



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владивостокский государственный университет экономики и сервиса»

УТВЕРЖДЕНО
на заседании Ученого совета ВГУЭС
протокол от 14.06 2020 № 8
Ректор И.В. Терентьева



ОСНОВНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

**Обеспечение информационной безопасности
распределённых информационных систем**

Квалификация

специалист по защите информации

Форма обучения

Очная

Владивосток 2020

Члены рабочей группы по разработке ОПОП

канд.техн.наук, Доброжинский Ю.В.,

д-р экон. наук, проф., Мазелис Л.С.,

д-р экон. наук, проф., советник ректора, Крюков В.В.,

ведущий инженер по защите информации центра информационно-технического обеспечения, Зимин В.В.

ОПОП рассмотрена и принята на заседании Кафедры информационной безопасности

Протокол заседания кафедры

от «12» мая 2020 г. № 1

И.о. зав.кафедрой  Доброжинский Ю.В.

СОГЛАСОВАНО

Директор

Департамента учебной и воспитательной работы



Ю.Г. Чебова

Компоненты ОПОП

- 1 Общая характеристика основной профессиональной образовательной программы
 - 1.1 Общие положения
 - 1.2 Характеристика основной профессиональной образовательной программы
 - 1.2.1 Цель ОПОП
 - 1.2.2 Требования к уровню подготовки, необходимому для освоения программы
 - 1.2.3 Формы обучения
 - 1.2.4 Срок получения образования
 - 1.2.5 Объем программы
 - 1.2.6 Образовательные технологии
 - 1.2.7 Квалификация, присваиваемая выпускникам
 - 1.2.8 Язык, на котором реализуется ОПОП
 - 1.2.9 Характеристика профессиональной деятельности выпускника
 - 1.2.9.1 Область профессиональной деятельности выпускника
 - 1.2.9.2 Объекты профессиональной деятельности выпускника
 - 1.2.9.3 Виды профессиональной деятельности выпускника
 - 1.2.9.4 Задачи профессиональной деятельности выпускника
 - 1.2.10 Планируемые результаты освоения ОПОП
 - 1.2.11 Структура ОПОП
 - 1.2.12 Требования к условиям реализации ОПОП
 - 1.2.12.1 Сведения о профессорско-преподавательском составе, необходимом для реализации программы
 - 1.2.12.2 Требования к материально-техническому и учебно-методическому обеспечению программы
- 2 Компетентностная модель выпускника
- 3 Учебный план
- 4 Рабочие программы дисциплин, включая фонды оценочных средств
- 5 Программы практик, включая фонды оценочных средств
- 6 Программа государственной итоговой аттестации
- 7 Договоры о базах практик (договоры о комплексном сотрудничестве с организациями)

1 Общая характеристика основной профессиональной образовательной программы

1.1 Общие положения

1.1.1 Основная профессиональная образовательная программа (далее – ОПОП) специалитета, реализуемая федеральным государственным бюджетным образовательным учреждением высшего образования «Владивостокский государственный университет экономики и сервиса» (далее – ВГУЭС) по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация № 7 «Обеспечение информационной безопасности распределённых информационных систем», представляет собой комплекс документов, разработанный с учетом требований рынка труда на основе федерального государственного образовательного стандарта высшего образования (далее – ФГОС ВО) по специальности 10.05.03 Информационная безопасность автоматизированных систем и утвержденный решением Ученого совета университета.

1.1.2 При разработке основной профессиональной образовательной программы использовались следующие нормативные документы:

- Федеральный закон Российской Федерации от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержден приказом Минобрнауки России от 01.12.2016 № 1509;
- Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержден приказом Минобрнауки России от 05.04.2017 № 301;
- Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов, утверждены Минобрнауки России от 22.01.2015 № ДЛ-01/05вн;
- профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н;
- нормативно-методические документы Минобрнауки России;
- Устав ВГУЭС, утвержден приказом Минобрнауки России от 19.08.2015 № 882;
- локальные нормативные акты ВГУЭС.

1.2 Характеристика ОПОП

1.2.1 Цель основной профессиональной образовательной программы по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределённых информационных систем» развитие у студентов личностных и деловых качеств, формирование у них компетенций в соответствии с требованиями ФГОС ВО, обеспечивающих готовность выпускников к профессиональной деятельности по выполнению комплекса мер по информационной безопасности объекта защиты; по выполнению работ по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации; по применению программных средств системного, прикладного и специального назначения, инструментальных средств и системы программирования.

1.2.2 Требования к уровню подготовки, необходимому для освоения программы специалитета.

К освоению программы специалитета допускаются лица, имеющие среднее общее образование.

1.2.3 Формы обучения. Обучение по программе осуществляется в очной форме обучения.

1.2.4 Срок получения образования по программе вне зависимости от применяемых

образовательных технологий:

- в очной форме обучения – 5 лет, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации;

- при обучении по индивидуальному учебному плану вне зависимости от формы обучения составляет не более срока получения образования, установленного для очной формы обучения;

- при обучении по индивидуальному плану лиц с ограниченными возможностями здоровья может быть увеличен по их желанию не более чем на 1 год по сравнению со сроком получения образования, установленным для очной формы обучения.

1.2.5 Объем программы составляет 300 зачетных единиц (далее – з.е).

Объем программы реализуемый за один учебный год составляет:

- в очной форме обучения – 60 з.е.;

Объем программы за один учебный год при обучении по индивидуальному плану вне зависимости от формы обучения не более 75 з.е.

1.2.6 Образовательные технологии. При реализации ОПОП сочетаются традиционное, электронное и смешанное обучение, применяются компьютерные технологии (интернет-платформы, интернет-сервисы, электронные информационные и образовательные ресурсы), активные и интерактивные методы обучения (проектная деятельность, проблемное обучение, дискуссии, деловые игры, решение ситуационных задач).

1.2.7 Квалификация, присваиваемая выпускникам

По окончании обучения по программе выпускникам присваивается квалификация - специалист по защите информации.

1.2.8 Язык, на котором реализуется ОПОП – русский.

1.2.9 Характеристика профессиональной деятельности выпускника

1.2.9.1 Область профессиональной деятельности выпускника

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

1.2.9.2 Объекты профессиональной деятельности выпускника

Объектами профессиональной деятельности выпускников, освоивших программу специалитета, являются:

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

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

- технологии обеспечения информационной безопасности автоматизированных систем;

- системы управления информационной безопасностью автоматизированных систем.

1.2.9.3 Виды профессиональной деятельности выпускника

Специалист по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем готовится к следующим **видам профессиональной деятельности**:

- научно-исследовательская;
- проектно-конструкторская;
- контрольно-аналитическая;
- организационно-управленческая;
- эксплуатационная.

Специализация, по которой готовятся выпускники, освоившие программу специалитета: специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем".

1.2.9.4 Задачи профессиональной деятельности выпускника

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

в соответствии с видами профессиональной деятельности:

научно-исследовательская деятельность:

- сбор, обработка, анализ и систематизация научно-технической информации по проблематике информационной безопасности автоматизированных систем;
- подготовка научно-технических отчетов, обзоров, докладов, публикаций по результатам выполненных исследований;
- моделирование и исследование свойств защищенных автоматизированных систем;
- анализ защищенности информации в автоматизированных системах и безопасности реализуемых информационных технологий;
- разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;

проектно-конструкторская деятельность:

- сбор и анализ исходных данных для проектирования защищенных автоматизированных систем;
- разработка политик информационной безопасности автоматизированных систем;
- разработка защищенных автоматизированных систем в сфере профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;
- выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
- разработка систем управления информационной безопасностью автоматизированных систем;

контрольно-аналитическая:

- контроль работоспособности и эффективности применяемых средств защиты информации;
- выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;
- проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов;

организационно-управленческая деятельность:

- организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
- организационно-методическое обеспечение информационной безопасности автоматизированных систем;
- организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;
- контроль реализации политики информационной безопасности;

эксплуатационная деятельность:

- реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;
- администрирование подсистем информационной безопасности автоматизированных систем;
- мониторинг информационной безопасности автоматизированных систем;
- управление информационной безопасностью автоматизированных систем;
- обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций;

В соответствии со специализацией N 7 "Обеспечение информационной безопасности распределенных информационных систем":

- разработка и исследование моделей информационно-технологических ресурсов, модели угроз и модели нарушителей информационной безопасности в распределенных информационных системах;
- удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах;
- аудит защищенности информационно-технологических ресурсов;
- координация деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятиях и в учреждениях.

1.2.10 Планируемые результаты освоения ОПОП

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

Выпускник, освоивший программу специалитета, должен обладать следующими **общекультурными компетенциями:**

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

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

способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

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

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

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

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

способностью к самоорганизации и самообразованию (ОК-8);

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

Выпускник, освоивший программу специалитета, должен обладать следующими **общепрофессиональными компетенциями:**

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

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

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

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

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

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

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

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

Выпускник, освоивший программу специалитета, должен обладать следующими

профессиональными компетенциями:

научно-исследовательская деятельность:

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

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

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

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

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

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

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

проектно-конструкторская деятельность:

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

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

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

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

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

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

контрольно-аналитическая деятельность:

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

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

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

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

организационно-управленческая деятельность:

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

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

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

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

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

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

эксплуатационная деятельность:

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

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

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

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

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

Выпускник, освоивший программу специалитета, должен обладать

профессионально-специализированными компетенциями, соответствующими специализации программы специалитета:

специализация N 7 "Обеспечение информационной безопасности распределённых информационных систем":

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

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

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

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

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

1.2.11 Структура ОПОП

Структура программы соответствует требованиям ФГОС ВО (утв. приказом Минобрнауки от 01.12.2016 № 1509) по данной специальности, что отражено в учебном плане.

1.2.12 Требования к условиям реализации ОПОП

1.2.12.1 Сведения о профессорско-преподавательском составе, необходимом для реализации программы

Квалификация руководящих и научно-педагогических работников организации соответствует квалификационным характеристикам, установленным в Едином квалификационном справочнике должностей руководителей, специалистов и служащих, разделе "Квалификационные характеристики должностей руководителей и специалистов высшего профес-

сионального и дополнительного профессионального образования", утвержденном приказом Министерства здравоохранения и социального развития Российской Федерации от 11 января 2011 г. № 1н (зарегистрирован Министерством юстиции Российской Федерации 23 марта 2011 г., регистрационный № 20237), и профессиональным стандартам (при наличии).

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

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

Доля научно-педагогических работников (в приведенных к целочисленным значениям ставок) имеющих образование и (или) ученую степень, соответствующие профилю преподаваемой дисциплины (модуля), в общем числе научно-педагогических работников, реализующих программу специалитета, составляет не менее 80 процентов, что соответствует требованиям ФГОС ВО.

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

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

1.2.12.2 Требования к материально-техническому и учебно-методическому обеспечению, программы

ВГУЭС, реализующий образовательную программу по специальности 10.05.03 «Информационная безопасность автоматизированных систем» располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

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

Электронная информационно-образовательная среда организации обеспечивает:

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

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

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

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

процесса;

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

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование электронной информационно-образовательной среды соответствует законодательству Российской Федерации.

Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

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

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

Перечень материально-технического обеспечения включает в себя лаборатории:

Лаборатория физики, оснащенная: учебные столы 6 шт., стулья 24 шт., спец. столы 8 шт., мультимедийное оборудование 1 шт., доска маркерная 1 шт., шкафы для хранения учебно-наглядных пособий 2 шт. учебно-лабораторные стенды по механике, электричеству и магнетизму, оптике.

Лаборатория электротехники, электроники и схемотехники, оснащенная: лабораторные столы 12 шт., стулья 32 шт., стол и стул для преподавателя, стеллаж для приборов - 1 шт., доска маркерная 1 шт., мультимедийный проектор, компьютерные столы 20 шт., персональные компьютеры - 20 шт. Учебно-лабораторные стенды для изучения работы компонентов узлов и блоков вычислительных устройств, рабочих мест разработчиков систем и устройств в системах автоматизированного проектирования, средствами для измерения и визуализации частотных и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов. Обучающее лицензионное ПО: NI LabView;

Лаборатория сетей и систем передачи информации, оснащенная: лабораторные столы 12 шт., стулья 32 шт., стол и стул для преподавателя, стеллаж для приборов - 1 шт., доска маркерная 1 шт., мультимедийный проектор, компьютерные столы 20 шт., персональные компьютеры - 20 шт. Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов, структурированной кабельной системой, телекоммуникационным оборудованием, обучающим программным обеспечением, эмулятором активного сетевого оборудования. в том числе: лабораторные стенды LED-INT "Интерфейс, протокол, связь", точки доступа Cisco AIR-CAP1702I-R-K9 2 шт., коммутаторы Cisco Catalyst WS-C2960+24TC-L 6 шт., маршрутизаторы Cisco 1941/K9 6 шт., межсетевые экраны Cisco ASA 550 2 шт. Обучающее лицензионное ПО: NI Labview, Snort, Nmap/Zenmap, OpenVPN, Cisco Packet Tracer, Netemul, GNS3, HP Network Simulator. Дополнительное лицензионное ПО: MS Visual C++, True Crypt v 7.2, VMware Horizon Agent v 7.0.0, Oracle VM VirtualBox, Java 8.

Лаборатория безопасности сетей ЭВМ: оснащенная: учебные столы 22 шт., стулья 22 шт., стол для преподавателя 1 шт., стул для преподавателя 1 шт., доска маркерная 1 шт., мультимедийный проектор 1 шт., персональные компьютеры 22 шт. Стенды для изучения проводных и беспроводных компьютерных сетей, включающих абонентские устройства,

коммутаторы, маршрутизаторы, точки доступа, межсетевые экраны, системы обнаружения компьютерных атак, системы углубленной проверки сетевых пакетов и системы защиты от утечки данных, анализаторы кабельных сетей, в том числе: лабораторный стенд "Телекоммуникационные линии связи" УП-139 1 шт. беспроводные точки доступа Cisco AIR-CAP1702I-R-K9 2 шт., коммутаторы Cisco Catalyst WS-C2960+24TC-L 6 шт., маршрутизатор Cisco 1941/K9 6 шт., межсетевой экран Cisco ASA 550 1 шт., Secret Net 8 (комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования) 15 шт., анализаторы кабельных сетей Fluke Networks MS2-ТТК 2 шт. Обучающее лицензионное ПО: NI Labview, Snort, Wireshark, Nmap/Zenmap, OpenVPN, Cisco Packet Tracer, Netemul, Nessus, FalconGaze SecureTower. Дополнительное лицензионное ПО: MS Visual C++, True Crypt v 7.2, VMware Horizon Agent v 7.0.0., Oracle VM VirtualBox, Java 8

Лаборатория технической защиты информации, оснащенная: лабораторные столы 12 шт., стулья 32 шт., стол и стул для преподавателя, стеллаж для приборов - 1 шт., доска маркерная 1 шт., мультимедийный проектор, компьютерные столы 20 шт., персональные компьютеры - 20 шт. Программно-аппаратный комплекс оценки эффективности защиты речевой информации от утечки по акустическому и виброакустическому каналам «Смарт-АВ» 1 шт., средство активной защиты информации от утечки информации за счет побочных электромагнитных излучений и наводок «Соната-Р3.1» 1 шт., система виброакустической и акустической защиты «Вуаль» 1 шт. в составе: вибропреобразователи оконные ВПО-ВЛ 2 шт., вибропреобразователи оконные ВПС-ВЛ с дюбелем 2 шт., вибропреобразователи для коммуникаций ВПТ-ВЛ 2 шт., вибропреобразователи для рам ВПР-ВЛ 2 шт., преобразователи акустические ПА-ВЛ (R-150 Ом) 2 шт.;

Лаборатория программно-аппаратных средств обеспечения информационной безопасности, оснащенная: учебные столы 22 шт., стулья 22 шт., стол для преподавателя 1 шт., стул для преподавателя 1 шт., доска маркерная 1 шт., мультимедийный проектор 1 шт., экран 1 шт., персональные компьютеры 22 шт. Лаборатория оснащена антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, средствами сканирования защищенности компьютерных сетей, устройствами чтения смарт-карт и радиометок, программно-аппаратными комплексами защиты информации, включая криптографические средства защиты информации. в том числе: аппаратно-программными модулями доверенной загрузки «Соболь» (версия 3.0, PCI-E) с идентификаторами Rutoken S (32 Кб) 15 шт., устройствами чтения смарт-карт и радиометок: PERCo-IR05.2 (5 шт.), PERCo-IR03.1B (10 шт.), Secret Net Studio 8 (комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования). Обучающее лицензионное ПО: Kaspersky Endpoint Security, Nessus, Hex-Rays Decompiler, OllyDbg 2.0. Дополнительное лицензионное ПО: MS SQL Server, MS Visual C++, True Crypt v 7.2;

Лаборатория защищенных автоматизированных систем, оснащенная: учебные столы 22 шт., стулья 22 шт., стол для преподавателя 1 шт., стул для преподавателя 1 шт., доска маркерная 1 шт., мультимедийный проектор 1 шт., персональные компьютеры 22 шт. Лаборатория оснащена аппаратно-программными средствами управления доступом к данным, шифрования, средствами дублирования и восстановления данных, средствами мониторинга состояния автоматизированных систем, источниками бесперебойного и аварийного питания, средствами контроля и управления доступом в помещения, охранной и пожарной сигнализацией, климатическим контролем, в том числе: Secret Net Studio 8 (комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования), аппаратно-программными модулями доверенной загрузки «Соболь» (версия 3.0, PCI-E) с идентификаторами Rutoken S (32 Кб) 15 шт., источниками бесперебойного и аварийного питания, средством контроля и управления доступом в помещение, охранной сигнализацией, пожарной сигнализацией, климатическим контролем. Обучающее лицензионное ПО: для дублирования и восстановления данных Cobian Backup 11, для мониторинга состояния автоматизированных систем AlienVault

OSSIM SIEM. Дополнительное лицензионное ПО: «ФИКС» (версия 2.0.2), «TERRIER» (версия 3.0), True Crypt v 7.2, Project Expert 7, MS Visual C++

Специализированный кабинет Интернет-технологий, оснащенный: компьютерный стол 33 шт., стулья 35 шт., стол для преподавателя 1 шт., экран 2 шт., сетевой терминал с нулевым клиентом LG 23CAV42K 32 шт., мультимедийный проектор 2 шт., маркерная доска 1 шт. Лицензионное ПО: Java 8, MS SQL Server, MS Visual C++, VMware Horizon Agent v 7.0.0., операционные системы семейства Linux, Windows, True Crypt v 7.2;

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная: учебные столы 30 шт., стулья 60 шт., проектор Full HD 1 шт., экран 1 шт., доска маркерная 1 шт., интерактивная доска, оборудование ВКС (видеоконференцсвязь), высокоскоростной доступ в Интернет, КонсультантПлюс, оборудованное ноутбуком место преподавателя с установленным офисным пакетом и набором необходимых для проведения исследований дополнительных аппаратных и программных средств, а также комплектом оборудования для печати.

Компьютерный класс, оборудованный: компьютерные столы 15 шт., стулья 17 шт., стол преподавателя 1 шт., облачный монитор 23 LG 14 шт., сетевой монитор: нулевой клиент Samsung NC 240 1 шт., UPS 1 шт., мультимедийный проектор 1 шт., экран 1 шт., маркерная доска 1 шт. Лицензионное ПО: MS Visual C++, True Crypt v 7.2, VMware Horizon Agent v 7.0.0, программное обеспечение NI LabView.

ВГУЭС имеет лаборатории и специально оборудованные кабинеты (классы, аудитории), обеспечивающие практическую подготовку в соответствии с реализуемой специализацией программы специалитета.

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

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

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

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

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

ВГУЭС обеспечен необходимым комплектом лицензионного программного обеспечения и сертифицированными программными и аппаратными средствами защиты информации, состав которых определяется в рабочих программах дисциплин (модулей).

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

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей).

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к

ограничениям их здоровья.

Финансовое обеспечение реализации программы специалитета осуществляется в объеме не ниже установленных Министерством образования и науки Российской Федерации базовых нормативных затрат на оказание государственной услуги в сфере образования для данного уровня образования и направления подготовки с учетом корректирующих коэффициентов, учитывающих специфику образовательных программ в соответствии с Методикой определения нормативных затрат на оказание государственных услуг по реализации образовательных программ высшего образования по специальностям (направлениям подготовки) и укрупненным группам специальностей (направлений подготовки), утвержденной приказом Министерства образования и науки Российской Федерации от 30 октября 2015 г. N 1272 (зарегистрирован Министерством юстиции Российской Федерации 30 ноября 2015 г., регистрационный N 39898).

2 Компетентностная модель выпускника

Результаты освоения ОПОП – компетенции выпускника, формируемые в процессе освоения ОПОП, отражены в компетентностной модели выпускника (далее – КМВ) по специальности. КМВ утверждена на заседании кафедры математики и моделирования, подписана заведующим кафедрой, является самостоятельным документом, составной частью ОПОП и прилагается к ней.

3 Учебный план

Учебный план, состоит из следующих структурных элементов: титульный лист, календарный учебный график, учебный план, таблица соответствия компетенций блокам и дисциплинам учебного плана.

4 Рабочие программы дисциплин, включая ФОС

В состав ОПОП входят рабочие программы всех учебных дисциплин как базовой, так и вариативной частей учебного плана, включая дисциплины по выбору студента. Рабочие программы дисциплин, включая фонды оценочных средств, представлены в ОПОП в соответствии с учебным планом по специальности 10.05.03 Информационная безопасность автоматизированных систем.

5 Программы практик, включая фонды оценочных средств

Программы практик, а также фонды оценочных средств по практикам разрабатываются, утверждаются и размещаются в соответствии с требованиями локального акта. Утвержденный вариант прилагается к ОПОП. Программы практик выполнены на основе Приказа Минобрнауки России от 27.11.2015 № 1383 «Об утверждении Положения о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования» (Зарегистрировано в Минюсте России 18.12.2015 N 40168).

В соответствии с учебным планом по специальности предусмотрены следующие виды практик:

Учебная практика по развитию социально-профессиональных умений и навыков

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

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

Производственная практика по получению профессиональных умений и опыта профессиональной деятельности

Производственная научно-исследовательская практика (НИР)

Производственная преддипломная практика.

6 Программа государственной итоговой аттестации

Государственная итоговая аттестация включает защиту выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

Программа государственной итоговой аттестации, включая перечень тем выпускных квалификационных работ, а также фонды оценочных средств разрабатываются, утверждаются и размещаются в соответствии с требованиями локального акта. Утвержденный вариант прилагается к ОПОП.

7 Договоры о базах практик

(договоры о комплексном сотрудничестве с организациями)

К ОПОП прилагаются договоры о комплексном сотрудничестве с организациями, деятельность которых соответствует профессиональным компетенциям, осваиваемым студентами в рамках ОПОП. Договоры о базах практик заключены с: Приморским отделением № 8635 ОАО «Сбербанк России», ПАО ВТБ, ОАО «Дальневосточный центр судостроения и судоремонта», ООО «ФарПост», Территориальный орган Федеральной службы государственной статистики по Приморскому краю, ООО «Ронда Софтваре», ПАО «Владивостокский морской торговый порт», АО «Международный аэропорт «Владивосток», Администрация Приморского края, ООО «Софус», АКБ «Приморье», ПАО «Арсеньевская авиационная компания «Прогресс», Приморское УФАС России, ПАО «Дальприбор», ПАО Банк «Открытие», АО «Дальневосточная распределительная компания».

8 Другие методические материалы по дисциплинам

К ОПОП прилагаются все учебно-методические материалы, разработанные по дисциплинам учебного плана.