильных операционных систем; - методы обеспечения сетевой безопасности; - принципы построения программного обеспечения для мобильных устройств; - архитектуры и интерфейсы прикладного программирования операционных систем мобильных устройств; - языки программирования, применяемые в мобильных системах; уметь: - реализовывать быстрые алгоритмы средствами мобильных операционных систем; - применять системы разработки программных продуктов для мобильных систем; - управлять параметрами	15 - 19	Безопасность системного программного обеспечения мобильных устройств Технология программирования мобильных устройств Мобильные операционные системы	ПСК-6.1 ПСК-6.2 ПСК-6.3 ПСК-6.4 ПСК-6.5 ПСК-6.6 ПСК-6.7

	мобильных устройств и конфигураций сетевых интерфейсов; - разрабатывать системное программное обеспечение для мобильных систем; - оценивать защищенность мобильных систем обеспечения для мобильных устройств на предмет противостояния угрозам безопасности; - разрабатывать системное и прикладное программное обеспечение мобильных устройств; - создавать приложения для компьютерных сетей, взаимодействующих с мобильными устройствами; владеть: - методами встраивания средств криптографической защиты информации в мобильные системы; - навыками администрирования безопасности на уровне операционных систем; - средствами разработки программного обеспечения для мобильных устройств; - средствами и методами контроля безопасности мобильных устройств; - технологиями создания безопасного программного обеспечения мобильных устройств.			
	7. Специализация "Информационно-аналитическая и техническая экспертиза компьютерных систем". С целью получения данной специализации при изучении базовой части цикла обучающийся должен: знать: - методы проведения расследования компьютерных преступлений, правонарушений и инцидентов;	15 - 19	Методы расследования компьютерных преступлений Инструментальные средства проведения расследования компьютерных инцидентов Экспертиза	ПСК-7.1 ПСК-7.2 ПСК-7.3 ПСК-7.4 ПСК-7.5 ПСК-7.6 ПСК-7.7

	- правовые и нормативные акты, регулирующие порядок проведения расследования; - основные методы и особенности поведения криминалистического анализа; уметь: - применять современные инструментальные средства проведения экспертизы; - применять нормативные и правовые актов при проведении криминалистической экспертизы и криминалистического анализа; - прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов; владеть: - навыками обнаружения и фиксации следов компьютерных преступлений, правонарушений и инцидентов; - навыками организации и проведения информационно-аналитических и технических экспертиз.		носителей компьютерной информации	
	8. Специализация "Информационная безопасность объектов информатизации на базе компьютерных систем". С целью получения данной специализации при изучении базовой части цикла обучающийся должен: знать: - методы определения и построения моделей угроз информационной безопасности объектов информатизации; - существующие подходы и методы построения моделей нарушителей информационной безопасности; - порядок и методы организации и осуществления работ и мероприятий по обеспечению информационной безопасности объектов информатизации на базе защищенном исполнении;	15 - 19	Обеспечение информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении Объекты защиты информации Проектирование и анализ систем обеспечения информационной безопасности объектов информатизации	ПСК-8.1 ПСК-8.2 ПСК-8.3 ПСК-8.4 ПСК-8.5 ПСК-8.6 ПСК-8.7

	- способы и методы анализа систем обеспечения информационной безопасности объектов информатизации; уметь: - проводить обследование объектов информатизации на базе компьютерных систем в защищенном исполнении; - разрабатывать модели угроз и нарушителей информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении; - формировать требования к обеспечению информационной безопасности и перечень функций безопасности; - выбирать рациональные способы и средства реализации функций безопасности объекта информатизации на базе компьютерных систем в защищенном исполнении; - проводить анализ проектных решений на предмет их соответствия требованиям по обеспечению информационной безопасности; - организовать работы по реализации процессов проектирования, создания, эксплуатации объектов информатизации на базе компьютерных систем в защищенном исполнении, обеспечивать информационную безопасность этих процессов; - разрабатывать проекты документов по обеспечению информационной безопасности объектов информатизации; владеть: - навыками организации и проведения обследования объектов информатизации и условий их размещения; - навыками и средствами проектирования систем			

	обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении.			
	Вариативная часть (знания, умения, навыки определяются ООП вуза)	28 - 32		
С.4	Физическая культура	2		ОК-11 ОК-12
С.5	Учебная и производственная практики, научно-исследовательская работа (практические умения и навыки определяются ООП вуза)	18 - 21		ОК-1 - ОК-11 ПК-5 ПК-7 ПК-8 ПК-9 ПК-10 ПК-11 ПК-14 ПК-15 ПК-16 ПК-17 ПК-18 ПК-19 ПК-20 ПК-21 ПК-23 ПК-24 ПК-25 ПК-26 ПК-27 ПК-28 ПК-29 ПК-33 ПСК-1.1 - ПСК-8.7
С.6	Итоговая государственная аттестация	21 - 24		ОК-3 ОК-5 ОК-7 ОК-8 ОК-9 ОК-10 ПК-1 ПК-2 ПК-3 ПК-4 ПК-11 ПК-12 ПК-14 ПК-15

				ПК-16 ПК-17 ПК-18 ПК-19 ПК-20 ПК-21 ПК-22 ПК-23 ПК-24 ПК-25 ПК-29 ПК-32 ПК-33 ПСК-1.1 - ПСК-8.7
	Общая трудоемкость основной образовательной программы	330		

---

* Трудоемкость циклов С.1, С.2, С.3 и разделов С.4, С.5 включает все виды текущей и промежуточной аттестаций.

** Суммарная трудоемкость базовых составляющих циклов С.1, С.2 и С.3 должна составлять не менее 75 процентов от общей трудоемкости указанных циклов.

Для вузов федеральных органов исполнительной власти, в которых предусмотрена военная служба и (или) служба в правоохранительных органах, нормативный срок освоения ООП может быть уменьшен за счет сокращения продолжительности каникулярного времени обучающихся в учебном году до 45 суток, переноса части аудиторных занятий по физической культуре на часы проведения утренней зарядки и часы спортивно-массовой работы, сокращения времени, выделяемого на проведение практик путем выполнения аналогичных задач в ходе полетов, вождения боевых машин, учений, несения учебно-боевого и других дежурств, внутренней, гарнизонной, караульной и других служб и практик при условии сохранения общей трудоемкости ООП, определенной данным стандартом.

VII. Требования к условиям реализации основных образовательных программ подготовки специалиста

7.1. Образовательные учреждения самостоятельно разрабатывают и утверждают ООП подготовки специалиста, которая включает в себя учебный план, рабочие программы учебных курсов, предметов, дисциплин (модулей) и другие материалы, обеспечивающие воспитание и качество подготовки обучающихся, а также программы учебной и производственной практик, календарный учебный график и методические материалы, обеспечивающие реализацию соответствующей образовательной технологии.

Специализация ООП подготовки специалиста определяется высшим учебным заведением в соответствии с ФГОС ВПО и примерной ООП подготовки специалиста.

Требования к результатам освоения и структуре ООП подготовки специалистов в части специализаций для вузов, в которых предусмотрена военная служба и (или)

служба в правоохранительных органах, определяются вузами по согласованию с федеральными органами исполнительной власти, в ведении которых находятся данные образовательные учреждения.

Реализация ООП по специальности 090301 Компьютерная безопасность допускается только при наличии у вуза лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну.

В случае, если ООП связана с освоением учебного материала, содержащего сведения, составляющие государственную тайну, то условия ее реализации должны соответствовать следующим требованиям:

наличие у лиц, участвующих в реализации образовательного процесса, содержащего сведения, составляющие государственную тайну, оформленного в установленном порядке допуска к государственной тайне по соответствующей форме;

наличие в образовательном учреждении нормативных правовых документов по обеспечению режима секретности и их выполнение;

осуществление образовательного процесса, содержащего сведения, составляющие государственную тайну, только в помещениях образовательного учреждения либо организаций, на базе которых реализуется образовательный процесс, удовлетворяющих требованиям нормативных правовых документов по режиму секретности, противодействию техническим разведкам и технической защите информации;

использование при реализации образовательного процесса, содержащего сведения, составляющие государственную тайну, средств вычислительной техники и программного обеспечения, удовлетворяющих требованиям нормативных правовых документов по режиму секретности, противодействию техническим разведкам и технической защите информации.

Высшие учебные заведения обязаны ежегодно обновлять ООП подготовки специалиста с учетом развития науки, техники, культуры, экономики, технологий и социальной сферы.

7.2. При разработке ООП подготовки специалиста должны быть определены возможности вуза в формировании общекультурных компетенций выпускников (компетенций социального взаимодействия, самоорганизации и самоуправления, системно-деятельностного характера). Вуз обязан сформировать социокультурную среду, создать условия, необходимые для всестороннего развития личности.

Вуз обязан способствовать развитию социально-воспитательного компонента учебного процесса, включая развитие студенческого самоуправления, участие обучающихся в работе общественных организаций, спортивных и творческих клубов, научных студенческих обществ.

7.3. Реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбор конкретных ситуаций, психологические и иные тренинги) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся. В рамках учебных курсов, связанных с проблемами обеспечения информационной безопасности, должны быть предусмотрены встречи с представителями органов государственной власти и управления, российских компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ООП подготовки специалиста, особенностью контингента обучающихся и содержанием конкретных дисциплин. В целом в учебном процессе они должны составлять не менее 25 процентов аудиторных занятий, в том числе специальных

профессиональных деловых игр (комплексных учений) в объеме не менее одной недели. Занятия лекционного типа для соответствующих групп обучающихся не могут составлять более 55 процентов аудиторных занятий.

7.4. В учебной программе каждой дисциплины (модуля) должны быть четко сформулированы конечные результаты обучения в органичной увязке с осваиваемыми знаниями, умениями и приобретаемыми компетенциями в целом по ООП подготовки специалиста.

Общая трудоемкость дисциплины не может быть менее двух зачетных единиц (за исключением дисциплин по выбору обучающихся и факультативных дисциплин). По дисциплинам, трудоемкость которых составляет более трех зачетных единиц, должна выставляться оценка ("отлично", "хорошо", "удовлетворительно", "неудовлетворительно").

7.5. ООП подготовки специалиста должна содержать дисциплины по выбору обучающихся в объеме не менее одной трети вариативной части суммарно по циклам С.1, С.2 и С.3. Порядок формирования дисциплин по выбору обучающихся устанавливает ученый совет вуза.

7.6. Максимальный объем учебной нагрузки обучающихся не может составлять более 54 академических часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы по освоению ООП и факультативных дисциплин, устанавливаемых вузом дополнительно к ООП подготовки специалиста и необязательными для изучения обучающимися.

Объем факультативных дисциплин не должен превышать 13 зачетных единиц за весь период обучения.

7.7. Объем аудиторных учебных занятий в неделю при освоении ООП в очной форме обучения составляет не менее 27 и не более 36 академических часов. В указанный объем не входят обязательные аудиторные занятия по физической культуре.

7.8. В случае реализации ООП подготовки специалиста в иных формах обучения максимальный объем аудиторных занятий устанавливается в соответствии с Типовым положением об образовательном учреждении высшего профессионального образования (высшем учебном заведении), утвержденным постановлением Правительства Российской Федерации от 14 февраля 2008 г. N 71 (Собрание законодательства Российской Федерации, 2008, N 8, ст. 731).

7.9. Общий объем каникулярного времени в учебном году должен составлять 7-10 недель, в том числе не менее двух недель в зимний период.

В высших учебных заведениях, в которых предусмотрена военная служба и (или) служба в правоохранительных органах, продолжительность каникулярного времени обучающихся определяется в соответствии с нормативными правовыми актами, регламентирующими порядок прохождения службы**.

7.10. Раздел "Физическая культура" ("Физическая подготовка" - для вузов, в которых предусмотрена военная служба и (или) служба в правоохранительных органах) трудоемкостью две зачетные единицы реализуется: при очной форме обучения, как правило, в объеме 400 часов, при этом объем практической, в том числе игровых видов, подготовки должен составлять не менее 360 часов.

7.11. Вуз обязан обеспечить обучающимся реальную возможность участвовать в формировании своей программы обучения, включая возможную разработку индивидуальных образовательных программ.

7.12. Вуз обязан ознакомить обучающихся с их правами и обязанностями при формировании ООП подготовки специалиста, разъяснить, что избранные обучающимися дисциплины (модули) становятся для них обязательными.

7.13. ООП подготовки специалиста вуза должна включать лабораторные практикумы и практические занятия по дисциплинам (модулям) базовой части циклов С.2 и С.3, формирующим у обучающихся умения и навыки в области физики, информатики, электроники и схемотехники, аппаратных средств вычислительной техники, сетей и систем передачи информации, технической защиты информации, защиты в операционных системах, основ построения защищенных баз данных и компьютерных сетей, защиты программ и данных, а также по дисциплинам специализации и вариативной части, рабочие программы которых предусматривают цели формирования у обучающихся соответствующих умений и навыков.

7.14. Наряду с установленными законодательными и другими нормативными правовыми актами, правами и обязанностями обучающиеся имеют следующие права и обязанности:

обучающиеся имеют право в пределах объема учебного времени, отведенного на освоение дисциплин (модулей) по выбору, предусмотренных ООП подготовки специалиста, выбирать конкретные дисциплины (модули);

при формировании своей индивидуальной образовательной программы обучающиеся имеют право получить консультацию в вузе по выбору дисциплин (модулей) и их влиянию на будущую специализацию ООП подготовки специалиста;

обучающиеся при переводе из другого высшего учебного заведения при наличии соответствующих документов имеют право на перезачет освоенных ранее дисциплин (модулей) на основании аттестации;

обучающиеся обязаны выполнять в установленные сроки все задания, предусмотренные ООП подготовки специалиста.

7.15. Раздел ООП подготовки специалиста "Учебная и производственная практики, научно-исследовательская работа" является обязательным и представляет собой форму организации учебного процесса, непосредственно ориентированных на профессионально-практическую подготовку обучающихся.

Конкретные виды практик определяются ООП вуза. Цели и задачи, программы и формы отчетности определяются вузом по каждому виду практики.

Практики проводятся в сторонних организациях, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данной специальности (специализации) или на кафедрах и в лабораториях вуза (учебная практика), обладающих необходимым кадровым и научно-техническим потенциалом.

В высших учебных заведениях, в которых предусмотрена военная служба и (или) служба в правоохранительных органах за счет времени, выделяемого на практики, могут проводиться специальные профессиональные деловые игры (комплексные учения).

Аттестация по итогам практики проводится на основании оформленного в соответствии с установленными требованиями письменного отчета и отзыва руководителя практики от организации. По итогам аттестации выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно).

7.16. Научно-исследовательская работа является обязательным разделом основной образовательной программы подготовки специалиста. Она направлена на комплексное формирование общекультурных, профессиональных и профессионально-специализированных компетенций в соответствии с требованиями ФГОС ВПО.

При разработке программы научно-исследовательской работы высшее учебное заведение должно предоставить возможность обучающимся:

изучать специальную литературу и другую научно-техническую информацию о достижениях отечественной и зарубежной науки и техники в соответствующей области

знаний;

участвовать в проведении научных исследований или выполнении технических разработок;

осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме (заданию);

принимать участие в стендовых и промышленных испытаниях опытных образцов (партий) проектируемых изделий;

составлять отчеты (разделы отчета) по теме или ее разделу (этапу, заданию), готовить рефераты;

выступить с докладом на конференции, научном семинаре.

В процессе выполнения научно-исследовательской работы и оценки ее результатов должно проводиться широкое обсуждение в учебных структурах вуза с привлечением работодателей, позволяющее оценить уровень компетенций, сформированных у обучающихся. Необходимо также дать оценку компетенций, связанных с формированием профессионального мировоззрения и определения уровня культуры.

7.17. Реализация ООП подготовки специалиста должна обеспечиваться научно-педагогическими кадрами, имеющими, как правило, базовое образование, соответствующее профилю преподаваемой дисциплины, и систематически занимающимися научной и (или) научно-методической деятельностью.

Доля преподавателей, имеющих ученую степень и (или) ученое звание, в общем числе преподавателей, обеспечивающих образовательный процесс по данной ООП, должна быть не менее 65 процентов, ученую степень доктора наук (в том числе степень, присваиваемую за рубежом, документы о присвоении которой прошли установленную процедуру признания и установления эквивалентности) и (или) ученое звание профессора должны иметь не менее 9 процентов преподавателей.

Преподаватели профессионального цикла должны иметь базовое образование и (или) ученую степень, соответствующие профилю преподаваемой дисциплины, или опыт деятельности в сфере обеспечения информационной безопасности.

Не менее 70 процентов преподавателей (в приведенных к целочисленным значениям ставок), обеспечивающих учебный процесс по профессиональному циклу, должны иметь ученые степени или ученые звания, при этом ученые степени доктора наук или ученое звание профессора должны иметь не менее 11 процентов преподавателей.

К образовательному процессу должно быть привлечено не менее пяти процентов преподавателей из числа действующих руководителей и работников профильных организаций, предприятий и учреждений.

До 10 процентов от общего числа преподавателей, имеющих ученую степень и (или) ученое звание может быть заменено преподавателями, имеющими стаж практической работы по данному направлению на должностях руководителей или ведущих специалистов не менее 5 последних лет.

В вузах, в которых предусмотрена военная служба и (или) служба в правоохранительных органах к преподавателям с учеными степенями и (или) учеными званиями приравниваются преподаватели военно-(специальных) профессиональных дисциплин, не имеющие ученых степеней и ученых званий, имеющие профильное высшее образование, опыт работы в войсках (на флотах), штабах, правоохранительных органах, учреждениях не менее 10 лет, воинское звание не ниже "подполковник", а также или боевой опыт, или государственные награды, или государственные (отраслевые) почетные звания, или государственные премии. В числе преподавателей с ученой степенью доктора наук и (или) ученым званием профессора

могут учитываться преподаватели военно-(специальных) профессиональных учебных дисциплин с ученой степенью кандидата наук, имеющие или государственные награды, или государственные (отраслевые) почетные звания, или государственные премии.

В структуре вуза, реализующего данную ООП подготовки специалиста, должна быть отдельная выпускающая кафедра по специальности "Компьютерная безопасность".

Общее руководство содержанием теоретической и практической подготовки по специализации должно осуществляться штатным научно-педагогическим работником вуза, имеющим ученую степень доктора или кандидата наук и (или) ученое звание профессора или доцента, стаж работы в образовательных учреждениях высшего профессионального образования не менее трех лет. К общему руководству содержанием теоретической и практической подготовки по специализации может быть привлечен высококвалифицированный специалист в соответствующей сфере профессиональной деятельности.

7.18. ООП подготовки специалиста должна обеспечиваться учебно-методической документацией и материалами по всем учебным курсам, дисциплинам (модулям) ООП. Содержание каждой из таких учебных дисциплин (модулей) должно быть представлено в сети Интернет или локальной сети образовательного учреждения с выполнением установленных требований по защите информации.

Внеаудиторная работа обучающихся должна сопровождаться методическим обеспечением и обоснованием времени, затрачиваемого на ее выполнение.

Каждый обучающийся должен быть обеспечен доступом к электронно-библиотечной системе, содержащей издания по основным изучаемым дисциплинам и сформированной на основании прямых договоров с правообладателями учебной и учебно-методической литературы.

При этом должна быть обеспечена возможность осуществления одновременного индивидуального доступа к такой системе не менее чем для 25 процентов обучающихся.

Библиотечный фонд должен быть укомплектован печатными и (или) электронными изданиями основной учебной литературы по дисциплинам базовой части всех циклов, изданными за последние 10 лет (для дисциплин базовой части гуманитарного, социального и экономического цикла - за последние пять лет), из расчета не менее 25 экземпляров таких изданий на каждые 100 обучающихся.

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

Электронно-библиотечная система должна обеспечивать возможность индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет с выполнением установленных требований по защите информации.

Оперативный обмен информацией с отечественными и зарубежными вузами и организациями должен осуществляться с соблюдением требований законодательства Российской Федерации об интеллектуальной собственности и защиты сведений, составляющих государственную тайну, а также международных договоров Российской Федерации в области интеллектуальной собственности. Для обучающихся должен быть обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам в том числе, по тематике информационной безопасности.

Каждому обучающемуся должен быть обеспечен доступ к комплектам библиотечного фонда, состоящего не менее чем из пяти наименований отечественных и не менее четырех наименований зарубежных журналов.

7.19. Ученый совет высшего учебного заведения при введении ООП подготовки специалиста утверждает размер средств на реализацию соответствующих ООП.

Финансирование реализации ООП подготовки специалиста должно осуществляться в объеме не ниже установленных нормативов финансирования высшего учебного заведения***.

7.20. Высшее учебное заведение, реализующее ООП подготовки специалистов, должно располагать материально-технической базой, включая приборы, оборудование и программно-аппаратные средства специального назначения, обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, практической и научно-исследовательской работы обучающихся, предусмотренных учебным планом вуза и соответствующей действующим санитарным и противопожарным правилам и нормам.

Минимально необходимый для реализации ООП подготовки специалистов перечень материально-технического обеспечения включает в себя:

лаборатории в области:

- физики;
- электроники и схемотехники;
- сетей и систем передачи информации;
- технической защиты информации;
- программно-аппаратных средств обеспечения информационной безопасности.

Лаборатории высшего учебного заведения должны быть оснащены современным оборудованием, стендами, приборами, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой ООП.

Специально оборудованные кабинеты и аудитории в области:

- иностранного языка;
- информатики;

Интернет-технологий;

- сетевых компьютерных технологий;
- аппаратных средств вычислительной техники.

Лаборатории и специально оборудованные кабинеты и аудитории должны быть предусмотрены также для реализации дисциплин (модулей) специализации и вариативной части, рабочие программы которых предусматривают цели формирования у обучающихся соответствующих умений и навыков.

Компьютерные классы должны быть оборудованы современной вычислительной техникой для занятий по дисциплинам из расчета одно рабочее место на одного обучаемого при проведении занятий в данных классах.

При использовании электронных изданий и проведении самостоятельной подготовки вуз должен обеспечить обучающихся возможностью выхода в сеть Интернет из расчета не менее одного рабочего места на 10 обучающихся по данной ООП.

Вуз должен быть обеспечен необходимым комплектом лицензионного программного обеспечения и сертифицированными программными и аппаратными средствами защиты информации.

VIII. Требования к оценке качества освоения основных образовательных программ подготовки специалиста

8.1. Высшее учебное заведение обязано обеспечивать гарантию качества подготовки, в том числе путем:

разработки стратегии по обеспечению качества подготовки выпускников с привлечением представителей работодателей;

мониторинга, периодического рецензирования образовательных программ;

разработки объективных процедур оценки уровня знаний и умений обучающихся, компетенций выпускников;

обеспечения компетентности преподавательского состава;

регулярного проведения самообследования по согласованным критериям для оценки деятельности (стратегии) и сопоставления с другими образовательными учреждениями с привлечением представителей работодателей;

информирования общественности о результатах своей деятельности, планах, инновациях.

8.2. Оценка качества освоения ООП подготовки специалиста должна включать текущий контроль успеваемости, промежуточную аттестацию обучающихся и итоговую государственную аттестацию выпускников.

8.3. Конкретные формы и процедуры текущего и промежуточного контроля знаний по каждой дисциплине разрабатываются вузом самостоятельно и доводятся до сведения обучающихся в течение первого месяца от начала обучения по конкретной дисциплине.

8.4. Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей ООП подготовки специалиста (текущий контроль успеваемости и промежуточная аттестация) создаются фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы контроля, позволяющие оценить знания, умения и уровень сформированности компетенций. Фонды оценочных средств разрабатываются и утверждаются вузом.

Фонды оценочных средств должны быть полными и адекватными отображениями требований ФГОС ВПО по данному направлению подготовки (специальности), соответствовать целям и задачам конкретной ООП подготовки специалиста и её учебному плану. Они призваны обеспечивать оценку качества общекультурных, профессиональных и профессионально-специализированных компетенций, приобретаемых выпускником в соответствии с этими требованиями.

При разработке оценочных средств для контроля качества изучения модулей, дисциплин, практик должны учитываться все виды связей между включенными в них знаниями, умениями, навыками, позволяющие установить качество сформированных у обучающихся компетенций и степень общей готовности выпускников к профессиональной деятельности.

Вузом должны быть созданы условия для максимального приближения системы контроля качества освоения обучающимися ООП к условиям их будущей профессиональной деятельности. С этой целью, кроме преподавателей конкретной дисциплины, в качестве внешних экспертов должны активно привлекаться работодатели (представители заинтересованных организаций), преподаватели, читающие смежные дисциплины.

8.5. Обучающимся, должна быть предоставлена возможность оценивания содержания, организации и качества учебного процесса в целом, а также работы отдельных преподавателей.

8.6. Итоговая государственная аттестация направлена на установление соответствия уровня профессиональной подготовки выпускников требованиям ФГОС ВПО.

Итоговая государственная аттестация включает защиту выпускной квалификационной работы (дипломного проекта, дипломной работы). Государственный экзамен вводится по решению ученого совета вуза.

Требования к содержанию, объему и структуре выпускной квалификационной работы, а также требования к государственному экзамену (при наличии) определяются вузом.

---

* Одна зачетная единица соответствует 36 академическим часам.

** Статья 30 Положения о порядке прохождения военной службы, утвержденного Указом Президента Российской Федерации от 16 сентября 1999 г. N 1237 "Вопросы прохождения военной службы"(Собрание законодательства российской Федерации, 1999, N 38, ст. 4534)

*** Пункт 2 статьи 41 Закона Российской Федерации "Об образовании"от 10 июля 1992 г. N 3266-1 (Собрание законодательства Российской Федерации, 1996, N 3, ст. 150; 2002, N 26, ст. 2517; 2004, N 30, ст. 3086; N 35, ст. 3607; 2005, N 1, ст. 25; 2007, N 17, ст. 1932; N 44, ст. 5280)