Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Комсомольский-на-Амуре государственный технический университет»

(ФГБОУ ВПО «КнАГТУ»)

У Т В Е Р Ж Д Е Н А

Первым проректором ФГБОУ ВПО «КнАГТУ»

_____ А.Р. Куделько

02 июня 2012

ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

высшего профессионального образования

Направление подготовки

090303 Информационная безопасность автоматизированных систем
(шифр) (наименование)

ФГОС ВПО программы утвержден приказом Минобрнауки России от 17.01.2011 № 60

Квалификация (степень) выпускника:	специалист
Нормативный срок обучения по очной форме:	5 лет
Форма обучения:	очная
Базовое образование:	среднее
Срок обучения:	5 лет
Технология обучения:	традиционная

Комсомольск-на-Амуре 2012

Содержание

1. Общие сведения о программе

«Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.»(Доктрина информационной безопасности Российской Федерации).

Актуальность подготовки специалистов по защите информации обусловлена повсеместным использованием информационных технологий. В настоящее время сложно представить себе предприятие не обрабатывающее конфиденциальную информацию о сотрудниках и контрагентах, не использующее сети Интернет и электронной-цифровой подписи. Специалист по защите информации должен владеть не только информационными технологиями, но и знаниями в области инженерно-технических методов защиты (охранная сигнализация, видеонаблюдение, контроль доступа и т.п.), знать толк в аппаратуре считывания информации, перехвата разговоров, разбираться в схемотехнике, микропроцессорной технике, электронике, то есть имеет представление о том, из чего состоят микросхемы, как собраны компьютеры.

Подготовка специалистов по защите информации по специальности 090303 «Информационная безопасность автоматизированных систем» направлена на укрепление государственной системы защиты информации и ориентирована на формирование в регионе, на предприятиях, в организациях штата компетентных сотрудников способных обеспечить конфиденциальность, целостность и доступность информации. Каждому студенту в процессе обучения оформляется допуск к сведениям составляющим государственную тайну, необходимый для прохождения практики на предприятиях города.

Нормативный срок освоения образовательной программы для очной формы обучения, включая каникулы, предоставляемые после прохождения итоговой государственной аттестации, составляет 5 лет. Трудоемкость программы равна 240 зачетным единицам. Одна зачетная единица соответствует 36 академическим часам.

Кроме того, юноши и девушки, обучающиеся по программе и годные по состоянию здоровья для службы в Вооруженных Силах, параллельно могут пройти обучение про программе подготовки офицеров запаса. В этом случае им, после защиты выпускной квалификационной работы и получения диплома специалиста по защите информации, присваивается воинское звание младшего офицера.

2. Профили(специализации) подготовки выпускников

Основной образовательной программой подготовки специалистов по защите информации по специальности 090303 «Информационная безопасность автоматизированных систем» предусмотрены следующие специализации выпускников:

1. Информационная безопасность распределенных информационных систем.

3. Характеристика профессиональной деятельности выпускников

3.1 Области профессиональной деятельности

Областью профессиональной деятельности специалистов по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем» являются сферы науки, техники и технологий, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере.

3.2 Объекты профессиональной деятельности

Объектами профессиональной деятельности специалистов по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем» являются

- автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащие 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.

3.3 Виды профессиональной деятельности

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».

3.4 Основные профессиональные задачи, подлежащие решению выпускниками, освоившими образовательную программу

Специалист по направлению подготовки (специальности) 090303 Информационная безопасность автоматизированных систем должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

1) 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;

2) 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;

3) 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;

4) 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;

5) 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.

4. Требования к результатам освоения образовательной программы

4.1 Требования федерального государственного образовательного стандарта (ФГОС ВПО)

Специалист по направлению подготовки (специальности) 090303 Информационная безопасность автоматизированных систем должен обладать следующими **общекультурными компетенциями(ОК)**:

- способностью действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма (**ОК-1**);
- способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики (**ОК-2**);
- способностью анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач (**ОК-3**);
- способностью понимать движущие силы и закономерности исторического процесса, роль личности в истории, политической организации общества, способностью уважительно и бережно относиться к историческому наследию, толерантно воспринимать социальные и культурные различия (**ОК-4**);
- способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (**ОК-5**);
- способностью к работе в коллективе, кооперации с коллегами, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (**ОК-6**);
- способностью логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично

представлять собственные и известные научные результаты, вести дискуссии (**ОК-7**);

- способностью к письменной и устной деловой коммуникации, к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков (**ОК-8**);
- способностью к логически-правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания (**ОК-9**);
- способностью самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой деятельности, развития социальных и профессиональных компетенций, изменения вида своей профессиональной деятельности (**ОК-10**);
- способностью к осуществлению воспитательной и образовательной деятельности (**ОК-11**);
- способностью самостоятельно применять методы физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, достижения должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (**ОК-12**).

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 документы 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, находить и принимать 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**).

Кроме того выпускник должен обладать компетенциями специализации:

- 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 в распределенных информационных системах (**ПСК-7.4**);
- способностью проводить аудит защищенности информационно-технологических ресурсов в распределенных информационных системах (**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**).

4.2 Региональные требования (требования работодателей)

Выпускник должен обладать следующими **профессиональными компетенциями, сформулированными работодателями (ПКР)**:

- способностью администрировать автоматизированные системы со специализированным программным обеспечением для работы с электронно-цифровой подписью (СБИС++, КриптоАРМ, CryptoPro CSP)(**ПКР-1**);
- способностью планировать, контролировать и выполнять работы связанные с проведением открытых аукционов в электронной форме в соответствии с ФЗ-94 на электронных торговых площадках(**ПКР-2**);
- способностью обеспечивать информационную безопасность в информационных системах персональных данных различных классов (**ПКР-3**);
- способностью организовывать работы по аттестации объектов информатизации на соответствие требованиям по защите информации(**ПКР-4**).