Автономное образовательное учреждение
высшего профессионального образования Курской области
«Курская академия государственной и муниципальной службы»
(Академия госслужбы)

ПРИНЯТО

Решением Ученого совета

от «01» сентября 2015г.

Протокол № 6.

УТВЕРЖДАЮ

И.В. Анциферова

«01» сентября 2015г.

ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ

10.03.01 (090900) ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Курск 2015

1. Общие положения

1.1. Цель ООП

Основная образовательная программа бакалавриата, реализуемая Автономным образовательным учреждением высшего профессионального образования Курской области «Курская академия государственной и муниципальной службы» (Академия госслужбы) по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «бакалавр») представляет собой систему документов, разработанную и утвержденную Академией госслужбы на основе Федерального государственного образовательного стандарта высшего образования по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «бакалавр») и рекомендованной примерной образовательной программы, с учетом потребностей рынка труда в регионе.

ООП регламентирует цели, ожидаемые результаты, содержание, условия и технологии реализации образовательного процесса, оценку качества подготовки выпускника по данной специальности и включает в себя учебный план, рабочие программы дисциплин и другие материалы, обеспечивающие качество подготовки обучающихся, а также программы практик, научно-исследовательской работы, график учебного процесса и программу государственной итоговой аттестации.

ООП ВО по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «бакалавр») предназначена для методического обеспечения учебного процесса и предполагает подготовку в области основ гуманитарных, социальных, экономических, математических и естественнонаучных знаний, предоставление образовательных услуг высшего образования, позволяющего выпускнику успешно работать в избранной сфере деятельности, обладать общекультурными, общепрофессиональными и профессиональными компетенциями, способствующими его социальной мобильности и востребованности на рынке труда.

ООП по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «бакалавр») ежегодно обновляется и рецензируется органами государственной власти и местного самоуправления.

1.2. Срок освоения ООП

Срок освоения ООП по очной форме обучения составляет 4 года.

1.3. Трудоемкость ООП

Трудоемкость ООП без факультативов составляет 240 зачетных единиц, 8968 академических часов, с факультативами 244 зачетных единиц, 9112 академических часов.

1.4. Требования к абитуриенту

Абитуриент должен иметь документ государственного образца о среднем общем образовании, среднем (полном) общем образовании или среднем профессиональном образовании, начальном профессиональном образовании при наличии записи о получении среднего (полного) общего образования, высшем образовании или высшем профессиональном образовании, владеть государственным языком Российской Федерации.

Абитуриент должен иметь свидетельства успешного прохождения вступительных испытаний (ЕГЭ) по трем предметам, являющимся вступительными испытаниями для данной ООП: русский язык, математика (профильная), физика.

2. Характеристика профессиональной деятельности выпускника

2.1. Область профессиональной деятельности выпускника

Область профессиональной деятельности выпускников, освоивших программу бакалавриата, включает: сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

2.2. Объекты профессиональной деятельности выпускника

Объектами профессиональной деятельности выпускников, освоивших программу бакалавриата, являются объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере; технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах; процессы управления информационной безопасностью защищаемых объектов.

2.3. Виды профессиональной деятельности выпускника

Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу бакалавриата:

эксплуатационная;

проектно-технологическая;

экспериментально-исследовательская;

организационно-управленческая.

2.4. Задачи профессиональной деятельности выпускника

Выпускник, освоивший программу бакалавриата, в соответствии с видом (видами) профессиональной деятельности, на который (которые) ориентирована программа бакалавриата, должен быть готов решать следующие профессиональные задачи:

эксплуатационная деятельность:

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;

администрирование подсистем информационной безопасности объекта;

проектно-технологическая деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

проведение проектных расчетов элементов систем обеспечения информационной безопасности;

участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов;

экспериментально-исследовательская деятельность:

сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

проведение экспериментов по заданной методике, обработка и анализ результатов;

проведение вычислительных экспериментов с использованием стандартных программных средств;

организационно-управленческая деятельность:

осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

организация работы малых коллективов исполнителей с учетом

требований защиты информации;

совершенствование системы управления информационной безопасностью;

изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны;

контроль эффективности реализации политики информационной безопасности объекта.

3. Компетенции, формируемые в результате освоения ООП

3.1. Матрица распределения компетенций

Результаты освоения ООП направления подготовки определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения и личные качества в соответствии с задачами профессиональной деятельности.

3.2. Характеристика компетенций

В результате освоения ООП направления подготовки Информационная безопасность выпускник должен обладать следующими компетенциями:

общекультурными компетенциями:

способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма (ОК-1);

способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм (ОК-2);

способностью уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия (ОК-3);

способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач (ОК-4);

способностью к кооперации с коллегами, работе в коллективе (ОК-5);

способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-6);

способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности,

готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-7);

способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления (ОК-8);

способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-9);

способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного (ОК-10);

способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства (ОК-11);

способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков (ОК-12);

способностью к самостоятельному применению методов физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, готовностью к достижению должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (ОК-13).

профессиональными компетенциями:

общепрофессиональными:

способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1);

способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2);

способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3);

способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4);

способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-5);

способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6);

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

способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-8);

эксплуатационная деятельность:

способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9);

способностью администрировать подсистемы информационной безопасности объекта (ПК-10);

способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-11);

проектно-технологическая деятельность:

способностью участвовать в разработке подсистемы управления информационной безопасностью (ПК-12);

способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности (ПК-13);

способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности (ПК-14);

способностью применять программные средства системного, прикладного и специального назначения (ПК-15);

способностью использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-16);

способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности (ПК-17);

способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-18);

экспериментально-исследовательская деятельность:

способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности (ПК-19);

способностью применять методы анализа изучаемых явлений, процессов и проектных решений (ПК-20);

способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-21);

способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов (ПК-22);

способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности (ПК-23);

способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-24);

организационно-управленческая деятельность:

способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПК-25);

способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью (ПК-26);

способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-27);

способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-28);

способностью участвовать в работах по реализации политики информационной безопасности (ПК-29);

способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК-30);

способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации (ПК-31);

способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПК-32);

способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю (ПК-33).

4. Документы, регламентирующие содержание и организацию образовательного процесса при реализации ООП

4.1. График учебного процесса.

График учебного процесса определяет последовательность реализации данной программы, включая теоретическое обучение, практики, промежуточную и итоговую аттестации, а также каникулы.

4.2. Рабочий учебный план

Рабочий учебный план разработан с учетом требований ФГОС ВПО и одобрен Ученым советом Академии госслужбы. Рабочий учебный план состоит из следующих циклов:

гуманитарный, социальный и экономический циклы;

естественнонаучный цикл;

профессиональный цикл;

и разделов:

физическая культура;

учебная и производственная практики и/или научно-исследовательская работа;

итоговая государственная аттестация.

Каждый учебный цикл имеет базовую (обязательную) часть и вариативную (профильную).

Структура программы бакалавриата:

«Гуманитарный, социальный и экономический цикл»

Базовая (обязательная) часть цикла предусматривает изучение следующих дисциплин: «Философия», «История», «Иностранный язык», «Экономика», «Правоведение», «Основы управленческой деятельности».

Вариативная (профильная) часть цикла предусматривает изучение следующих обязательных дисциплин: «Социология», «Русский язык и культура речи», «Логика»; дисциплин по выбору: «Национальная безопасность», «История Курского края», «Культурология», «Этика и этикет».

«Математический и естественнонаучный цикл»

Базовая (обязательная) часть цикла предусматривает изучение следующих дисциплин: «Математика», Теория вероятностей и математическая статистика», «Дискретная математика», «Физика», «Информатика», «Теория информации».

Вариативная (профильная) часть цикла предусматривает изучение следующих обязательных дисциплин: «Экономико-математические методы и модели», «Теория систем и системный анализ», «Основы математической логики»; дисциплин по выбору: «Экология», «Региональное природопользование», «Современная научная картина мира»,

«Математический анализ», «Численные методы», «Теория игр», «Средства и системы технического обеспечения обработки, хранения и передачи информации», «Радиоэлектроника», «Эконометрика», «Основы математического моделирования социально-экономических процессов».

«Профессиональный цикл»

Базовая (общепрофессиональная) часть цикла предусматривает изучение следующих дисциплин: «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Программно-аппаратные средства защиты информации», «Криптографические методы защиты информации», «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации», «Сети и системы передачи информации», «безопасность жизнедеятельности», «языки программирования», «Технологии и методы программирования», «Управление информационной безопасностью», «Документоведение», «Электротехника», «Электроника и схемотехника», «Информационные технологии».

Вариативная часть цикла предусматривает изучение следующих обязательных дисциплин: «Комплексная защита информации на предприятии», «Операционные системы», «Проектирование информационных систем», «Базы данных», «Введение в специальность», «Защита и обработка конфиденциальных документов», «Защита информационных процессов в компьютерных системах», «История и современные системы защиты информации в России», «Системы защиты информации в ведущих зарубежных странах», «Мультимедиа технологии», «Надежность информационных систем», «Системы поддержки принятия решений»; дисциплин по выбору: «Безопасность баз данных», «Безопасность операционных систем», «Web-программирование», «Web-дизайн», «Платежные системы», «Электронный бизнес», «Структура и основы деятельности предприятий различных форм собственности», «Нравственные основы профессиональной деятельности».

Вариативная часть дает возможность расширения и углубления знаний, умений и навыков, определенных содержанием базовых дисциплин и позволяет обучающимся получить углубленные знания и навыки для успешной профессиональной деятельности.

4.3. Рабочие программы дисциплин

По всем дисциплинам рабочего учебного плана ведущими преподавателями разрабатываются рабочие программы дисциплин с учетом компетентностного подхода, применением активных и интерактивных форм и методов обучения. Рабочие программы дисциплин обсуждаются на кафедрах академии госслужбы и утверждаются на Межкафедральном учебно-методическом совете. Аннотации рабочих программ дисциплин

представлены на сайте образовательной организации. В структуре аннотации отражены цели освоения дисциплины, требования к результатам освоения и содержание дисциплины. Рабочие программы представлены в локальной