МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ
Первый проректор
_____
(подпись, расшифровка подписи)
«__» _____ 20__ г.

ПРОГРАММА

государственной итоговой аттестации выпускников по специальности

090303 «Информационная безопасность автоматизированных систем»
(код) (наименование направления подготовки, специальности)

Квалификация – специалист
(наименование квалификации, степени)

2015

Рабочая программа разработана, обсуждена и одобрена на заседании кафедры «Информационная безопасность автоматизированных систем»

Заведующий кафедрой _____ И.А. Трещев

«02» 02 2015 г.

СОГЛАСОВАНО

Начальник учебно-методического управления _____ М.Г. Некрасова

«17» 02 2015 г.

Декан факультета компьютерных технологий _____ В.П. Котляров

«03» 02 2015 г.

Рабочая программа рассмотрена, одобрена и рекомендована к использованию методической комиссией факультета компьютерных технологий

Председатель методической комиссии факультета/института _____ В.П. Котляров

«03» 02 2015 г.

Программа обсуждена и утверждена на Учебно-методическом совете университета, протокол № _____ от _____ .

1 Общие положения

1.1 Цель государственной итоговой аттестации

Целью государственной итоговой аттестации является установление уровня подготовки выпускника к выполнению профессиональных задач и соответствия его подготовки требованиям Федерального государственного образовательного стандарта высшего профессионального образования (ФГОС ВПО) и основной образовательной программы высшего профессионального образования (ООП ВПО), разработанной в Комсомольском-на-Амуре государственном техническом университете.

1.2Состав государственной итоговой аттестации

Государственная итоговая аттестации по направлению подготовки (специальности)

090303 «Информационная безопасность автоматизированных систем»

(код и наименование направления подготовки (специальности))

включает:

а) государственный экзамен;

б) защиту выпускной квалификационной работы.

1.3 Нормативная база итоговой аттестации

1.3.1 Итоговая аттестация осуществляется в соответствии с локальным нормативным документом университета **СТП 7.5-2 Итоговая аттестация. Положение**. В указанном документе определены и регламентированы:

- общие положения по итоговой аттестации;
- правила и порядок организации и процедура проведения итоговой государственной аттестации;
- обязанности и ответственность руководителя выпускной квалификационной работы
- результаты итоговой государственной аттестации;
- порядок апелляции итоговой государственной аттестации;
- документация по итоговой государственной аттестации.

1.3.2 Оформление выпускной квалификационной работы осуществляется в соответствии с требованиями РД 013-2012 Текстовые студенческие работы. Правила оформления.

2Характеристика выпускника

2.1 Квалификационная характеристика (требования)

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.

2.2 Виды профессиональной деятельности

Основной образовательной программой по направлению подготовки (специальности)

090303 «Информационная безопасность автоматизированных систем»

(код и наименование направления подготовки (специальности))

предусматривается подготовка выпускников к следующим видам профессиональной деятельности:

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

Специалист может адаптироваться к следующим видам смежной профессиональной деятельности:

- управленческо-хозяйственной;
- экспертно-консультационной;
- научно-методической;
- телекоммуникация и связь;
- промышленная электроника;
- правовой;
- научно-педагогической (по профилю специальности).

2.3 Задачи профессиональной деятельности

Основные свои профессиональные задачи специалист по защите информации решает в организациях обрабатывающих конфиденциальную информацию, а так же государственную тайну.

Задачами профессиональной деятельности выпускников - специалистов по защите информации являются:

	Содержание задач профессиональной деятельности
ЗПД1	разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем
ЗПД2	разработка политик информационной безопасности автоматизированных систем;
ЗПД3	контроль работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации
ЗПД4	организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем
ЗПД5	реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем
ЗПД6	администрирование подсистем информационной безопасности автоматизированных систем
ЗПД7	обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций

3 Требования к результатам освоения образовательной программы

3.1Квалификационные требования, необходимые для профессиональной деятельности

Дипломированный специалист должен:

- разрабатывать и исследовать модели информационно-технологических ресурсов в автоматизированных системах;
- разрабатывать модели угроз и модели нарушителя информационной безопасности в автоматизированных системах;
- проводить анализ рисков информационной безопасности в автоматизированных системах;
- разрабатывать и руководить разработкой политики безопасности в автоматизированных системах;
- проводить аудит защищенности информационно-технологических ресурсов в автоматизированных системах;
- проводить удаленное администрирование операционных систем в автоматизированных системах;
- проводить удаленное администрирование систем баз данных в автоматизированных системах;
- координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации;
- применять криптографические протоколы для передачи и хранения данных в автоматизированных системах;

3.2 Знания, умения, навыки, опыт деятельности

Требования к профессиональной подготовке выпускника обусловливаются задачами и содержанием его будущей деятельности по специальности «Информационная безопасность автоматизированных систем». В результате освоения образовательной программы студент должен:

знать	
З1	общие принципы построения и использования современных языков программирования высокого уровня
З2	принципы построения и функционирования, примеры реализаций современных операционных систем
З3	принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных
З4	способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации
З5	программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях
З6	содержание и способы реализации ныне действующей нормативно-правовой базы в

	сфере защиты информации; основные российские положения и стандарты, относящейся к обеспечению информационной безопасности автоматизированных систем.
уметь	
У1	работать с интегрированной средой разработки программного обеспечения
У2	использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем
У3	разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных
У4	проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы
У5	анализировать и оценивать угрозы информационной безопасности объекта
иметь опыт (навыки)	
Н1	разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования
Н2	навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры
Н3	навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев
Н4	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
Н5	навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей
Н6	навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности
Н7	методами и средствами технической защиты информации
Н8	методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
Н9	навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации.

3.3 Связь элементов итоговой аттестации и профессиональных задач

По результатам государственной итоговой аттестации проверятся степень освоения выпускником способности решать следующие задачи профессиональной деятельности:

Элементы государственной итоговой аттестации	**Задачи профессиональной деятельности**						
	ЗПД1	ЗПД2	ЗПД3	ЗПД4	ЗПД5	ЗПД6	ЗПД7
Государственный экзамен							
Информатика				З1			З2
Языки программирования					З1	У3	
Безопасность операционных систем		З2				Н3	У2
Безопасность систем баз данных				З3	Н4	З3	

Элементы государственной итоговой аттестации	Задачи профессиональной деятельности						
	ЗПД1	ЗПД2	ЗПД3	ЗПД4	ЗПД5	ЗПД6	ЗПД7
Техническая защита информации	Н2		З4				Н5
Программно-аппаратные средства обеспечения информационной безопасности			У4	У4	З5		З5
Комплексное обеспечение информационное безопасности автоматизированных систем	З6	У5					
Технология построения защищенных автоматизированных систем		Н8		Н6			
Выпускная квалификационная работа							
Введение	Н9						
Теоретическая глава		Н9					
Аналитическая глава	У5					Н8	
Проектная глава (прикладная)			Н7		У1	Н1	
Заключение				Н9			

4 Государственный экзамен

4.1 Состав государственного экзамена

В состав государственного квалификационного экзамена включаются основные вопросы по учебным дисциплинам:

- информатика;
- языки программирования;
- безопасность операционных систем;
- безопасность систем баз данных;
- техническая защита информации;
- программно-аппаратные средства обеспечения информационной безопасности;
- комплексное обеспечение информационное безопасности автоматизированных систем;
- технология построения защищенных автоматизированных систем.

Примерный перечень вопросов и литература по ним, представлены в Приложении А.

В Приложении Б представлены примеры типовых практических заданий (задач), выносимых на государственный экзамен.

Билет состоит из пяти теоретических вопросов по разным дисциплинам и одной задачи. Примеры экзаменационных билетов представлены в Приложении В.

4.2 Критерии оценки государственного экзамена

Результаты государственного экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

При оценке уровня профессиональной подготовленности по результатам государственного экзамена необходимо учитывать следующие критерии:

- знание учебного материала (учебных дисциплин);
- знание нормативно-законодательных актов и различных информационных источников;
- способность к абстрактному логическому мышлению;
- умение выделить проблемы;
- умение определять и расставлять приоритеты;
- умение аргументировать свою точку зрения.

Уровень знаний определяется следующими оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется студенту, глубоко и прочно усвоившему программный материал, исчерпывающе, грамотно и логически стройно его излагающему, в свете которого тесно увязывается теория с практикой. При этом студент не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами контроля знаний, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами решения практических задач.

Оценка «хорошо» выставляется студенту, твердо знающему программный материал, грамотно и по существу излагающего его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми приемами их решения.

Оценка «удовлетворительно» выставляется студенту, который имеет знания только основного материала, но не усвоил его детали, допускает неточности, недостаточно правильные формулировки, нарушения последовательности в изложении программного материала и испытывает трудности в выполнении практических заданий.

Оценка «неудовлетворительно» выставляется студенту, который не усвоил значительной части программного материала, допускает существенные ошибки, неуверенно, с большим затруднением решает практические задачи. Списывание (или использование недопустимых материалов) является основанием для получения оценки «неудовлетворительно».

5 Выпускная квалификационная работа

Выпускная квалификационная работа по специальности «Информационная безопасность автоматизированных систем» представляет собой законченную разработку, в которой должны быть изложены вопросы связанных с построением, исследованием и эксплуатацией систем и технологий обеспечения информационной безопасности автоматизированных систем.

5.1 Вид выпускной квалификационной работы

Выпускная квалификационная работа выполняется в виде дипломной работы.

5.2 Цель выполнения выпускной квалификационной работы и предъявляемые к ней требования

Выполнение выпускной квалификационной работы имеет своей целью:

- систематизацию, закрепление и углубление полученных теоретических и практических знаний по специальности;
- развитие навыков обобщения практических материалов, критической оценки теоретических положений и выработки своей точки зрения по рассматриваемой проблеме;
- развитие умения аргументировано излагать свои мысли и формулировать предложения;
- выявление у студентов творческих возможностей и готовности к практической деятельности.

К выпускной квалификационной работе предъявляются следующие основные требования:

- раскрытие актуальности темы, ее теоретической и практической значимости;
- правильное использование законодательных и нормативных актов, методических, учебных пособий, а также научных и других источников информации, их критическое осмысление, и оценка практических материалов по выбранной теме;
- эффективно решать актуальные проблемы, в том числе для предполагаемого работодателя-заказчика в сфере построения, исследования и эксплуатации систем и технологий обеспечения информационной безопасности автоматизированных систем;
- полное раскрытие темы выпускной квалификационной работы, аргументированное обоснование выводов и формулировка предложений, представляющих научный и практический интерес, с обязательным использованием практического материала;
- раскрытие способностей обеспечения систематизации и обобщения собранных по теме материалов, развития навыков самостоятельной работы при проведении научного исследования.

5.2 Примерная тематика и порядок утверждения тем выпускных квалификационных работ

При выборе темы необходимо учитывать ее актуальность в современных условиях, практическую значимость для организаций и предприятий, где были получены фактические материалы для подготовки выпускной работы. При выборе темы целесообразно руководствоваться опытом, накопленным при написании курсовых работ, подготовки рефератов и докладов для выступления на семинарах и практических занятиях, конференциях, что позволит обеспечить преемственность научных и практических интересов.

Название темы дипломной работы должно быть кратким, отражать основное содержание работы. В названии темы нужно указать объект и

инструментарий, на которые ориентирована работа. В работе следует применять новые технологии и современные методы.

Примерная тематика ВКР представлена в Приложении Г.

5.3 Структура выпускной квалификационной работ. Требования к ее содержанию

После выбора и утверждения темы ВКР студент приступает к составлению плана, который согласовывается с научным руководителем. Правильно составленный план работы является основой в подготовке работы. Он позволяет студенту систематизировать научный, источниковый и методологический материал, обеспечить последовательность его изложения. В процессе работы возможно уточнение плана (расширение отдельных разделов, пунктов или, наоборот, их сокращение). Все изменения в плане согласовываются с научным руководителем. Окончательный вариант плана работы утверждается научным руководителем.

Предлагаемая тематика ВКР охватывает широкий круг вопросов. Поэтому структура каждой работы может уточняться студентом совместно с научным руководителем и консультантом (если он назначен), исходя из интересов студента, степени проработанности данной темы в литературе, наличия информации и т.п. Однако в большинстве случаев выпускная работа имеет свою типовую структуру (см. табл.).

Исходя из рекомендуемой структуры ВКР, её объем (без учета приложений) должен составлять примерно 100 – 120 страниц машинописного текста. Текст ВКР делится на разделы, каждый из которых включает не менее двух подразделов.

Наименование составных частей ВКР	Примерный объем составных частей ВКР
Реферат	1 страница машинописного текста
Содержание	1страница машинописного текста
Введение	до 5% общего объема
Раздел 1	до 25% общего объема текста
Раздел 2	до 25% общего объема текста
Раздел 3	не менее 30% общего объёма текста
Экономическая часть работы или проекта	до 5% общего объема
Экологичность и безопасность работы или проекта	до 5% общего объема
Заключение	до 5% общего объема
Список использованных источников и литературы	не менее 60 наименований
Приложения	объем не ограничен
Итого	**100–120 страниц**

Весь материал, приводимый в ВКР, должен сопровождаться расчетами, иллюстративным материалом, выводами, рекомендациями автора.

Выпускная квалификационная работа должна быть выполнена на компьютере с использованием различных технологий, в том числе текстовых, графических, статистических и прочих редакторов.

5.4 Критерии оценки квалификационных (дипломных) работ

При оценке уровня профессиональной подготовленности по результатам защиты выпускной квалификационной работы необходимо учитывать следующие критерии:

- актуальность тематики и ее значимость;
- масштабность работы;
- реальность поставленных задач;
- характер проведенных расчетов;
- апробация результатов, подтвержденная документально;
- наличие опубликованных работ;
- наличие авторской позиции по тематике ВКР;
- качество доклада;
- качество и полнота ответов на вопросы.

«Отлично» выставляется за квалификационную работу, которая носит исследовательский характер, имеет грамотно изложенную теоретическую главу, глубокий анализ, критический разбор практической деятельности, логичное, последовательное изложение материала с соответствующими выводами и обоснованными предложениями. Она имеет положительные отзывы научного руководителя и рецензента. При ее защите студент-выпускник показывает глубокое знание вопросов темы, свободно оперирует данными исследования, вносит обоснованные предложения, а во время доклада использует наглядные пособия (таблицы, схемы, графики и т.п.) или раздаточный материал, легко отвечает на поставленные вопросы.

«Хорошо» выставляется за квалификационную работу, которая носит исследовательский характер, имеет грамотно изложенную теоретическую главу, в ней представлены достаточно подробный анализ и критический разбор практической деятельности, последовательное изложение материала с соответствующими выводами, однако с не вполне обоснованными предложениями. Она имеет положительный отзыв научного руководителя и рецензента. При ее защите студент-выпускник показывает знание вопросов темы, оперирует данными исследования, вносит предложения по теме исследования, во время доклада использует наглядные пособия (таблицы, схемы, графики и т.п.) или раздаточный материал, без особых затруднений отвечает на поставленные вопросы.

«Удовлетворительно» выставляется за квалификационную работу, которая носит исследовательский характер, имеет теоретическую главу, базируется на практическом материале, но имеет поверхностный анализ и недостаточно критический разбор, в ней просматривается

непоследовательность изложения материала, представлены необоснованные предложения. В отзывах рецензентов имеются замечания по содержанию работы и методике анализа. При ее защите студент-выпускник проявляет неуверенность, показывает слабое знание вопросов темы, не всегда дает исчерпывающие аргументированные ответы на заданные вопросы.

«Неудовлетворительно» выставляется за квалификационную работу, которая не носит исследовательского характера, не имеет анализа, не отвечает требованиям, изложенным в методических указаниях кафедры. В работе нет выводов либо они носят декларативный характер. В отзывах научного руководителя и рецензента имеются критические замечания. При защите квалификационной работы студент-выпускник затрудняется отвечать на поставленные вопросы по ее теме, не знает теории вопроса, при ответе допускает существенные ошибки. К защите не подготовлены наглядные пособия и раздаточный материал.

ПРИЛОЖЕНИЕ А
(обязательное)

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ГОСУДАРСТВЕННОМУ ЭКЗАМЕНУ

Раздел 1
Вопросы по дисциплине «ИНФОРМАТИКА»

1 Охарактеризовать десятичную, двоичную, шестнадцатеричную системы счисления. Указать правила взаимного перевода. Представление чисел в памяти ЭВМ.

2 Дать понятие прямого, обратного и дополнительного кода в двоичной системе счисления. Сложение и вычитание целых чисел в двоичной системе счисления. Логические операции над двоичными числами.

3 Перечислить поколения ЭВМ и охарактеризовать их с точки зрения элементарной базы. Классификация Флинна.

4 Дать понятие информации. Проведите общую характеристику процессов сбора, передачи, обработки и накопления информации. Определите понятия конфиденциальность, целостность, доступность.

5 Указать состав программного и аппаратного обеспечения современного компьютера. Дать понятие об операционной системе, о трансляторе, интерпретаторе, прикладной программе. Наиболее распространенные виды прикладного программного обеспечения.

6 Охарактеризовать файловую систему современного компьютера. Дать понятие файла, каталога, жесткой ссылки, мягкой ссылки. Перечислить часто используемые файловые системы в современных операционных системах. Перечислить основные типы файлов.

7 Перечислить этапы решения задачи на компьютере. Дать понятие алгоритма. Свойства алгоритма. Способы записи алгоритма. Алгоритмическая сложность.

8 Охарактеризовать язык блок-схем – как способ записи алгоритма. Перечислите основные типы блоков. Перечислите основные типы алгоритмов и способы их записи на языке блок-схем. Приведите пример алгоритма описанного в виде блок-схемы.

9 Дать понятие об архитектуре ЭВМ. Назвать принципы фон Неймановской архитектуры. Архитектуры отличные от фон Неймановской.

10 Охарактеризовать оперативную память компьютера. Дать понятие бита, байта, слова, двойного слова, учетверенного слова. Понятие адреса байта и слова. Принципы отладки программного обеспечения.

11 Дать понятие о языке Ассемблера. Этапы разработки программы на ассемблере. Адресация в реальном и защищенном режиме работы микропроцессора.

12 Классификация языков программирования. Современные языки программирования. Языки программирования для параллельных архитектур.

Список основной литературы

1 Челухин, В. А. Информатика и защита информации: Учеб. пособие / В. А Челухин. – Комсомольск-на-Амуре: ГОУВПО «КнАГТУ», 2010. – 198 с.

2 Агальцов, В. П. Информатика для экономистов: [учебник] / В. П. Агальцов, В. М. Титов – М.: Форум, 2011. - 447 с.

3 Алехина, Г. В. Информатика. Базовый курс : учебное пособие / Под ред. Г. В. Алехиной. - 2-е изд., доп. и перераб. – М.: Маркет ДС Корпорейшн, 2010. - 731 с.

4 Квинт, И. HTML и CSS на 100%./ И.Квинт – Спбю: Питер, 2008. -352 с.:ил. – (Серия «На 100%»).

Список дополнительной литературы

1 Гуда, А. Н., Колесников В. И. Информатика и программирование: компьютерный практикум - М.: Дашков и К, 2010. - 240 с.

2 Васильков, А. В. Информационные системы и их безопасность / А. В. Васильков, А. А. Васильков, И. А. Васильков - М.: Форум, 2010. - 525 с.

Раздел 2
Вопросы по дисциплине «ЯЗЫКИ ПРОГРАММИРОВАНИЯ»

1 Какие технологии программирования Вы знаете? Охарактеризуйте одну из них, приведите примеры.(COM,COM+,DCOM,CORBA,OLE,ActiveX и др.)

2 Какие шаги входят в процесс управления рисками? Охарактеризуйте их.

3 Что понимается под тестированием и отладкой программ? Какие методы тестирования Вы знаете? Какие методы отладки вы знаете? Приведите их.

4 Приведите основные понятия объектно-ориентированного программирования. Приведите примеры реализации.

5 Приведите основные положения Computer-Aided System Engineering (CASE) технологии. CASE средства для разработки программного обеспечения.

6 Что понимается под структурой данных, абстракцией данных? Приведите структуры данных, которые Вы знаете, охарактеризуйте их.

7 Приведите алгоритмы для работы со списковыми структурами.

8 Какие структуры данных относятся к линейным структурам данных переменного типа? Перечислите их, дайте им характеристику, способы реализации.

9 Раскройте понятие – «сортировка». Рассмотрите любые два алгоритма на выбор из списка: подсчета, Шелла, быстрая, пирамидальная, пузырьковая, выбором, вставками.

10 Раскройте понятие – структура данных типа дерево. Рассмотрите двоичные деревья, деревья поиска, сбалансированных деревья, построение деревьев, алгоритмы обхода деревьев.

11 Раскройте понятие – «поиск». Рассмотрите любой алгоритм на выбор из списка: последовательный перебор, перебор с возвратом, двоичный поиск, блочный поиск, поиск по двоичному дереву, поиск с использованием прямого доступа к данным.

12 Охарактеризуйте структуру данных – граф. Рассмотрите любой алгоритм на выбор из списка: обход графа в длину и в ширину, построение минимального остовного дерева нагруженного графа, парасочетания, проверка ацикличности графа.

Список основной литературы

1 Колисниченко, Д. Rootkits под Windows. Теория и практика программирования "шапок-невидимок"; М.: Наука и техника, 2012. - 320 с.

2 Голицына О. Л., Попов И. И. Программирование на языках высокого уровня; Форум - Москва, 2010. - 496 с.

3 Гуриков С. Р. Введение в программирование на языке Microsoft Visual Basic .NET; ДРОФА - , 2010. - 528 с.

4 Синицын С. В., Михайлов А. С., Хлытчиев О. И. Программирование на языке высокого уровня; Академия - Москва, 2010. - 400 с.

Список дополнительной литературы

1 Мещеряков Р.В. Структуры данных и прикладные алгоритмы. Учебное пособие. -Томск: ТМЦДО, 2002.-230 с.

2 Мещеряков Р.В. Методы программирования. Часть 1. Методические указания к лабораторным работам по курсу «Методы программирования» для студентов специальности 090105. Часть 1. Томск.: ТУСУР, 2005. – 273 с.

Раздел 3
Вопросы по дисциплине «Безопасность операционных систем»

1 Что такое «режим прерывания» и его роль в современных операционных системах? Как происходит смена задачи.

2 Дайте следующие определения и назначение систем: универсальная операционная система (ОС), специализированная ОС, диалоговая ОС, пакетная ОС, кластерная ОС, ОС с разделением времени, ОС реального времени.

3 Поясните следующие свойства операционных систем: детерминированность, перемещаемость, гибкость, расширяемость, ясность, реентерабельность.

4 Известны четыре типа ресурсов, которыми управляет операционная система. Назовите их и приведите (кратко) особенности управления ими.

5 Что такое «процесс», «поток», «нить» в современных операционных системах. Каким образом происходит перевод процесса из одного состояния в другое?

6 Назовите основные функциональные отличия ОЗУ от других типов памяти. Зачем используются различные способы распределения памяти (страничное, сегментное, разделами и т.д.) и их особенности?

7 Можно выделить три основных этапа при планировании защиты операционной системы. В чем их суть и сложности?

8 Что такое «политика безопасности»? Какие существуют категории и требования безопасности?

9 Какие механизмы диспетчеризации процессов, потоков Вы знаете? Охарактеризуйте их.

10 Раскройте понятия – проблема взаимного доступа к памяти, взаимные блокировки, гонки приоритетов. Механизмы синхронизации потоков и процессов в современных операционных системах.

11 Существуют два вида контроля доступа: мандатный и произвольный. Чем они характерны, их основные особенности? Механизм контроля доступа прикладного уровня разбит на два компонента. Какие и зачем?

12 Охарактеризуйте архитектуры современных операционных систем, приведите примеры.

Список основной литературы

1 Партыка, Т. Л. Операционные системы, среды и оболочки [Текст] : учебное пособие / Т. Л. Партыка, И. И. Попов. – 3-е изд., перераб. и доп. – М. : Форум, 2010. – 544 с.

2 С. В. Назаров. Операционные системы: Практикум: учебное пособие/с.В.Назаров, Л.П.Гудыно, А.А.Кириченко.- М.: КНОРУС, 2012.- 376 с.

3 С. В. Назаров. " Операционные среды, системы и оболочки. Основы структурной и функциональной организации " - М.: КУДИЦ-Пресс, 2007, 504 с.

4 С. В. Назаров, Л. П. Гудыно, А. А. Кириченко. " Операционные системы. Практикум для бакалавров " - М.: КноРус, 2012, 376 с.

5 Э. Таненбаум, Д. Уэзеролл. " Компьютерные сети " – СПб.: Питер, 2012, 960 с.

6 Андрианов, В.И.; Соколов, А.В. Устройства для защиты объектов и информации; СПб: Полигон; Издание 2-е, перераб. и доп., 2012. - 256 с.

Список дополнительной литературы

1 Илюшкин В.А. Теоретические основы конструирования и надежности ЭВС. Раздел 2. Учебное пособие. - Томск: ТМЦДО, 2003.-101 с.

2 Илюшкин В.А. Теоретические основы конструирования и надежности ЭВС. Раздел 1. Учебное пособие. - Томск: ТМЦДО, 2003.-103 с.

3 Дейтел Х.М., Дейтел П.Дж., Чофнес Д.Р. Операционные системы. Основы и принципы: Третье издание. Пер. с англ. М.: ООО «Бином-Пресс», 2006 г., 1024 с.

4 А. А. Безбогов, А. В. Яковлев, Ю. Ф. Мартемьянов. Безопасность операционных систем. М.: Гелиос АРВ, 2008.

5 Колисниченко Д.Н. Linux. Полное руководство. М.: Изд-во "Наука и технологии", 2006. 777с.

6 Побегайло А.П. Системное программирование в Windows. СПб.: БХВ-Петербург, 2006.

Раздел 4
Вопросы по дисциплине «БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ»

1 Что представляет собой реляционная модель данных? Дайте определения понятиям: отношение, кортеж, домен, операции реляционной алгебры.

2 Почему необходимо проводить нормализацию базы данных? Поясните на примерах процесс нормализации.

3 Поясните, что представляет структурная, языковая, ссылочная и семантическая целостность на уровне отношений и доменов.

4 Какие команды SQL, и каким образом обеспечивают языковую поддержку безопасности баз данных?

5 Охарактеризуйте основные положения технологии Integrated DEFinition (IDEF).

6 Какие проблемы информационной безопасности необходимо решить при распределенной обработке данных, и тиражировании?

7 Дайте определение транзакции. Какими свойствами она обладает? Поясните принципы восстановления после мягкого и жесткого сбоев.

8 Охарактеризуйте типовые архитектуры клиент/сервер.

9 Перечислите функции администратора базы данных. Что входит в понятие «Аксиомы безопасности базы данных»?

10 Каким образом курсоры можно использовать как механизм обеспечения безопасности?

11 Как обеспечивается организация аудита событий в базе данных и какие средства контроля целостности информации в них применяются?

12 Приведите примеры манипулирования данными и выбора данных в SQL.

Список основной литературы

1 Дейт, К. Дж. Введение в системы баз данных, 8-е издание / К. Дж. Дейт. – СПб.: Издательский дом «Вильямс», 2010. – 848 с.

2 Диго, С. М. Проектирование и использование баз данных : учеб. пособие / С. М. Диго. – М.: Финансы и статистика, 2011. – 208 с.

3 Мейер, Д. Теория реляционных баз данных / Д. Мейер. – М.: Наука, 2011. – 608 с.

Список дополнительной литературы

1 Горев, А. Эффективная работа с СУБД. / А. Горев, Р. Ахаян, С. Макашарипов. – СПб.: Питер, 2007. – 704 с.

2 Жилинский, А. Самоучитель Microsoft SQL Server 2005 / А. Жилинский. – М: Либроком, 2009. – 217 с.

3 Рассел, Д. Реляционная база данных / Д. Рассел. – М: Наука, 2012. – 102 с.

Раздел 5
Вопросы по дисциплине «Техническая защита информации»

1 Какое определение имеют технические каналы утечки информации, технические средства приема, обработки, хранения и передачи информации, вспомогательные технические средства и системы? Какими характеристиками обладают каналы утечки информации и указанные средства?

2 Какие существуют средства перехвата акустических сигналов по воздушным и виброакустическим каналам?

3 Какие существуют способы перехвата акустических сигналов по электроакустическим и оптико-электронным каналам утечки информации.

4 Какова физическая природа паразитных связей между проводными линиями передачи информации? Какие виды паразитных связей имеют место в реальной электронной аппаратуре?

5 Какими демаскирующими признаками характеризуются объекты технической разведки в видимом и инфракрасном диапазонах электромагнитного спектра?

6 Какие существуют инженерно-технические средства обеспечения безопасности объектов?

7 Какие существуют методы и средства защиты электронных устройств и объектов от побочных электромагнитных излучений?

8 Какими способами можно защитить информацию от утечки при передаче ее по слаботочным линиям?

9 Какими демаскирующими признаками характеризуются радиоэлектронные средства обработки и передачи информации?

10 Какие существуют средства обеспечения информационной безопасности в компьютерных системах?

11 Какие существуют способы контроля и прослушивания телефонных каналов связи?

12 Какими демаскирующими признаками характеризуются радиоэлектронные средства и акустические закладки?

Список основной литературы

1 Ворона В. А., Тихонов В. А. Технические средства наблюдения в охране объектов; Горячая Линия - Телеком - , 2011. - 184 с.

2 Рассел Джесси Технические средства защиты авторских прав; Книга по Требованию - Москва, 2012. - 563 с.

Список дополнительной литературы

1 Зайцев А.П. Технические средства обеспечения информационной безопасности. Часть 1. Технические каналы утечки информации. Учебное пособие.- Издание 2-ое переработанное и дополненное. - Томск: В-Спектр, 2007.-200 с.

2 Зайцев А.П. Технические средства обеспечения информационной безопасности. Часть 2. Средства защиты информации от утечки по техническим каналам. Учебное пособие.- Издание 2-ое переработанное и дополненное. - Томск: В-Спектр, 2007.-280 с.

3 Зайцев А.П., Шелупанов А.А. Технические средства и методы защиты информации. Лабораторный практикум. Гриф СибРОУМО. - Томск: В-Спектр, 2007.-120с.

4 Зайцев А.П., Шелупанов А.А. Практикум по техническим средствам и методам защиты информации. Учебное пособие. Гриф СибРОУМО. Издание 2-е, исправленное и дополненное. - Томск: Изд-во "В-Спектр", 2006.-128с.

5 Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Техническая защита информации. Учебник для ВУЗов. Гриф УМО ВУЗов России. 5-е изд. – М.: Горячая линия – Телеком, 2009. – 616 с.

Раздел 6
Вопросы по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности»

1 Состав программно-аппаратного комплекса «Secret Net».

2 Методы создания безопасных систем обработки информации.

3 Рассказать о типичной структуре диспетчера доступа комплексной системы защиты информации.

4 Рассказать о подсистеме управления доступом, реализованной в программно-аппаратном комплексе «SecretNet».

5 Рассказать о подсистеме обеспечения целостности, реализованной в программно-аппаратном комплексе «SecretNet»+«Соболь».

6 Способы встраивания средств защиты в программное обеспечение на примере HASP ключей.

7 Существует два типа вредоносных программ. Охарактеризуйте их.

8 Раскрыть понятие «монитор безопасности объектов».

9 Раскрыть понятие «монитор безопасности субъектов».

10 Устройства хранения ключевой информации. Основные характеристики.

11 Раскрыть понятие «изолированная программная среда». Охарактеризовать ИПС в программно-аппаратном комплексе «SecretNet».

12 Базовая теорема «изолированной программной среды».

Список основной литературы

1 Платонов В. В. Программно-аппаратные средства защиты информации; Академия - Москва, 2013. - 336 с.

2 Колесниченко Олег , Шишигин Игорь , Соломенчук Валентин Аппаратные средства PC; БХВ-Петербург - Москва, 2010. - 800 с.

3 Айден, К.; Колесниченко, О.; Крамер, М. Аппаратные средства PC; Санкт-Петербург: BHV-Санкт-Петербург; Издание 2-е, перераб. - Москва, 1998. - 608 с.

4 Борисов М. А., Заводцев И. В., Чижов И. В. Основы программно-аппаратной защиты информации; Либроком - Москва, 2013. - 376 с.

Список дополнительной литературы

1 Духан Е. И. Применение программно-аппаратных средств защиты компьютерной информации: учеб. пособие / Е. И. Духан, И. Н. Синадский, Д. А. Хорьков. – Екатеринбург: ГОУ ВПО УГТУ-УПИ, 2007. – 174 с.

2 Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2005. — 256 с.

3 Зайцев А.П. Программно-аппаратные средства обеспечения информационной безопасности. Раздел 1. Учебное пособие. Гриф СибРОУМО. 3-е изд., перер. и доп.- Томск: В-Спектр, 2009. - 144 с.

4 Зайцев А.П. Программно-аппаратные средства обеспечения информационной безопасности. Раздел 2. Учебное пособие. Гриф СибРОУМО. 3-е изд., перер. и доп.- Томск: В-Спектр, 2009. - 118 с.

Раздел 7
Вопросы по дисциплине «Комплексное обеспечение информационное безопасности автоматизированных систем»

1 Перечислите стадии и этапы проектирования комплексной системы обеспечения информационной безопасности.

2 Приведите типовую структуру Комплексной системы обеспечения информационной безопасности от несанкционированного доступа.

3 Приведите последовательность работ при проектировании комплексной системы обеспечения информационной безопасности от несанкционированного доступа.

4 Что включает в себя предпроектное исследование системы безопасности.

5 Приведите основы игровых моделей принятия решений системы информационной безопасности, анализ информированности в них.

6 Приведите основы метода экспертных структурных опросников для оценки качества комплексной системы обеспечения информационной безопасности.

7 Каковы элементы аттестации по требованиям безопасности.

8 Приведите основные положения концепции комплексной системы обеспечения информационной безопасности.

9 Перечислите требования к эксплуатационной документации комплексной системы обеспечения информационной безопасности.

10 Что включает в себя организационное управление защитой информации? Перечислите организационно-функциональные задачи службы безопасности.

11 Как производится моделирование угроз информационной безопасности и защиты от них?

12 Что включает в себя мониторинг и контроль состояния окружающей среды?

Список обязательной литературы

1 Гришина Н. В. Комплексная система защиты информации на предприятии; Форум - Москва, 2010. - 240 с.

2 Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: ИД. "Форум" : ИНФРА - М. 2013-592с.

3 Галатенко, В.А. Стандарты информационной безопасности; М.: Интуит. ру Интернет-Университет Информационных Технологий, **2013.** - 328 с.

4 Шишов О. В. Современные технологии и технические средства информатизации; Инфра-М - , 2012. - 464 с.

5 Мезенцев К. Н. Автоматизированные информационные системы; Академия - Москва, 2013. - 176 с.

Список дополнительной литературы

1 Девянин П.К. Модели безопасности компьютерных систем: учебное пособие для вузов/ П. Н. Девянин. - М.: Академия, 2005. - 142с.

2 Основы информационной безопасности. Учебное пособие для ВУЗов // Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. – М.: Горячая линия – Телеком, 2006. – 544с.

3 Мещеряков Р.В., Шелупанов А.А. Комплексное обеспечение информационной безопасности автоматизированных систем. – Томск: Изд-во В-Спектр, 2007. –350с.

ПРИЛОЖЕНИЕ Б
(обязательное)
Примеры типовых практических заданий (задач), выносимых на государственный экзамен

Задача 1

Для заданных входных данных продемонстрировать алгоритм Шелла.

Задача 2

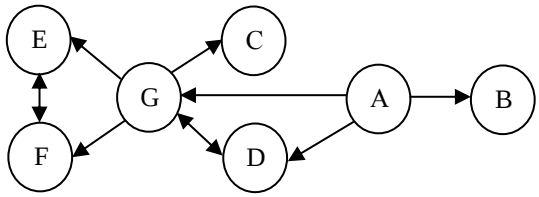
Задан файл, состоящий из 10 000 чисел. Вывести на экран наименьшие 20 чисел из этого файла.

Задача 3

Используя существующую базу данных в MS SQL Server, создать нового пользователя и задать ему разные права доступа к различным таблицам.

Задача 4

Из данного набора функциональных зависимостей удалить все избыточные, используя аксиомы вывода:



Задача 5

При измерении ПЭМИ (на расстоянии 1 м), от видеосистемы на частоте 189МГц, был обнаружен информативный сигнал. Оператор снял с приемника показания (57,3 Дб). После отключении тест программы приемник показал уровень напряженности поля 50,3Дб. Рассчитать $R_{\text{норм}}$ на заданной частоте. Коэффициент калибровки измерительной антенны составляет 20,3 Дб на частоте 189МГц.

Задача 6

Оператор исследует телефон на предмет утечки информативного сигнала по каналу АЭП. Результаты измерений приведены в таблице. Установить на каких частотах не выполняются нормы.

f (Гц)	$U_{\text{ш}}$ (V)	$U_{c+\text{ш}}$ (V)	U_c	Δ
250	0,0003	0,0004		
500	0,0001	0,00012		
1000	0,00009	0,00011		
2000	0,00008	0,000095		
4000	0,00015	0,00017		

Задача 7

Создайте в операционной системе Windows произвольную структуру каталогов, но при помощи дискреционной модели разграничения доступа сделайте каталог не доступный пользователям на исполнение.

Задача 8

Создайте в операционной системе Linux произвольную структуру каталогов, но при помощи дискреционной модели разграничения доступа сделайте каталог не доступный пользователям на запись.

Задача 9

Сколько существует различных наборов значений логических переменных x1, x2, x3, x4, x5, y1, y2, y3, y4, y5, которые удовлетворяют всем перечисленным ниже условиям?

(x1→x2)/\(x2→x3)/\(x3→x4)/\(x4→x5)=1

(y1→y2)/\(y2→y3)/\(y3→y4)/\(y4→y5)=1

x1\/y1 =1

Задача 10

Определите, какое число будет напечатано в результате выполнения следующего алгоритма:

```
#include<stdio.h>
int F(int x)
{
  return 9*(x+19)*(x-19)+1;
}
void main()
{
  int a, b, t, M, R;
  a = -20;  b = 20;
 M = a; R = F(a);
   for (t=a; t<=b; t++){
     if (F(t)<R) {
       M = t; R = F(t);
     }
  }
  printf("%d", M);
}
```

ПРИЛОЖЕНИЕ В
(обязательное)
Примеры структуры и состава экзаменационных билетов

Билет № 1

1 Указать состав программного и аппаратного обеспечения современного компьютера. Дать понятие об операционной системе, о трансляторе, интерпретаторе, прикладной программе. Наиболее распространенные виды прикладного программного обеспечения.

2 Приведите основные понятия объектно-ориентированного программирования. Приведите примеры реализации.

3 Можно выделить три основных этапа при планировании защиты операционной системы. В чем их суть и сложности?

4 Что представляет собой реляционная модель данных? Дайте определения понятиям: отношение, кортеж, домен, операции реляционной алгебры.

5 Какими демаскирующими признаками характеризуются радиоэлектронные средства обработки и передачи информации

6 Сколько существует различных наборов значений логических переменных x1, x2, x3, x4, x5, y1, y2, y3, y4, y5, которые удовлетворяют всем перечисленным ниже условиям?

$(x1 \rightarrow x2) \wedge (x2 \rightarrow x3) \wedge (x3 \rightarrow x4) \wedge (x4 \rightarrow x5) = 1$

$(y1 \rightarrow y2) \wedge (y2 \rightarrow y3) \wedge (y3 \rightarrow y4) \wedge (y4 \rightarrow y5) = 1$

$x1 \vee y1 = 1$

ПРИЛОЖЕНИЕ Г
(обязательное)
Примерная тематика ВКР

1. Аттестация объекта информатизации на соответствие требованиям по защите информации для (на материалах конкретного предприятия).
2. Исследование … (наименование технического канала утечки информации) в (на материалах конкретного предприятия).
3. Аттестация ИСПДн класса …(указание класса) для (на материалах конкретного предприятия).
4. Комплексная система защиты информации (на материалах конкретного предприятия).
5. Выбор СЗИ (на материалах конкретного предприятия).
6. Исследование параметров (наименование технического канала утечки информации) (на материалах конкретного предприятия).
7. Проектирование защищенной автоматизированной системы (на материалах конкретного предприятия).
8. Управление рисками информационной безопасности на предприятии.
9. Разработка программного комплекса для расчета параметров защиты от утечки по каналу (наименование технического канала утечки информации).
10. Совершенствование системы защиты информации в соответствии с актуальными требованиями законодательства.
11. Обеспечение информационной безопасности распределенных информационных систем.
12. Создание и аттестация альтернативной измерительной площадки (на материалах конкретного предприятия).
13. Проектное управление информационной безопасностью.
14. Разработка программных комплексов защиты от НСД.
15. Разработка программно-аппаратных комплексов защиты от НСД.
16. Разработка программно-технических комплексов для удостоверяющих центров.
17. Разработка программного обеспечения для автоматизации процесса аудита информационной безопасности.
18. Разработка программно-технических комплексов для защиты от утечки по (наименование технического канала утечки информации).
19. Разработка системы контроля устранения выявленных в работе по информационной безопасности несоответствий (на материалах конкретного предприятия).
20. Разработка защищенных мобильных приложений.
21. Организация защищенного канала связи с использованием ГОСТ 28147-89.
22. Защита интеллектуальной собственности. Автоматизация формирования заявок на (патент, свидетельство о регистрации ПО и др.
23. Создание(модернизация) сервера в защищенном исполнении, в соответствии с требованиями по информационной безопасности.

24. Создание(модернизация) системы хранения данных в защищенном исполнении, в соответствии с требованиями по информационной безопасности.

25. Использование генетических алгоритмов в задачах защиты информации.

26. Создание(модернизация) средств контроля от утечки по (наименование технического канала утечки информации).

27. Выбор оптимальной структуры ПАСЗИ и ТСЗИ (на материалах конкретного предприятия).

28. Выбор оптимальной структуры средств контроля защищенности от утечек по техническим каналам, НСД для нужд лаборатории по аттестации ОИ.

29. Проектирование системы защиты информации (на материалах конкретного предприятия).

30. Разработка стратегического плана по развитию системы ЗИ (на материалах конкретного предприятия).

31. Разработка путей снижения рисков информационной безопасности (на материалах конкретного предприятия).

32. Разработка математических моделей для анализа защищенности информационной системы.

33. Разработка математических моделей для анализа защищенности информационной системы (на материалах конкретного предприятия).

34. Разработка системы управления информационной безопасностью (на материалах конкретного предприятия).

35. Криптоанализ отечественных и зарубежных алгоритмов шифрования.

36. Стеганографические алгоритмы сокрытия информации.

37. Оптимизация затрат на организацию и управление информационной безопасностью (на материалах конкретного предприятия).

38. Исследование защищенности сети предприятия (на материалах конкретного предприятия).

39. Разработка программного обеспечения для анализа исходных текстов приложений.

40. Особенности реализации угроз безопасность в ОС Windows или Unix.

41. Разработка программного обеспечения для имитации тестовых сигналов от различных устройств для проведения аттестации по требованиям информационной безопасности.

42. Разработка программного обеспечения для сопряжения (далее следует указание устройства, например R&S FSC3) с ПЭВМ и анализа полученных данных.

43. Разработка программного обеспечения для расчета опасных зон информативного сигнала по каналу ПЭМИ.

44. Исследование защищенной сети (на материалах конкретного предприятия) на наличие программно-аппаратных уязвимостей.

45. Исследование АЭП, возникающих в СВЧ зоне.

46. Исследование каналов ВЧО и ВЧН.

47. Оптимизация затрат на создание и аттестацию экранированной безэховой камеры.

48. Систематизация и исследование оконечных устройств пожаро-охранных сигнализаций на подверженность АЭП.

49. Исследование затуханий информативного сигнала в ВОЛС.

50. Разработка устройства перехвата информативных сигналов по (далее следует наименование технического канала утечки информации).

51. Исследование пассивных средств защиты от утечки по (далее следует наименование технического канала утечки информации).

52. Разработка частной модели угроз безопасности (на материалах конкретной организации).

53. Оптимизация затрат на создание помещения для ведения конфиденциальных переговоров (на материалах конкретного предприятия).

54. Исследование возможности автоматизированного перехода от одной модели разграничения доступа к другой.

55. Исследование подходов к проектированию системы защиты информации на предприятии.

56. Организация защиты траффика в территориально-распределенной локальной вычислительной сети с использованием систем защиты Континент.

57. Организация защиты траффика в территориально-распределенной локальной вычислительной сети с использованием систем защиты VipNet.

58. Математическое моделирование действий злоумышленника с использованием сетей Петри.

59. Оценка угроз безопасности с использованием системы уравнений Колмогорова.

60. Построение интегральной оценки возможности реализации угроз безопасности.

61. Использование эвристических оценок возможности реализации угроз безопасности.

62. Оценка подходов к управлению информационной безопасностью (на материалах конкретного предприятия).

63. Моделирование системы пропускного контроля с использованием нейронных сетей.

64. Использование геоинформационных технологий для позиционирования на местности с целью определения допустимых границ контролируемой зоны.

65. Создание системы контроля доступа на ОИ в защищенном исполнении.

66. Аттестация и контроль систем видео-конференций для обмена конфиденциальной информацией, на соответствие требованиям по защите информации.

67. Исследование возможности программно-математических воздействий на информацию защищенную (далее следует наименование криптографического алгоритма).

68. Криптоанализ на сверхвысокопроизводительных ЭВМ.

69. Исследование сложности криптоанализа (отечественных или зарубежных алгоритмов) с учетом выполнения на сверхвысокопроизводительных ЭВМ.

70. Криптоанализ в реальном времени.

71. Проектирование защищенных автоматизированных систем с учетом распределенной информационной системы и функционирования в условиях повышенной готовности.

72. Управление информационной безопасностью в системах массового обслуживания.

73. Создание и эксплуатация систем массового обслуживания с одноразовыми паролями.

74. Разработка системы защиты с учетом использования ресурсов сети Интернет.

75. Создание инновационных разработок для (обеспечения обороноспособности, безопасности личности).

76. Разработка систем мониторинга радио обстановки в реальном времени с учетом зашумленности канала.

77. Исследование возможности демодуляции информативного сигнала на нестандартных каналах утечки информации.

78. Проектирование защищенной вычислительной сети предприятия с учетом использования беспроводных каналов передачи информации.

79. Исследование защищенности операционных систем с учетом наличия программных закладок.

80. Исследование возможности автономного питания средств защиты и средств измерений в условиях длительной эксплуатации.

81. Разработка программного обеспечения для автоматизированного расчета сопротивления на объекте информатизации.

82. Разработка программно-аппаратных комплексов автоматизированной поверки оборудования используемого при проведении аттестации объектов информатизации.

83. Противодействие программно-математическим воздействиям на объект информатизации с использованием системы обнаружения вторжений.

84. Разработка программного обеспечения для автоматизации деятельности по учету и периодическому контролю оборудования и программного обеспечения лабораторий по аттестации объектов информатизации.

85. Таксономии уязвимостей.

86. Исследование и моделирование рефлексивной разведки с учетом многоступенчатости информационного обмена.

87. Разработка программного обеспечения для автоматизации проведения расчетов при аттестации объекта информатизации.

88. Разработка программного обеспечения для автоматизации проведения спецпроверок или специсследований.

89. Создание (далее следует наименование технического средства) в защищенном исполнении.

90. Разработка программного обеспечения автоматизированного анализа информационных систем на наличие программных и аппаратных уязвимостей.

91. Проектирование и анализ систем автоматического дизассемблирования исходных текстов программ.

92. Исследование способов защиты программного кода от дизассемблирования.

93. Обеспечение информационной безопасности в условиях использования высокоскоростных каналов передачи данных (терабит).

94. Использование нейронных сетей в задачах криптоанализа.

95. Разработка программно-аппаратных комплексов для контроля системы разграничения доступа на ОИ.

96. Разработка программно-аппаратных комплексов для построения системы разграничения доступа на ОИ.

97. Разработка программно-аппаратных решений для фильтрации сетевого траффика.

98. Разработка программно-технических решений для фиксации и контроля исходного состояния программного комплекса ЭВМ.

99. Разработка программно-аппаратных комплексов контроля утечки информации по (далее следует наименование технического канала утечки информации).

ВКР выполняемые по предложенным ниже тематикам могут относиться к ДР или ДП, содержащим сведения составляющие государственную тайну.

100. Особенности реализации угроз безопасности в ОС подразделения ответственного за обработку сведений, составляющих государственную тайну.

101. Особенности аттестации помещений для обработки сведений, составляющих государственную тайну.

102. Организация защищенного обмена в ЛВС, предназначенной для обработки сведений составляющих государственную тайну.

103. Разработка системы управления документацией для подразделения ответственного за обработку сведений, составляющих государственную тайну.

104. Разработка программного обеспечения учета и контроля для подразделения ответственного за обработку сведений, составляющих государственную тайну.

105. Форма, порядок и подход к аттестации подразделения ответственного за обработку сведений, составляющих государственную тайну (на материалах конкретного предприятия).

106. Разработка программного обеспечения для проведения аттестации подразделения ответственного за обработку сведений, составляющих государственную тайну, с использованием (далее следует наименование оборудования, например Октава 110-ЭКО).

107. Оптимизация затрат на создание лаборатории по аттестации объектов, предназначенных для обработки сведений составляющих государственную тайну, по требованиям защиты информации.

108. Оптимизация затрат на создание подразделения ответственного за обработку сведений, составляющих государственную тайну (на материалах конкретного предприятия).

109. Разработка программного обеспечения для оценки утечки информации из подразделения ответственного за обработку сведений, составляющих государственную тайну по (далее следует наименование технического канала утечки информации).

110. Разработка системы управления средствами защиты информации для подразделения ответственного за обработку сведений, составляющих государственную тайну.

ПРИЛОЖЕНИЕ Д
(обязательное)
Примерный график прохождения этапов итоговой аттестации

Примерный график подготовки, организации и проведения государственного экзамена

Виды работ	Сроки для 5-летнего обучения	Ответственный исполнитель
Формирование состава ГЭК по специальности	сентябрь	Зав. кафедрой
Формирование (актуализация) программы государственного экзамена по специальности	сентябрь	Зав. кафедрой, ведущие преподаватели
Подготовка вопросов к государственному экзамену по специальности	сентябрь-октябрь	Зав. кафедрой, Преподаватели кафедры
Выдача вопросов студентам по государственному экзамену по специальности	Январь-февраль	вед. специалист
Организация обзорных лекций и консультаций по государственному экзамену по специальности	февраль	Преподаватели кафедры
Подготовка и утверждение комплектов билетов	февраль	Председатель ГЭК вед. специалист
Утверждение расписания государственного экзамена и информирование студентов	Январь-февраль	вед. специалист
Приказ о допуске студентов к государственному экзамену по специальности (за неделю до экзамена)	март	Декан факультета
Проведение государственного экзамена	март	ГЭК

Примерный график прохождения этапов подготовки к защите дипломной работы

Виды работ	Сроки для 5-летнего обучения	Ответственный исполнитель
Формирование состава ГЭК	Октябрь-ноябрь	Зав. кафедрой
Преддипломная практика	***21 декабря-14 февраля (8 недель)***	***Зав. кафедрой***
Определение места преддипломной практики	Сентябрь-ноябрь	студент
Подача на кафедру заявления и гарантийного письма о месте прохождения преддипломной практики.	1-10 ноября	студент
Подготовка приказа на преддипломную практику.	10-20 ноября	вед. специалист кафедры, Руководители ДП
Начало преддипломной практики. Выдача заданий. Проведение собрания.	20 декабря - 23 декабря	Руководители ДП
Контроль за ходом преддипломной практики	21 декабря - 14 февраля	Руководители ДП
Защита отчетов по преддипломной практике	13 февраля – 14 февраля	Руководители ДП
Дипломное проектирование	***15 марта-5 июня (12 недель)***	***Зав. кафедрой***
Представление тем ДР, выбор темы ДР и научного руководителя	в последнем учебном семестре	Преподаватели кафедры студенты
Подача заявления о закреплении темы дипломной работы и научного руководителя.	1-10 ноября	Студент выпускной группы
Подготовка приказа по утверждению тем и руководителей ДР	15-20 ноября	вед. специалист кафедры, Руководители ДР
Составление и утверждение заданий на ДР и календарного графика на ДР	15 - 19 февраля	Руководитель ДР, за кафедрой
Составление и согласование задания на ДР с зав. кафедрой	15 - 19 февраля	Зав. кафедрой, руководители ДР
Организация консультаций (по отдельным главам и нормоконтролю)	май	Зав. кафедрой
Контроль за ходом выполнения ДР I этап (30%) II этап (80%) III этап (100%)	 5 апреля 5 мая 1 июня	Зав. кафедрой, руководители ДР
Проведение предзащиты на кафедре	10 мая- 15 мая	Зав. кафедрой, руководители ДР
Утверждение дат защит ДР	Первая неделя мая	Зав. кафедрой секретарь ГЭК
Назначение рецензентов (за две недели до защиты)	Первая неделя мая	руководители ДР, Зав. кафедрой

Виды работ	Сроки для 5-летнего обучения	Ответственный исполнитель
Получение резолюций по нормоконтролю, рецензента, консультантов (за неделю до защиты)	Последняя неделя мая	Студент выпускной группы
Подготовка проекта приказа о допуске к защите ДР (за неделю до защиты)	Последняя неделя мая	Зав. кафедрой, деканат
Защита ДР в ГЭК	Первая неделя июня	Зав. кафедрой Члены ГЭК

Примерный график организации самостоятельной работы студентов по подготовке к защите ДР

Этапы работ	Планируемая трудоемкость, %	Дата выполнения		Подпись руководителя
		План	Факт	
1. Сбор, изучение и систематизация учебной, научно-технической литературы, учебно-методической документации и патентной информации.	…	Во время преддипломной практики	…	…
2. Разработка общей части (введения, теоретической главы) работы.		5 апреля		
3. Аналитические и проектные разработки. Этапы решения поставленной задачи. Подготовка аналитической и практической глав.		5 мая		
4. Написание заключения и аннотации.		30 мая		
5. Окончательное оформление расчетно-пояснительной записки и графических материалов.				
6. Подготовка на проверку и подпись ВКР руководителю.				
7. Подготовка на проверку и подпись ВКР заведующему кафедрой. Получение допуска к защите.				
Итого				