Приложение

Утвержден
приказом Министерства образования
и науки Российской Федерации
от «17» января 2011 г. №60

ФЕДЕРАЛЬНЫЙ ГОСУДАРСТВЕННЫЙ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

по направлению подготовки (специальности)

090303 Информационная безопасность автоматизированных систем

(квалификация (степень) «специалист»)

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) **090303 Информационная безопасность автоматизированных систем** 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 лет	300**

*Одна зачетная единица соответствует 36 академическим часам.

**Трудоемкость ООП 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 обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере.

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

4.3. Специалист по направлению подготовки (специальности) **090303 Информационная безопасность автоматизированных систем** готовится к следующим видам профессиональной деятельности:

научно-исследовательская;

проектно-конструкторская;

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) **090303 Информационная безопасность автоматизированных систем,** наряду с квалификацией (степенью) «специалист» присваивается специальное звание «специалист по защите информации».

4.4. Специалист по направлению подготовки (специальности) **090303 Информационная безопасность автоматизированных систем** 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 информационной безопасности автоматизированных систем;

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

моделирование и исследование защищенных автоматизированных систем, анализ их уязвимостей и эффективности средств и способов защиты;

анализ безопасности информационных технологий, реализуемых в автоматизированных системах;

разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;

проектно-конструкторская деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации;

разработка политик информационной безопасности автоматизированных систем;

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

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

разработка системы управления информационной безопасностью автоматизированных систем;

контрольно-аналитическая:

контроль работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

экспериментально-исследовательские работы при сертификации средств защиты автоматизированных систем;

экспериментально-исследовательские работы при аттестации автоматизированных систем;

инструментальный мониторинг защищенности автоматизированных систем;

организационно-управленческая деятельность:

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

разработка предложений по совершенствованию и повышению эффективности принятых мер по обеспечению информационной безопасности автоматизированных систем;

организация работ по выполнению требований защиты информации ограниченного доступа;

методическое и организационное обеспечение информационной безопасности автоматизированных систем;

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

контроль реализации политики информационной безопасности;

эксплуатационная деятельность:

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

администрирование подсистем информационной безопасности автоматизированных систем;

мониторинг информационной безопасности автоматизированных систем;

управление информационной безопасностью автоматизированных систем;

обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций.

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 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 нестандартных ситуациях 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 логическому 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 профессиональной деятельности, развития социальных и профессиональных компетенций, к изменению вида своей профессиональной деятельности (ОК-10);

способностью к 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 использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);

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-4);

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

способностью использовать нормативные правовые акты в своей профессиональной деятельности (ПК- 6);

способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ПК- 7);

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

в научно - исследовательской деятельности:

способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

способностью применять современные методы исследования с использованием компьютерных технологий (ПК-10);

способностью разрабатывать и исследовать модели автоматизированных систем (ПК-11);

способностью проводить анализ защищенности автоматизированных систем (ПК-12);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);

способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-14);

способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-16);

в проектно-конструкторской деятельности:

способностью проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (ПК-17);

способностью участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18);

способностью участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19);

способностью разрабатывать политики информационной безопасности автоматизированных систем (ПК-20);

способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-21);

способностью участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы (ПК-22);

в контрольно-аналитической деятельности:

способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23);

способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем (ПК-24);

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации (ПК-25);

способностью проводить инструментальный мониторинг защищенности автоматизированных систем (ПК-26);

в организационно-управленческой деятельности:

способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-27);

способностью разрабатывать оперативные планы работы первичных подразделений (ПК-28);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-29);

способностью организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности (ПК-30);

способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-31);

способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите (ПК-32);

способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-33);

способностью формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы (ПК-34);

в эксплуатационной деятельности:

способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-35);

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы (ПК-36);

способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-37);

способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы (ПК-38);

способностью управлять информационной безопасностью автоматизированной системы (ПК-39);

способностью обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций (ПК-40).

Специализация № 1 «Автоматизированные информационные системы специального назначения».*

Специализация № 2 «Высокопроизводительные вычислительные системы специального назначения».*

---

* В соответствии с п. 7.1 настоящего стандарта требования к специализации определяются вузом.

Специализация № 3 «Информационная безопасность автоматизированных систем критически важных объектов»:

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

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

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

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

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

способностью восстанавливать работоспособность средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-3.6).

Специализация № 4 «Безопасность открытых информационных систем»:

способностью проводить анализ и исследовать модели защищенности открытых информационных систем (ПСК-4.1);

способностью участвовать в разработке компонентов открытых информационных систем (ПСК-4.2);

способностью обеспечить эффективное применение информационно-технологических ресурсов открытых информационных систем с учетом нормативных требований по защите информации (ПСК-4.3);

способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.4);

способностью участвовать в проектировании и эксплуатации системы управления информационной безопасностью открытой информационной системы (ПСК-4.5);

способностью проводить инструментальный мониторинг защищенности открытых информационных систем (ПСК-4.6);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью открытой информационной системы (ПСК-4.7);

способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.8).

Специализация № 5 «Информационная безопасность автоматизированных банковских систем»:

способностью проводить анализ и исследовать модели автоматизированных банковских систем (ПСК-5.1);

способностью на практике применять стандарты, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем (ПСК-5.2);

способностью на практике применять криптографические протоколы и стандарты при обеспечении информационной безопасности автоматизированных банковских систем (ПСК-5.3);

способностью проводить синтез и анализ проектных решений по обеспечению информационной безопасности автоматизированных банковских систем (ПСК-5.4);

способностью обеспечивать эффективное применение информационно-технологических ресурсов автоматизированных банковских систем с учетом нормативных требований по защите информации (ПСК-5.5);

способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем (ПСК-5.6);

способностью участвовать в проектировании и эксплуатации системы управления информационной безопасностью автоматизированных банковских систем (ПСК-5.7);

способностью проводить инструментальный мониторинг защищенности автоматизированных банковских систем (ПСК-5.8);

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной банковской системы (ПСК-5.9);

способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы (ПСК-5.10).

Специализация № 6 «Защищенные автоматизированные системы управления»:

способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления (ПСК-6.1);

способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления (ПСК-6.2);

способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях (ПСК-6.3);

способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления (ПСК-6.4);

способностью планировать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью защищенных автоматизированных систем управления и организаций (ПСК-6.5);

способностью применять современные технологии проектирования защищенных автоматизированных систем управления (ПСК-6.6);

способностью участвовать в разработке и оценке соответствия средств защиты информации подсистем обеспечения информационной безопасности защищенных автоматизированных систем управления нормативным требованиям по защите информации (ПСК-6.7).

Специализация № 7 «Обеспечение информационной безопасности распределенных информационных систем»:

способностью разрабатывать и исследовать модели информационно-технологических ресурсов в распределенных информационных системах (ПСК-7.1);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.2);

способностью проводить анализ рисков информационной безопасности в распределенных информационных системах (ПСК-7.3);

способностью разрабатывать и руководить разработкой политики безопасности распределенных информационных систем (ПСК-7.4);

способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.5);

способностью проводить удаленное администрирование операционных систем в распределенных информационных системах (ПСК-7.6);

способностью проводить удаленное администрирование систем баз данных в распределенных информационных системах (ПСК-7.7);

способностью координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации (ПСК-7.8);

способностью применять криптографические протоколы для передачи и хранения данных в распределенных информационных системах (ПСК-7.9).

Специализация № 8 «Анализ безопасности информационных систем»:

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

способностью разрабатывать методики и тесты для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации (ПСК-8.2);

способностью применять инструментарий анализа безопасности программного обеспечения (ПСК-8.3);

способностью применять методы дизассемблирования программ и методы восстановления алгоритма программы по ее дизассемблированному коду (ПСК-8.4);

способностью принимать участие в проведении исследований и испытаний защищенных информационных систем (ПСК-8.5);

способностью участвовать в сертификационных испытаниях по существующим требованиям (ПСК-8.6).

Специализация № 9 «Создание автоматизированных систем в защищенном исполнении»:

способностью разрабатывать модели угроз и модели нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении (ПСК-9.1);

способностью принимать участие в разработке, реализации и управлении процессами создания и эксплуатации автоматизированных систем в защищенном исполнении на всех стадиях и этапах их жизненного цикла (ПСК-9.2);

способностью рационально выбирать методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении (ПСК-9.3);

способностью применять современные технологии проектирования автоматизированных систем в защищенном исполнении (ПСК-9.4);

способностью применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла (ПСК-9.5);

способностью проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении (ПСК-9.6).

Специализация № 10 «Информационная безопасность автоматизированных систем на транспорте»:

способностью участвовать в разработке защищенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта (ПСК-10.1);

способностью применять программные, программно-аппаратные и технические методы и средства защиты информации в распределенных

автоматизированных, информационно-управляющих и информационно-логистических системах транспорта (ПСК-10.2);

способностью разрабатывать предложения по совершенствованию мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности в распределенных автоматизированных, информационно-управляющих и информационно-логистических системах транспорта (ПСК-10.3);

способностью проводить оценку эффективности средств защиты информации, использующихся в автоматизированных, информационно-управляющих и информационно-логистических системах транспорта (ПСК-10.4);

способностью разрабатывать политику безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта (ПСК-10.5);

способностью разрабатывать предложения по совершенствованию системы аудита и управления информационной безопасностью автоматизированных и информационно-управляющих систем транспорта (ПСК-10.6);

способностью осуществлять мониторинг и аудит уровня защищенности, оценку соответствия и аттестацию распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта с учетом нормативных требований по защите информации (ПСК-10.7);

способностью осуществлять рациональный выбор элементной базы обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта (ПСК-10.8);

способностью обеспечить эффективное применение средств защиты технологического электронного документооборота и технического документоведения на транспорте (ПСК-10.9);

способностью выявлять и прогнозировать угрозы информационной безопасности автоматизированных и информационно-управляющих систем транспорта, разрабатывать меры противодействия (ПСК-10.10).

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)[1]	Перечень дисциплин для разработки программ (примерных), а также учебников и учебных пособий	Коды формируемых компетенций
С.1	**Гуманитарный, социальный и экономический цикл**	**32-39**		
	Базовая часть В результате изучения базовой части цикла обучающийся 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	**24-29**[3]	Философия История Отечества Иностранный язык Правоведение Экономика 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-5 ПК-6 ПК-9 ПК-27 ПК-28 ПК-31 ПК-33

Продолжение цикла С.1				
	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 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,			

Продолжение цикла С.1				
	анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности; – 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**	**74-83**		
	Базовая часть В результате изучения базовой части цикла обучающийся 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;	**65-69**[3]	Алгебра и геометрия Математический анализ Дискретная математика Теория вероятностей и математическая статистика Математическая логика и теория алгоритмов	ОК-5 ОК-7 ОК-9 ОК-10 ПК-1 ПК-2 ПК-4 ПК-5 ПК-8 ПК-9 ПК-10 ПК-17 ПК-18 ПК-19 ПК-22 ПК-23 ПК-24

Продолжение цикла С.2				
	– основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики; – основы комбинаторного анализа; – основные понятия теории автоматов; – основные дискретные структуры: конечные автоматы, грамматики, графы, комбинаторные структуры; – методы перечисления для основных дискретных структур; – основные принципы математической логики; – формализации понятия алгоритма: машины Тьюринга, рекурсивные функции; – основные понятия теории сложности алгоритмов; – основные понятия теории информации и кодирования: энтропия, взаимная информация, источники сообщений, каналы связи, коды; – основные результаты о кодировании при наличии и отсутствии шума; – основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи; – 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 обеспечении информационной безопасности автоматизированных систем; – основные понятия информатики; – формы и способы представления данных в персональном компьютере; – состав, назначение функциональных компонентов и		Теория информации Информатика Физика	ПК-25 ПК-26

Продолжение цикла С.2				
	программного обеспечения персонального компьютера; – классификацию современных компьютерных систем; – типовые структуры и принципы организации компьютерных сетей; **уметь:** – строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач; – определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач; – решать основные задачи векторной алгебры и аналитической геометрии; – решать основные задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды; – оперировать с числовыми многочленами, матрицами; – решать основные задачи линейной алгебры, системы линейных уравнений над полями; – применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач; – пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач; – применять стандартные методы дискретной математики и теории автоматов для решения профессиональных задач; – оценивать сложность алгоритмов и вычислений; – вычислять теоретико-информационные характеристики источников сообщений и каналов связи; – решать типовые задачи кодирования и декодирования;			

Продолжение цикла С.2				
	– строить математические модели физических явлений и процессов; – решать типовые прикладные физические задачи; – анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; – применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); – пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; **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; – методами линейной алгебры; – навыками использования стандартных теоретико-вероятностных и статистических методов при решении прикладных задач; – навыками построения дискретных моделей при решении профессиональных задач; – способами оценки сложности работы алгоритмов; – основами построения математических моделей систем передачи информации; – навыками применения математического аппарата для решения прикладных теоретико-информационных задач; – навыками пользования библиотеками прикладных программ для решения прикладных			

Продолжение цикла С.2				
	математических задач; – 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).			
	1. Специализация **«Автоматизированные информационные системы специального назначения»**[2]	**7-10**		
	2. Специализация **«Высокопроизводительные вычислительные системы специального назначения»**[2]	**7-10**		
	3. Специализация **«Информационная безопасность автоматизированных систем критически важных объектов».** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основы теории погрешностей измерений, методы обработки результатов измерений; – способы нормирования и формы задания метрологических характеристик средств измерений; – основные нормативные правовые акты в области метрологии; – цели и методы сертификации; – принципы, методы измерений радиотехнических величин и структурные схемы радиоизмерительных приборов; – принципы построения и структуру автоматизированных средств	**7-10**	Теория функций комплексного переменного Метрология и электро-радиоизмерения Основы радиотехники Антенно-фидерные устройства Теория надежности	ПСК-3.1 ПСК-3.2 ПСК-3.3 ПСК-3.4 ПСК-3.5 ПСК-3.6

Продолжение цикла С.2				
	измерений и контроля; – методы статистической радиотехники; – основные тенденции развития теории и техники антенн и сверхвысокочастотных устройств; – методы расчета и измерения параметров основных линий передачи сверхвысокочастотного диапазона; – основные понятия теории надежности; – способы расчета оценочных показателей надежности аппаратных и программных средств автоматизированных систем обработки информации и управления; – способы повышения надежности систем; **уметь:** – дифференцировать функции комплексного переменного, строить конформные отображения простейших областей, вычислять комплексные интегралы, раскладывать функции в ряд Тейлора и ряд Лорана, а также вычислять вычеты функций; – определять структуру оптимальных устройств обработки сигналов информационных радиотехнических систем и оценивать эффективность их работы; – определять оптимальные алгоритмы работы, оптимальную структуру и характеристики различных радиотехнических устройств; – использовать современные программные средства для проектирования технологической документации; – выбирать и оценивать различные структуры систем с точки зрения надежности; **владеть:** – методами комплексного анализа для вычисления определенных и			

Продолжение цикла С.2				
	несобственных интегралов и решения других задач алгебры и анализа; – методами проектирования систем, удовлетворяющих заданным требованиям надежности.			
	4. Специализация **«Безопасность открытых информационных систем».** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – базовые вопросы построения открытых информационных систем; – основные криптографические протоколы и стандарты; – основные стандарты построения и взаимодействия открытых систем; **уметь:** – применять на практике стандарты, относящиеся к открытым информационным системам; **владеть:** – методикой анализа структуры открытых информационных систем.	**7-10**	Открытые информационные системы Криптографические протоколы и стандарты	ПСК-4.1 ПСК-4.2
	5. Специализация **«Информационная безопасность автоматизированных банковских систем».** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – базовые вопросы построения автоматизированных банковских систем; – основные стандарты, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем; – основы обеспечения катастрофоустойчивости автоматизированных банковских систем; – основные криптографические протоколы и стандарты, используемые в автоматизированных банковских системах;	**7-10**	Автоматизированные банковские системы Катастрофо-устойчивость автоматизированных банковских систем Криптография в банковском деле	ПСК-5.1 ПСК-5.2 ПСК-5.3

Продолжение цикла С.2				
	уметь: – применять на практике стандарты, относящиеся к обеспечению информационной безопасности банковской организации; **владеть:** – методикой анализа структуры автоматизированной банковской системы.			
	6. Специализация «**Защищенные автоматизированные системы управления**». С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основы системного подхода к управлению; – физические явления возникновения побочных сигналов в различных физических полях; – связь информативных признаков с параметрами побочных сигналов; – спектрально-энергетические характеристики информативных сигналов в физических полях любой природы; – основные понятия теории конфликтов; – основные понятия теории игр; – основные понятия теории принятия решений; – основные методы срыва процесса своевременного принятия решения; – основные методы навязывания принятия ложного решения; – основные методы принятия решений в условиях: неопределенности, неполноты сведений, навязывания ложной информации, дефицита времени и вычислительных ресурсов; **уметь:** – выбирать и описывать тип системы управления при решении специализированных прикладных профессиональных задач; – применять измерительное	**7-10**	Основы теории управления Физические основы защиты информации Теория принятия решений в условиях информационных конфликтов	ПСК – 6.1 ПСК – 6.2 ПСК – 6.3

Продолжение цикла С.2				
	оборудование для измерения параметров информативных сигналов в физических полях; – выбирать методы и модели принятия решений в защищенных автоматизированных системах управления; – разрабатывать алгоритмы принятия решений для заданных условий эксплуатации защищенных автоматизированных систем управления; – выявлять уязвимости различных методов и алгоритмов принятия решений для заданных условий эксплуатации защищенных автоматизированных систем управления; **владеть:** – навыками анализа и синтеза систем управления; – навыками выбора и оптимизации вида базисных функций, соответствующих обрабатываемым сигналам и элементной базе; – навыками оценки технических характеристик информативных сигналов в различных физических полях; – навыками разработки алгоритмов защиты от принятия несвоевременных и ложных решений; – навыками оценки вычислительной сложности реализации выбранных или разработанных алгоритмов принятия решений.			
	7. Специализация **«Обеспечение информационной безопасности распределенных информационных систем»**. С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – общую постановку задач математического программирования, динамического программирования, сетевого планирования, теории игр;	**7-10**	Исследование операций и теории игр Теория графов и ее приложения	ПСК-7.1 ПСК-7.2 ПСК-7.4 ПСК-7.5 ПСК-7.9

Продолжение цикла С.2				
	- универсальные приемы исследования оптимизационных проблем при различной степени неопределенности условий; – структуру представления конечных групп; **уметь:** – формировать множество альтернативных решений, ставить цель и выбрать оценочный критерий оптимальности, сформулировать ограничения на управляемые переменные, связанные со спецификой моделируемой системы; – обосновать выбор подходящего математического метода и привести алгоритм решения задачи; – анализировать приводимые представления конечных групп; **владеть:** – навыками построения и анализа моделей типичных операционных задач.			
	8. Специализация **«Анализ безопасности информационных систем»**. С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – математические основы моделирования распределенных систем (графовая модель, сети Петри, логические модели, потоковые модели), модели программ; – формальные методы и подходы к верификации программного обеспечения; – практические основы построения систем статического и динамического анализа программ; – методы анализа и тестирования протоколов; – основы теории формальной спецификации и верификации программного обеспечения; – способы защиты систем от исследования и отладки;	**7-10**	Верификация безопасности информационных систем Анализ безопасности протоколов Математический аппарат и средства анализа безопасности программного обеспечения	ПСК 8.1 ПСК 8.2 ПСК 8.3 ПСК 8.4

Продолжение цикла С.2				
	– подходы к испытанию средств криптографической защиты и требования к встраиванию криптосистем в информационные системы; – методы и алгоритмы дизассемблирования программ; – современные средства отладки и эмуляции программного кода; – методы восстановления алгоритма программы по ее дизассемблированному коду, а также методы построения графа передачи управления программы по исполняемому коду; **уметь:** – формализовать задачи анализа безопасности информационных систем, определять объем необходимых тестов и контрольных экспериментов, разрабатывать методики испытаний, применять существующие инструментальные средства статического и динамического анализа программного обеспечения, средства мониторинга и аудита безопасности; – разрабатывать модели нарушителя и угроз для информационных систем, выделять подсистемы и модули, содержащие критическую информацию; – создавать формальное описание протоколов с целью их дальнейшего анализа; – дизассемблировать и отлаживать программу; – выявить атаку в информационных журналах системы, описать природу атаки, ее признаки и методы обнаружения, оценивать систему с точки зрения проведения возможных атак на систему; **владеть:** – методами и инструментальными средствами анализа безопасности программного обеспечения; – методами и средствами поиска уязвимостей, анализа и верификации			

Продолжение цикла С.2				
	протоколов; – современными методами обработки результатов экспериментов для оценки полноты и достоверности испытаний; – методами и инструментарием эмуляции и виртуализации для проведения испытаний сложных систем; – инструментальными и аппаратными средствами для проверки функционала испытуемых систем; – общими подходами к испытанию систем криптографической защиты (аутентификация, защита данных); – типовыми средствами анализа сетевых протоколов; – современными средствами отладки и тестирования программы; – современными средствами поиска уязвимостей.			
	9. Специализация **«Создание автоматизированных систем в защищенном исполнении»**. С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основы теории электрорадиоизмерений; – основы теории надежности; – основы расчета единичных и комплексных показателей надежности автоматизированных систем и их компонентов; **уметь:** – определять необходимые устройства для измерения параметров информативных сигналов от технических средств обработки информации; – выбирать и оценивать различные структуры систем с точки зрения надежности; **владеть:** – методами обработки результатов электрорадиоизмерений;	**7-10**	Метрология и электрорадио-измерения Основы теории надежности Основы радиотехники	ПСК-9.1 ПСК-9.2 ПСК-9.3 ПСК-9.6

Продолжение цикла С.2				
	– методами проектирования систем по заданным требованиям надежности.			
	10. Специализация **«Информационная безопасность автоматизированных систем на транспорте»**. С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – языки описания цифрового автомата с памятью и методы синтеза схем цифрового автомата произвольного назначения на элементах различного базиса и степени интеграции; – влияние способов кодирования на сложность структуры цифрового автомата, его быстродействие, устойчивость работы (исключение состязаний) и надежность работы; – методы синтеза цифрового автомата с программируемой логикой; – основные методы разработки алгоритмов и программ, структуры данных, используемые для представления типовых информационных объектов; – основные задачи анализа алгоритмов; – основные машинные алгоритмы и характеристики их сложности для типовых задач, часто встречающихся и ставших "классическими" в области информатики и программирования; **уметь:** – получать стандартные формы представления цифрового автомата с памятью по их описанию на начальных языках; – синтезировать логические схемы блоков операционного и управляющего автоматов с использованием методов синтеза цифрового автомата; – разрабатывать алгоритмы,	**7-10**	Теория автоматов Структуры и алгоритмы обработки данных	ПСК-10.1 ПСК-10.2 ПСК-10.3 ПСК-10.9 ПСК-10.10

Продолжение цикла С.2				
	используя общие схемы, методы и приемы построения алгоритмов, выбирая подходящие структуры данных для представления информационных объектов; – доказывать корректность составленного алгоритма и оценивать основные характеристики его сложности; – реализовывать алгоритмы и используемые структуры данных средствами языков программирования высокого уровня; – исследовать эффективность алгоритма и программы; **владеть:** – навыками разработки алгоритмов и программ, структур данных, используемых для представления типовых информационных объектов; – системным подходом при построении алгоритмов; – навыками реализации алгоритмов и используемых структур данных, средствами языков программирования высокого уровня.			
	Вариативная часть (знания, умения, навыки определяются ООП вуза)	**9-14**		
С.3	**Профессиональный цикл**	**140-150**		
	Базовая (общепрофессиональная) часть В результате изучения базовой части цикла обучающийся должен: **знать:** – основные информационные технологии, используемые в автоматизированных системах; – опасные и вредные факторы системы «человек – среда обитания»; – научные и организационные основы защиты окружающей среды и ликвидации последствий аварий, катастроф, стихийных бедствий; – общие принципы построения и использования современных языков программирования высокого уровня; – язык программирования высокого	**102-108**[3]	Безопасность жизнедеятельности Языки программирования Технологии и методы программирования Электроника и схемотехника Безопасность операционных систем Безопасность сетей	ОК-1 ОК-2 ОК-5 ОК-6 ОК-7 ОК-8 ОК-9 ОК-10 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-10 ПК-11 ПК-12 ПК-13

Продолжение цикла С.3			
уровня (объектно-ориентированное программирование); – возможности, классификацию и область применения макрообработки; – способы обработки исключительных ситуаций; – современные технологии и методы программирования; – показатели качества программного обеспечения; – методологии и методы проектирования программного обеспечения; – методы тестирования и отладки программного обеспечения; – принципы организации документирования разработки, процесса сопровождения программного обеспечения; – основные структуры данных и способы их реализации на языке программирования; – основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности; – 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; – принципы построения и функционирования, примеры реализаций современных операционных систем; – функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; – критерии оценки эффективности и надежности средств защиты операционных систем; – принципы организации и структуру		ЭВМ Безопасность систем баз данных Основы информационной безопасности Криптографические методы защиты информации Организация ЭВМ и вычислительных систем Техническая защита информации Сети и системы передачи информации Организационное и правовое обеспечение информационной безопасности Программно-аппаратные средства обеспечения информационной безопасности Разработка и эксплуатация защищенных автоматизированных систем Управление информационной безопасностью	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 ПК-39 ПК-40

Продолжение цикла С.3				
	подсистем защиты операционных систем семейств UNIX и Windows; – принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей; – основные протоколы компьютерных сетей; – последовательность и содержание этапов построения компьютерных сетей; – эталонную модель взаимодействия открытых систем; – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях; – принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; – основные модели данных, физическую организацию баз данных; – средства обеспечения безопасности данных; – последовательность и содержание этапов проектирования баз данных; – 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 задачи и понятия криптографии; – требования к шифрам и основные характеристики шифров;		Инженерная графика	

Продолжение цикла С.3				
	– типовые поточные и блочные шифры; – частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки; – типовые шифры с открытыми ключами; – модели шифров и математические методы их исследования; – архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем; – терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; – технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; – 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 характеристики сигналов электросвязи, спектры и виды модуляции; – принципы построения и функционирования систем и сетей передачи информации; – способы кодирования информации; – основные телекоммуникационные протоколы; – основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые			

Продолжение цикла С.3				
	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; – 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; – программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; – методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; – содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности			

Продолжение цикла С.3				
	автоматизированных систем; – методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; – основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах; – основные методы управления информационной безопасностью; – методы аттестации уровня защищенности автоматизированных систем; – принципы формирования политики информационной безопасности в автоматизированных системах; – основные положения стандартов Единой системы конструкторской документации, Единой системы программной документации; **уметь:** – реализовывать и контролировать выполнение требований по охране труда и технике безопасности в профессиональной деятельности; – применять основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий; – работать с интегрированной средой разработки программного обеспечения; – использовать шаблоны классов и средства макрообработки; – использовать динамически подключаемые библиотеки; – формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; – планировать разработку сложного			

Продолжение цикла С.3				
	программного обеспечения; – проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; – проводить комплексное тестирование и отладку программных систем; – проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; – реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; – проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач; – применять на практике методы анализа электрических цепей; – работать с современной элементной базой электронной аппаратуры; – использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации; – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; – оценивать эффективность и надежность защиты операционных систем; – планировать политику безопасности операционных систем; – проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; – эффективно использовать различные методы и средства			

Продолжение цикла С.3				
	защиты информации для компьютерных сетей; – проводить мониторинг угроз безопасности компьютерных сетей; – разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных; – реализовывать политику безопасности баз данных; – выделять сущности и связи предметной области; – отображать предметную область на конкретную модель данных; – нормализовывать отношения при проектировании реляционной базы данных; – создавать объекты базы данных; – выполнять запросы к базе данных; – разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных; – применять средства обеспечения безопасности данных; – классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; – эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; – применять математические методы исследования моделей шифров; – проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем; – осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий;			

Продолжение цикла С.3				
	– анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; – пользоваться нормативными документами по противодействию технической разведке; – анализировать и оценивать угрозы информационной безопасности объекта; – применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем; – анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; – 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; – проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; – разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; – администрировать подсистемы информационной безопасности автоматизированных систем; – восстанавливать работоспособность подсистемы			

Продолжение цикла С.3				
	информационной безопасности автоматизированных систем в нештатных ситуациях; – исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; – разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; – определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; – разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем; – оценивать информационные риски в автоматизированных системах; – определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; – составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; – разрабатывать частные политики информационной безопасности автоматизированных систем; – контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; – разрабатывать предложения по			

Продолжение цикла С.3				
	совершенствованию системы управления информационной безопасностью автоматизированных систем; – применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; **владеть:** – профессиональной терминологией в области информационной безопасности; – навыками безопасного использования технических средств в профессиональной деятельности; – навыками проектирования программного обеспечения с использованием средств автоматизации; – навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; – навыками разработки программной документации; – навыками программирования с использованием эффективных реализаций структур данных и алгоритмов; – навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры; – навыками работы с программными средствами схемотехнического моделирования; – навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; – навыками оценки быстродействия и оптимизации работы электронных схем на базе современной			

Продолжение цикла С.3				
	элементной базы; – навыками работы с современными операционными системами, восстановления операционных систем после сбоев; – навыками установки и настройки современных операционных систем с учетом требований по обеспечению информационной безопасности; – навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; – навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; – навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей; – навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; – криптографической терминологией; – навыками использования типовых криптографических алгоритмов; – навыками использования ЭВМ в анализе простейших шифров; – навыками математического моделирования в криптографии; – методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем; – навыками работы с технической документацией на ЭВМ и вычислительные системы; – методами и средствами технической защиты информации; – методами расчета и инструментального контроля показателей технической защиты			

Продолжение цикла С.3				
	информации; – навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; – 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; – навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; – навыками анализа основных узлов и устройств современных автоматизированных систем; – навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; – методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; – навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; – навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; – методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных			

Продолжение цикла С.3				
	систем; – методами управления информационной безопасностью автоматизированных систем; – методами оценки информационных рисков; – навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем; – навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации.			
	1. Специализация **«Автоматизированные информационные системы специального назначения»**[2]	**9-11**		
	2. Специализация **«Высокопроизводительные вычислительные системы специального назначения»**[2]	**9-11**		
	3. Специализация **«Информационная безопасность автоматизированных систем критически важных объектов»**. С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – характеристики основных технических каналов утечки информации на критически важных объектах; – методы и процедуры выявления угроз информационной безопасности на критически важных объектах; – средства защиты информации, используемые на критически важных объектах; – тактико-технические характеристики и возможности систем и средств технической разведки; – способы и средства охраны объектов;	**9-11**	Обеспечение информационной безопасности на критически важных объектах Инженерно-техническая защита информации и технические средства охраны на критически важных объектах Основы аттестации объектов информатизации критически важных объектов Методы и средства противодействия террористической	ПСК – 3.1 ПСК – 3.2 ПСК – 3.3 ПСК – 3.4 ПСК – 3.5 ПСК – 3.6

Продолжение цикла С.3				
	уметь: – формулировать основные требования к методам и средствам технической защиты информации на критически важных объектах; – реализовывать с учетом особенностей функционирования критически важных объектов требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам защиты информации ограниченного доступа; – составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности применения мер по технической защите информации на критически важных объектах; **владеть:** – терминологией и системным подходом построения защищенных автоматизированных систем критически важных объектов; – навыками анализа угроз и уязвимостей информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов; – навыками формирования политик безопасности для критически важных объектов и автоматизированных систем критически важных объектов; – навыками проведения специальных исследований и инструментального контроля защищенности автоматизированных систем критически важных объектов; – навыками работы с нормативными правовыми актами в области технической защиты информации ограниченного доступа на предприятии (в организации, учреждении).		деятельности в системах управления критически важных объектов	
	4. Специализация «**Безопасность открытых**	**9-11**	Информационная безопасность	ПСК-4.1 ПСК-4.2

Продолжение цикла С.3				
	информационных систем». С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – подходы к интеграции сетей в открытых информационных системах; – принципы работы сетевых протоколов и технологий передачи данных в открытых информационных системах; – основные методы и средства реализации удаленных сетевых атак на открытые информационные системы; – о политиках безопасности и мерах защиты в открытых информационных системах; – о комплексном подходе к построению эшелонированной защиты для открытых информационных систем; – принципы построения современных виртуальных локальных и частных сетей и направления их развития; – виды виртуальных сетей и их преимущества при конкретном применении; – политику безопасности для виртуальных сетей; – основные стандарты построения виртуальных сетей; – принципы работы сетевых протоколов и технологий передачи данных в виртуальных сетях; – подходы к интеграции виртуальных сетей с открытыми информационными системами; **уметь:** – проектировать защищенные открытые информационные системы; – определять и устранять основные угрозы информационной безопасности для открытых информационных систем; – строить модель нарушителя информационной безопасности для		открытых систем Виртуальные частные сети Аудит информационных технологий и систем обеспечения информационной безопасности	ПСК-4.3 ПСК-4.4 ПСК-4.5 ПСК-4.6 ПСК-4.7 ПСК-4.8

Продолжение цикла С.3				
	открытых информационных систем; – выявлять и устранять уязвимости в основных компонентах открытых информационных систем; – обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам; – применять стандартные решения для защиты информации в открытых информационных системах и квалифицированно оценивать их качество; – используя современные методы и средства, разрабатывать и оценивать модели и политику безопасности для открытых информационных систем; – реализовывать системы защиты информации в открытых информационных системах в соответствии со стандартами по оценке защищенных систем; – практически решать задачи защиты программ и данных программно-аппаратными средствами и давать оценку качества предлагаемых решений; – осуществлять мониторинг и аудит сетевой безопасности; – осуществлять администрирование открытых информационных систем; – осуществлять управление информационной безопасностью в открытых информационных системах; – применять стандартные решения для защиты информации в виртуальных сетях и квалифицированно оценивать их качество; – используя современные методы и средства, разрабатывать и оценивать модели и политику безопасности для виртуальных сетей; – практически реализовывать различные варианты построения виртуальных сетей в соответствии со стандартами по оценке защищенных систем и давать оценку качества предлагаемых решений;			

Продолжение цикла С.3				
	– проектировать защищенные открытые информационные системы; **владеть:** – терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей; – навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; – навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей.			
	5. Специализация **«Информационная безопасность автоматизированных банковских систем»**. С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основные методы защиты информации в автоматизированных банковских системах; – о комплексном подходе к построению эшелонированной защиты для автоматизированных банковских систем; – методы электронного документооборота в автоматизированных банковских системах; – основные методы обеспечения безопасности пластиковых карт; **уметь:** – проводить синтез и анализ проектных решений по обеспечению информационной безопасности автоматизированных банковских систем; – эффективно применять информационно-технологические ресурсы автоматизированных банковских систем с учетом требований информационной безопасности;	**9-11**	Защита информации в банковских системах Защита электронного документооборота Безопасность систем пластиковых карт Нормативная база обеспечения информационной безопасности банковской организации	ПСК - 5.1 ПСК - 5.2 ПСК - 5.3 ПСК - 5.4 ПСК - 5.5 ПСК - 5.6 ПСК - 5.7 ПСК - 5.8 ПСК - 5.9 ПСК - 5.10

Продолжение цикла С.3				
	– разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем; – проектировать и эксплуатировать системы управления информационной безопасностью автоматизированных банковских систем; – проводить инструментальный мониторинг защищенности автоматизированных банковских систем; – разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных банковских систем; – формировать и эффективно применять комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированных банковских систем; **владеть:** – терминологией и системным подходом построения защищенных автоматизированных банковских систем; – навыками анализа угроз информационной безопасности и уязвимостей в автоматизированных банковских системах; – навыками анализа угроз и формирования политик безопасности для автоматизированных банковских систем; – навыками формирования и эффективного применения комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированных банковских систем и банковских организаций.			

Продолжение цикла С.3				
	6. Специализация **«Защищенные автоматизированные системы управления»** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – принципы защиты программного обеспечения защищенных автоматизированных систем управления от несанкционированного копирования с привязкой к магнитным носителям, регистрационным кодам и специальным аппаратным устройствам защиты (электронным ключам); – средства защиты программного обеспечения защищенных автоматизированных систем управления; – современные системы проектирования программного и аппаратного обеспечения защищенных автоматизированных систем управления; – основы построения систем менеджмента информационной безопасности на базе современных международных и национальных стандартов; – основные критерии, методы и меры обеспечения доверия к информационной безопасности; **уметь:** – применять инструментальные средства для исследования программного обеспечения защищенных автоматизированных систем управления в машинных кодах; – выявлять уязвимости защиты программного обеспечения защищенных автоматизированных систем управления и находить пути их устранения; – проектировать и реализовывать защиту программного обеспечения	**9-11**	Защита программного обеспечения защищенных автоматизированных систем Технологии проектирования защищенных автоматизированных систем Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления Обеспечение доверия к информационной безопасности защищенных автоматизированных систем управления	ПСК - 6.1 ПСК - 6.2 ПСК - 6.3 ПСК - 6.4 ПСК - 6.5 ПСК - 6.6 ПСК - 6.7

Продолжение цикла С.3				
	защищенных автоматизированных систем управления, исходя из поставленных целей защиты; – разрабатывать модели жизненного цикла защищенных автоматизированных систем управления с учетом требований по обеспечению информационной безопасности на основе современных международных и национальных стандартов; – применять основные положения системного и объектно-ориентированного проектирования и моделирования защищенных автоматизированных систем управления; – разрабатывать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью; – выбирать, разрабатывать и внедрять практические меры по управлению информационной безопасностью на основе современных международных и национальных стандартов; **владеть:** – навыками работы с современными инструментальными средствами для исследования программного обеспечения защищенных автоматизированных систем управления; – навыками разработки защиты программного обеспечения для защищенных автоматизированных систем управления; – навыками автоматизации и управления процессом проектирования защищенных автоматизированных систем управления; – навыками разработки систем мониторинга информационной безопасности защищенных автоматизированных систем управления; – навыками применения различных			

Продолжение цикла С.3				
	методов и мер обеспечения доверия к информационной безопасности: лицензирование, аккредитация, оценка и подтверждение соответствия.			
	7. Специализация **«Обеспечение информационной безопасности распределенных информационных систем».** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основные положения теории управления; – специфику математического моделирования организационных задач в автоматизированных системах; – способы обеспечения информационной безопасности систем организационного управления; – принципы построения распределенных систем и объектно-ориентированных систем управления базами данных, технологии автоматизированного проектирования баз данных и хранилищ данных, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования; – нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты; **уметь:** – разрабатывать модели систем организационного управления; – использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности	**9-11**	Информационная безопасность распределенных информационных систем Методы проектирования защищенных распределенных информационных систем Технология построения защищенных распределенных приложений	ПСК-7.1 ПСК-7.2 ПСК-7.3 ПСК-7.4 ПСК-7.5 ПСК-7.6 ПСК-7.7 ПСК-7.8 ПСК-7.9

Продолжение цикла С.3			
функционирования распределенной информационной системы; – применять нормативные документы по метрологии, стандартизации и сертификации на практике; **владеть:** – навыками разработки политики безопасности систем организационного управления; – навыками семантического моделирования данных, навыками проектирования информационных систем на базе корпоративных систем управления базами данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения; – навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.			
8. Специализация «**Анализ безопасности информационных систем**» С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – принципы построения современных систем обеспечения информационной безопасности; – принципы статистического анализа; – способы описания поведения систем; – типовые архитектуры и принципы построения современных защищенных информационных систем; – угрозы и атаки, характерные для распределенных информационных систем; **уметь:** – формализовать задачу контроля параметров безопасности	**9-11**	Мониторинг безопасности информационных систем Анализ рисков информационной безопасности	ПСК – 8.2 ПСК – 8.3 ПСК – 8.5 ПСК – 8.6

Продолжение цикла С.3				
	информационными системами; – разрабатывать методы и средства для проверки выполнения требований информационной безопасности и поиска уязвимостей; **владеть:** – методиками оценки рисков информационной безопасности; – средствами фиксации параметров безопасности информационных систем; – методами реализации и верификации моделей контроля и управления доступом; – навыками применения средств анализа безопасности информационных систем.			
	9. Специализация **«Создание автоматизированных систем в защищенном исполнении»** С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – методы и процедуры выявления угроз и нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении; – методы и средства для обеспечения информационной безопасности автоматизированных систем в защищенном исполнении на различных стадиях и этапах их жизненного цикла; – современные технологии проектирования автоматизированных систем в защищенном исполнении; – нормативную правовую базу, руководящие и методические документы, регламентирующие реализацию процессов создания автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла; – методы и средства анализа	**9-11**	Угрозы информационной безопасности автоматизированных систем Создание автоматизированных систем в защищенном исполнении Оценка информационной безопасности автоматизированных систем в защищенном исполнении	ПСК-9.1 ПСК-9.2 ПСК-9.3 ПСК-9.4 ПСК-9.5 ПСК-9.6

Продолжение цикла С.3				
	достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении; **уметь:** – разрабатывать модели угроз и нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении; – формировать требования по обеспечению информационной безопасности автоматизированных систем в защищенном исполнении; – разрабатывать проектные решения по автоматизированным системам в защищенном исполнении, их системам обеспечения информационной безопасности, реализовывать их, управлять процессами разработки и реализации этих проектных решений; – проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении; **владеть:** – терминологией и технологиями проектирования автоматизированных систем в защищенном исполнении; – навыками анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении; – навыками проведения специальных исследований и инструментального контроля защищенности автоматизированных систем в защищенном исполнении.			
	10. Специализация **«Информационная безопасность автоматизированных систем на транспорте»**	**9-11**	Информационная безопасность информационно-управляющих и	ПСК-10.1 ПСК-10.2 ПСК-10.3 ПСК-10.4

Продолжение цикла С.3				
	С целью получения данной специализации при изучении базовой части цикла обучающийся должен: **знать:** – основы комплексного обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта; – основные свойства схем шифрования, электронной цифровой подписи и аутентификации при решении задач защиты технологического электронного документооборота и документоведения; – принципы применения и построения систем управления ресурсами предприятия и технологий поддержки жизненного цикла, методы и средства обеспечения их информационной безопасности; **уметь:** – используя современные методы и средства, разрабатывать и оценивать модели и политики безопасности автоматизированных и информационно-управляющих систем на транспорте; – анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте, применять автоматизированные средства мониторинга, аудита и анализа защищенности данных систем; – реализовывать системы защиты информации в распределенных автоматизированных, информационно-управляющих и информационно-логистических системах на транспорте в соответствии со стандартами по		информационно-логистических систем транспорта Защита информации в распределенных информационных системах и центрах обработки данных Информационная безопасность автоматизированных транспортных систем Защита электронного технологического документооборота	ПСК-10.5 ПСК-10.6 ПСК-10.7 ПСК-10.8 ПСК-10.9 ПСК-10.10

Продолжение цикла С.3				
	оценке защищенных систем; – обеспечивать защиту электронного технологического документооборота на основе электронной цифровой подписи; – решать практические задачи информационной безопасности на основе инфраструктуры открытых ключей; – обеспечивать безопасность систем управления ресурсами предприятия и технологий поддержки жизненного цикла; **владеть:** – навыками анализа угроз и уязвимостей информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте; – навыками анализа угроз и навыками построения политик безопасности распределенных автоматизированных информационно-управляющих и информационно-логистических систем транспорта; – навыками развертывания и обеспечения работы программных комплексов, обеспечивающих работу с цифровыми сертификатами; – методами эксплуатации средств защиты информации; – системным подходом к организации информационных процессов (в том числе систем управления ресурсами предприятия и технологий поддержки жизненного цикла), анализу информационной безопасности распределенных автоматизированных информационно-управляющих и информационно-логистических систем транспорта.			
	Вариативная часть (знания, умения, навыки определяются ООП вуза)	**38-42**		
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)	**15-18**		ОК-1 – ОК-11 ПК-1 – ПК-40 ПСК-1.1 – ПСК-10.10
С.6	**Итоговая государственная аттестация**	**18-21**		ОК-3 ОК-5 ОК-7 – ОК-10 ПК-1 – ПК-22 ПК-29 ПК-31 – ПК-34 ПСК-1.1 – ПСК-10.10
	Общая трудоемкость основной образовательной программы	**300**		

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

[2] В соответствии с п. 7.1 настоящего стандарта требования к результатам освоения и структуре ООП в части специализаций определяются вузом.

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

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 **090303 Информационная безопасность автоматизированных систем** 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 актов 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 актов 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 актов 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, разборов конкретных ситуаций, психологических и иных тренингов) 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 необязательных 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 № 71 от 14 февраля 2008 г. (Собрание законодательства Российской Федерации, 2008, № 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,

---

* Статья 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).

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, электроники и схемотехники, сетей и систем передачи информации, технологии и методов программирования, безопасности сетей ЭВМ, безопасности операционных систем, безопасности систем баз данных, программно-аппаратных средств обеспечения информационной безопасности, технической защиты информации, 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 ориентированную 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 ООП 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;

выступать 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 обучающегося. 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 «Информационная безопасность автоматизированных систем».

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 нормативные правовые 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;

---

* Пункт 2 статьи 41 Закона Российской Федерации «Об образовании» от 10 июля 1992 г. № 3266 -1 (Собрание законодательства Российской Федерации, 1996, № 3, ст. 150; 2002, № 26, ст. 2517; 2004, № 30, ст. 3086; № 35, ст. 3607; 2005, № 1, ст. 25; 2007, № 17, ст. 1932; № 44, ст. 5280).

- технологии и методов программирования;
- безопасности сетей ЭВМ.

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;
- безопасности операционных систем;
- безопасности систем баз данных.

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 соответствующей 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.