Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Ректор КГУ
_____ / Н.В. Дубив /
«21» сентября 2020 г.

Программа
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

по образовательной программе высшего образования –
программе специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Направленность: (специализация №7) **Обеспечение информационной безопасности распределенных информационных систем**

Формы обучения: очная

Курган 2020

Программа государственной итоговой аттестации разработана в соответствии с учебным планом по программе специалитета 10.05.03 – Информационная безопасность автоматизированных систем (Обеспечение информационной безопасности распределенных информационных систем), утвержденной 28 августа 2020 года.

Программа государственной итоговой аттестации утверждена на заседании кафедры «Безопасность информационных и автоматизированных систем» 29 сентября 2020 года, протокол № 2.

Программу государственной
итоговой аттестации разработал
канд. пед. наук, доцент  Е. Н. Полякова

СОГЛАСОВАНО:

Зав. кафедрой «Безопасность
Информационных
и автоматизированных систем»
канд. пед. наук, доцент  Е. Н. Полякова

Специалист по учебно-методической
работе Учебно-методического отдела  Г.В. Казанкова

Начальник Управления
образовательной деятельности  С.Н. Синицын

1. ОБЩИЕ ПОЛОЖЕНИЯ

Государственная итоговая аттестация (далее – ГИА) выпускника проводится в соответствии с п.6.8. федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и Положением о проведении государственной итоговой аттестации студентов, обучающихся по программам бакалавриата, программам специалитета и программам магистратуры, утвержденным ученым советом университета 27 февраля 2015 г. (далее - Положение).

Для проведения ГИА формируются государственные экзаменационные комиссии (далее – ГЭК).

Государственная итоговая аттестация проводится в целях определения соответствия результатов освоения обучающимися основных образовательных программ соответствующим требованиям федерального государственного образовательного стандарта по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и их готовности к выполнению профессиональных задач.

ГИА включает в себя подготовку к процедуре защиты и процедуру защиты выпускной квалификационной работы (далее – ВКР). Государственная итоговая аттестация выпускников очной формы обучения проводится на 5 курсе в 10 семестре. Общий объем ГИА составляет 9 зачетных единиц (6 недель, 324 академических часа).

К государственной итоговой аттестации допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план по соответствующей образовательной программе высшего образования

Обучающимся и лицам, привлекаемым к государственной итоговой аттестации, во время ее проведения запрещается иметь при себе и использовать средства связи.

2. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКА

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

2.2. Объектами профессиональной деятельности выпускников, освоивших программу специалитета, являются:

- автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;
- информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и действующие информационно-технологические ресурсы, подлежащие защите;
- технологии обеспечения информационной безопасности автоматизированных систем;
- системы управления информационной безопасностью автоматизированных систем.

2.3. Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу специалитета:

научно-исследовательская;

проектно-конструкторская;

контрольно-аналитическая;

организационно-управленческая;

эксплуатационная.

2.4. Задачи профессиональной деятельности выпускника

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

в соответствии с видами профессиональной деятельности:

научно-исследовательская деятельность:

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

проектно-конструкторская деятельность:

- сбор и анализ исходных данных для проектирования защищенных автоматизированных систем;

- разработка политик информационной безопасности автоматизированных систем;

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

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

- разработка систем управления информационной безопасностью автоматизированных систем;

контрольно-аналитическая:

- контроль работоспособности и эффективности применяемых средств защиты информации;

- выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;

- проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов;

организационно-управленческая деятельность:

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

- организационно-методическое обеспечение информационной безопасности автоматизированных систем;

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

- контроль реализации политики информационной безопасности;

эксплуатационная деятельность:

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

- администрирование подсистем информационной безопасности автоматизированных систем;

- мониторинг информационной безопасности автоматизированных систем;

- управление информационной безопасностью автоматизированных систем;

- обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций;

профессиональные задачи в соответствии со специализацией «Обеспечение информационной безопасности распределенных информационных систем»:

- разработка и исследование моделей информационно-технологических ресурсов, модели угроз и модели нарушителей информационной безопасности в распределенных информационных системах;

- удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах;

- аудит защищенности информационно-технологических ресурсов;

- координация деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятиях и в учреждениях;

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Реализация компетентностного подхода в соответствии с ФГОС ВО предусматривает, что выпускник в ходе государственной итоговой аттестации показывает уровень своей квалификации с учетом следующих компетенций:

Код компетенции	Компетенция	Планируемые результаты обучения	Этап проверки
			ВКР
Общекультурные компетенции			
ОК-1	Способность использовать основы философских знаний для формирования мировоззренческой позиции	**Знать:** основные философские понятия и категории, закономерности развития природы, общества и мышления **уметь:** выделять основные причины возникновения проблем и понимать пути их решения **владеть:** понятийным и аналитическим аппаратом.	+
ОК-2	Способность использовать основы экономических знаний в различных сферах деятельности	**Знать:** основы математического анализа, линейной алгебры, теории вероятностей и математической статистики, необходимые для решения экономических задач; **уметь:** применять методы математического анализа и моделирования, теоретического и экспериментального исследования для решения экономических задач; **владеть:** методикой построения, анализа и применения стандартных теоретических и эконометрических моделей, анализировать и содержательно интерпретировать полученные результаты;	+
ОК-3	способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	**Знать:** закономерности и этапы исторического процесса основные события и процессы мировой и отечественной экономической истории, история и законы развития общественных процессов **уметь:** ориентироваться в мировом историческом процессе, анализировать процессы и явления, происходящие в обществе **владеть:** навыками системного мышления и анализа, навыками философского мышления для выработки системного, целостного взгляда на проблемы общества	+
ОК-4	способность использовать основы правовых знаний в различных сферах деятельности	**Знать** основные нормативные правовые документы; **уметь** ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих сферу профессиональной деятельности; **владеть** навыками работы с нормативной документацией;	+
ОК-5	Способность понимать социальную значимость своей		+

	будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	**Знать** и понимать социальную значимость своей будущей профессии; **уметь** обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства; **владеть** навыками и нормами профессиональной этики.	
ОК-6	Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	**Знать** глобальные проблемы современности с точки зрения культурологии; **уметь** использовать полученные знания в общении с представителями различных культур, учитывая особенности этнокультурного, конфессионального, социального контекста; **владеть** работы в коллективе.	+
ОК-7	Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	**Знать** нормы делового речевого этикета; основную терминологию и языковые конструкции в сфере деловой и профессиональной коммуникации; **уметь** воспринимать на слух и понимать основное содержание профессионально-ориентированных текстов; обмениваться информацией профессионального и научного характера в процессе профессионального общения; делать сообщения в области профессиональной тематики; использовать знания иностранного языка для профессионального самосовершенствования. **владеть**: деловым речевым этикетом и правилами поведения при деловом общении с представителями стран изучаемого языка; навыками использования иностранного языка в устной и письменной форме в сфере профессиональной коммуникации; навыками публичной коммуникации (делать сообщения, доклады, презентации, выступать на научных конференциях).	+
ОК-8	Способность к самоорганизации и самообразованию	**Знать**: профессиональные функции в соответствии с направлением и уровнем подготовки; принципы психологической оценки личности; **уметь**: применять методы и средства познания для интеллектуального развития повышения культурного уровня, профессиональной компетентности; формулировать задачи и цели современного финансового работника, критически оценивать уровень своей квалификации и необходимость ее повышения; **владеть**: навыками саморазвития и методами развития личности; навыками саморазвития и методами повышения квалификации;	+
ОК-9	Способность использовать методы и средства физической культуры для обеспечения	**Знать**: средства самостоятельного методически правильного использования методов физического воспитания и укрепления здоровья; **уметь**: правильно использовать методы физического воспитания и укрепления здоровья для обеспечения	+

	полноценной социальной и профессиональной деятельности	полноценной социальной и профессиональной деятельности; **владеть**: средствами самостоятельного методически правильного использования методов физического воспитания и укрепления здоровья для достижения должного уровня физической подготовленности и обеспечения полноценной социальной и профессиональной деятельности;	
Общепрофессиональные компетенции:			
ОПК-1	Способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач	**Знать** основные физические законы используемые при защите информации; **уметь** использовать физические явления, процессы и применять соответствующий математический аппарат в своей профессиональной деятельности; **владеть** навыками практического использования физических явлений и процессов при работе по обеспечению защиты информации.	+
ОПК-2	Способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	**Знать** определения и свойства функций алгебры логики, простейшие алгоритмические модели; **уметь** приобретать новые фундаментальные математические и инженерные знания с использованием современных информационных технологий; **владеть** основами построения математических моделей систем передачи информации.	+
ОПК-3	Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности	**Знать** области и особенности применения языков программирования высокого уровня; **уметь** реализовывать на языке высокого уровня алгоритмы решения профессиональных задач; **владеть** навыками разработки, документирования, тестирования и отладки программ.	+
ОПК-4	Способность понимать значение информации в развитии современного общества, применять	**Знать** современные информационные технологии; основы функционирования глобальных сетей; **уметь** применять достижения современных	+

	достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах	информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах; **владеть** навыками использования информационных технологий как средства управления информацией; навыками использования информации, полученной из сети интернет и библиотечных фондов.	
ОПК-5	Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	**знать** методы научных исследований в профессиональной деятельности; **уметь** применять научные исследования в междисциплинарных и инновационных проектах; **владеть** навыками научных исследований в профессиональной деятельности.	+
ОПК-6	Способность применять нормативные правовые акты в профессиональной деятельности	**Знать** основные нормативные правовые документы; **уметь** ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих сферу профессиональной деятельности; **владеть** навыками работы с нормативной документацией.	+
ОПК-7	Способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций	**Знать** потенциальные факторы риска для жизни и здоровья людей; **уметь** оценивать степень опасности возможных последствий аварий, катастроф и стихийных бедствий для персонала и применять приемы оказания первой помощи; **владеть** практическими навыками защиты населения в условиях чрезвычайных ситуаций.	+
ОПК-8	Способность к освоению новых образцов программных, технических средств и информационных технологий	**Знать** новые образцы программных, технических средств и информационных технологий; **уметь** проводить комплексное тестирование и отладку программных систем; **владеть** навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования.	+
Профессиональные компетенции			
ПК-1	Способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	**Знать** способы поиска научно-технической информации; **уметь** самостоятельно находить научно-техническую нормативную и методическую информацию из различных источников (периодические издания, Интернет, справочная, учебная, художественная литература) в сфере профессиональной деятельности; **владеть** способами обобщения нормативных и методических материалов.	+

ПК-2	Способность создавать и исследовать модели автоматизированных систем	**Знать** принципы построения информационных систем с применением современных технических средств хранения, обработки, поиска и передачи информации; **уметь** разработать модель автоматизированной системы; **владеть** навыками исследования модели автоматизированных систем.	+
ПК-3	Способность проводить анализ защищенности автоматизированных систем	**Знать** последовательность и содержание этапов построения автоматизированных систем; **уметь** проектировать и администрировать автоматизированные системы, реализовывать политику безопасности автоматизированных систем; **владеть** навыками эксплуатации и администрирования баз данных автоматизированных систем с учетом требований по обеспечению информационной безопасности.	+
ПК-4	Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	**Знать** источники и способы воздействия угроз на объекты информационной безопасности автоматизированной системы; **уметь** анализировать и оценивать угрозы информационной безопасности; **владеть** методикой выявления и анализа потенциально существующих угроз безопасности информации.	+
ПК-5	Способность проводить анализ рисков информационной безопасности автоматизированной системы	**Знать** методы определения размеров возможного ущерба; **уметь** оценивать риски информационной безопасности автоматизированных систем; **владеть** методами анализа рисков информационной безопасности автоматизированной системы.	+
ПК-6	Способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	**Знать** методику выявления и анализа потенциально существующих угроз безопасности информации; **уметь** обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности; **владеть** методами обработки и анализа экспериментальных данных.	+
ПК-7	Способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	**Знать** правила оформления научно-технической документации; **уметь** самостоятельно находить научно-техническую нормативную и методическую информацию из различных источников; **владеть** методами обработки и анализа экспериментальных данных.	+
ПК-8	Способность разрабатывать и анализировать проектные решения по обеспечению	**Знать** действующие нормативные и методические материалы, регламентирующие работу по защите информации, положения, инструкции и другие организационно-распорядительные документы; **уметь** анализировать проектные решения по	+

	безопасности автоматизированных систем	обеспечению безопасности автоматизированных систем; **владеть** навыками построения моделей систем защиты информации	
ПК-9	Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	**Знать** последовательность и содержание этапов построения автоматизированных систем; **уметь** проектировать и администрировать автоматизированные системы, реализовывать политику безопасности автоматизированных систем; **владеть** навыками эксплуатации и администрирования баз данных автоматизированных систем с учетом требований по обеспечению информационной безопасности.	+
ПК-10	Способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	**Знать** типовые схемотехнические решения основных узлов и блоков электронной аппаратуры, общие принципы построения и использования современных языков программирования высокого уровня, программно-аппаратные средства обеспечения информационной безопасности в системах; **уметь** работать с современной базой электронной аппаратуры, реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования, проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности; **владеть** навыками работы с программными средствами схемотехнического моделирования, использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.	+
ПК-11	Способность разрабатывать политику информационной безопасности автоматизированной системы	**Знать** методы и средства выявления угроз безопасности автоматизированных систем; **уметь** разрабатывать частные политики безопасности автоматизированных систем; **владеть** методами оценки информационных рисков.	+
ПК-12	Способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	**Знать** основные методы управления информационной безопасностью; **уметь** разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; **владеть** методами управления информационной безопасностью автоматизированных систем.	+
ПК-13	Способность участвовать в проектировании средств защиты информации автоматизированной системы	**Знать** способы и средства защиты информации; **уметь** разрабатывать проекты с использованием средств защиты информации автоматизированной системы; **владеть** навыками работы со средствами защиты информации.	+
ПК-14	Способность проводить контрольные проверки	**Знать** критерии оценки эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;	+

	работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	**уметь** применять криптографические протоколы и криптографические алгоритмы для передачи и хранения данных в распределенных информационных системах; **владеть** способностью к освоению новых образцов программных, технических средств и информационных технологий.	
ПК-15	Способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	**Знать** правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; органы по сертификации средств защиты информации; **уметь** применять методы обработки и анализа экспериментальных данных; **владеть** навыками проведения экспериментально-исследовательских работ при сертификации средств защиты информации в автоматизированных систем.	+
ПК-16	Способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	**Знать** руководящие документы по аттестации автоматизированных систем; **уметь** применять экспериментально-исследовательские работы при аттестации автоматизированных систем с учетом нормативных документов по защите информации; **владеть** навыками методами обработки и анализа экспериментальных данных.	+
ПК-17	Способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	**Знать** источники и способы воздействия угроз на объекты информационной безопасности; **уметь** проводить инструментальный мониторинг защищенности автоматизированных систем; **владеть** навыками инструментального мониторинга угроз безопасности автоматизированных систем.	+
ПК-18	Способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	**Знать** социально–психологические основы формирования личности; влияние личностных качеств руководителя и подчиненных на взаимоотношения в коллективе, концепции лидерства; **уметь** сопоставлять права и обязанности подчиненных; приводить примеры возможных конфликтов и стрессов в коллективе и методов их преодоления; **владеть** навыками анализа современных технологий управления и организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности.	+
ПК-19	Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	**Знать** структуру, правовые основы и содержание деятельности предприятий различных форм собственности; **уметь** работать в коллективе, принимать управленческие решения и оценивать их эффективность; **владеть** навыками анализа современных технологий управления и организовывать работу коллективов	+

	автоматизированной системы	исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности.	
ПК-20	Способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	**Знать** этапы разработки и внедрения информационно-аналитической системы; **уметь** разработать модель информационной системы; **владеть** методологиями моделирования процессов и применения определенных программных продуктов.	+
ПК-21	Способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	**Знать** основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; **уметь** разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации; **владеть** регламентом работ, связанным с комплексным обеспечением информационной безопасности автоматизированных систем.	+
ПК-22	Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**Знать** методологию и технологии комплексной защиты информации; **уметь** формировать политику информационной безопасности в автоматизированных системах; **владеть** навыками обеспечения защищённого хранения информации на носителях; защита данных, передаваемых по каналам связи; создание резервных копий, послеаварийное восстановление.	+
ПК-23	Способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	**Знать** методологии и технологии комплексной защиты информации ограниченного доступа; **уметь** выполнять полный объем работ, связанных с защитой информации ограниченного доступа; **владеть** методикой выявления и анализ потенциально существующих угроз безопасности информации, составляющей государственную и другие виды тайны.	+
ПК-24	Способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	**Знать** принципы построения информационных систем с применением современных технических средств хранения, обработки, поиска и передачи информации; **уметь** использовать принципы построения информационных систем с применением современных технических средств хранения, обработки, поиска и передачи информации; **владеть** навыками обеспечения защищённого хранения информации и послеаварийного восстановления.	+
ПК-25	Способность обеспечить эффективное применение средств	**Знать** мероприятия по защите информации законодательного, организационного и программно-технического характера;	+

	защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	**уметь** использовать отечественные и международные стандарты в области информационной безопасности; **владеть** навыками построения подсистемы информационной безопасности.	
ПК-26	Способность администрировать подсистему информационной безопасности автоматизированной системы	**Знать** принципы построения и функционирования, примеры реализации современных ОС; **уметь** администрировать подсистему информационной безопасности автоматизированной системы; **владеть** навыками эксплуатации и администрирования баз данных, локальных компьютерных систем с учетом требований по обеспечению информационной безопасности.	+
ПК-27	Способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	**Знать** методы и средства выявления угроз безопасности автоматизированных систем; **уметь** проводить инструментальный мониторинг и аудит безопасности автоматизированных систем; **владеть** навыками контроля реализации частных политик информационной безопасности автоматизированной системы	+
ПК-28	Способность управлять информационной безопасностью автоматизированной системы	**Знать** источники и классификацию угроз информационной безопасности; **уметь** разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы; **владеть** навыками выбора, обоснования, реализации и контроля результатов управленческого решения.	+
Компетенции специализации			
ПСК-7.1	Способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	**Знать** источники и способы воздействия угроз на объекты информационной безопасности предприятий; **уметь** строить информационные системы с применением современных технических средств хранения, обработки, поиска и передачи информации; **владеть** методикой выявления и анализа потенциально существующих угроз безопасности информации в распределенных информационных системах.	+
ПСК-7.2	Способность проводить анализ рисков информационной безопасности и	**Знать** методы определения размеров возможного ущерба; **уметь** оценивать риски информационной безопасности в распределенных информационных системах;	+

	разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	**владеть** методами анализа рисков информационной безопасности автоматизированной системы.	
ПСК-7.3	Способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	**Знать** виды и цели аудита, этапы выполнения работ по аудиту; **уметь** анализировать риски и давать оценку текущего уровня защищенности распределенных информационных систем; **владеть** навыками оценки ресурсов системы на соответствие стандартам в области информационной безопасности.	+
ПСК-7.4	Способность проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	**Знать** операции резервного копирования и восстановления; **уметь** управлять файлами базы данных; **владеть** навыками администрирования пользователей.	+
ПСК-7.5	Способность координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении	**Знать** основные методы управления информационной безопасностью; **уметь** разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; **иметь** навыки организации и управления деятельностью служб защиты информации на предприятии.	+

4. ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

4.1. Общие требования к ВКР

Видом выпускной квалификационной работы является дипломный проект (работа).

ВКР носит практическую направленность в соответствии со специализацией «Обеспечение информационной безопасности распределенных информационных систем» и должна представлять собой законченную разработку на заданную тему. ВКР может основываться на обобщении выполненных выпускником курсовых работ и проектов.

4.2. Выбор и утверждение темы ВКР

Тематика ВКР разрабатывается кафедрой «Безопасность информационных и автоматизированных систем» в соответствии с ООП с учетом видов профессиональной деятельности выпускников. Перечень тем ВКР доводится до сведения выпускников не позднее, чем за 6 месяцев до начала государственной итоговой аттестации. Обучающийся может предложить свою тему с необходимым обоснованием целесообразности ее разработки. Закрепление темы за обучающимся осуществляется на основании личного заявления

обучающегося на имя заведующего выпускающей кафедрой. Заявления обучающихся об утверждении темы ВКР рассматриваются на заседании кафедры не позднее, чем за 2 недели до начала преддипломной практики. Утверждение обучающимся тем ВКР оформляется приказом ректора университета не позднее чем, за неделю до начала преддипломной практики.

4.3. Организация работы обучающегося при подготовке ВКР

Для подготовки ВКР обучающемуся (нескольким обучающимся, выполняющим ВКР совместно) приказом ректора университета назначаются из числа профессорско-преподавательского состава кафедры, или специалистов иных организаций, осуществляющих деятельность по профилю соответствующей образовательной программы, руководитель ВКР и, при необходимости, консультант (консультанты) по подготовке ВКР. В случае если руководитель ВКР не является работающим на постоянной основе работником университета, в обязательном порядке назначается консультант по ВКР из числа профессорско-преподавательского состава выпускающей кафедры.

Руководитель обязан осуществлять руководство ВКР, в том числе:

– оказывать консультативную помощь обучающемуся в определении окончательной темы ВКР;

– разработать задание ВКР. Задание оформляется в двух экземплярах и хранится до защиты ВКР: один экземпляр – у руководителя, второй – у обучающегося;

– оказывать консультативную помощь обучающемуся в подборе литературы и фактического материала;

– содействовать в выборе методики исследования (разработки);

– осуществлять систематический контроль за ходом выполнения ВКР в соответствии с планом и графиком ее выполнения, полнотой и качеством разработки ее разделов;

– информировать заведующего кафедрой в случае несоблюдения обучающимся графика выполнения ВКР;

– давать квалифицированные рекомендации по содержанию ВКР;

– подготовить отзыв руководителя.

Консультант обязан:

– оказывать консультативную помощь обучающемуся в выборе методики исследования, в подборе литературы и фактического материала;

– давать квалифицированные рекомендации по содержанию отдельных разделов выпускной квалификационной работы;

– подтвердить своей подписью на титульном листе работы (пояснительной записки) и в двух экземплярах задания выполнение обучающимся отдельных разделов ВКР.

4.4. Требования к оформлению и содержанию ВКР

Структура, содержание и объем ВКР определяются заданием, оформленным по установленной форме.

Рекомендуемые объемы пояснительной записки и графической части ВКР, а также требования к ее оформлению устанавливаются в учебном пособии по выполнению и оформлению выпускных квалификационных работ для студентов образовательной программы высшего образования: программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» «Дипломное проектирование».

4.5. Порядок представления ВКР к защите

Обучающийся обязан представить окончательный вариант ВКР с отзывов руководителя на работу, рецензией и справкой о заимствовании на выпускающую кафедру не менее чем за 10 дней до назначенной даты защиты выпускной квалификационной работы.

Руководитель выпускной квалификационной работы готовит отзыв на работу, где отмечает:

– соответствие темы квалификационной работы заданию;

– полнота раскрытия темы;

– теоретический уровень и практическая значимость работы;

– уровень подготовленности (сформированности требуемых стандартом и образовательной программой компетенций) обучающегося;

– качество оформления работы;

– возможность допуска студента к защите квалификационной работы;

– рекомендуемая оценка и мнение о возможности присвоения квалификации.

Отзыв оформляется в рукописном или печатном варианте на бланке. Руководитель подписывает титульный лист работы (пояснительной записки) и два экземпляра задания, рекомендуя ВКР к защите перед экзаменационной комиссией.

Если руководитель не считает возможным допустить обучающегося к защите ВКР, то он обосновывает свое мнение в отзыве. Основаниями для не допуска руководителем обучающегося к защите являются:

– несоответствие работы выданному заданию;

– неполнота, низкое качество, грубые ошибки в разработке отдельных разделов;

– выявленная руководителем несамостоятельность обучающегося при выполнении работы.

Обучающийся, не представивший в установленный срок ВКР с отзывом руководителя и рецензией на ВКР, не допускается к защите и отчисляется из университета как не прошедший государственную итоговую аттестацию с выдачей ему справки об обучении в университете установленного образца.

Окончательное решение о допуске выпускника к защите выпускной квалификационной работы перед государственной экзаменационной комиссией принимается на заседании кафедры. Оформляется такое решение протоколом и подписывается заведующим кафедрой на титульном листе и задании на дипломную работу (проект).

Заведующий кафедрой может своим распоряжением установить на кафедре предварительное слушание выпускных квалификационных работ.

В случае принятия кафедрой решения о несоответствии представленной работы требованиям, предъявляемым к ВКР, и обучающийся не допускается к защите ВКР, в организационный отдел передается выписка из протокола заседания кафедры. Директор института на основании решения кафедры представляет обучающегося к отчислению из университета, как не прошедшего государственную итоговую аттестацию с выдачей ему справки об обучении в университете установленного образца.

Выпускная квалификационная работав обязательном порядке проходит процедуру нормоконтроля. Она выявляет степень знания будущим специалистом требований по оформлению технической документации. При отсутствии замечаний, нормоконтролер ставит свою подпись на титульном листе пояснительной записки. При наличии замечаний нормоконтролер ставит подпись на титульном листе пояснительной записки, но с резолюцией «С замечаниями».

Выпускная квалификационная работа в сброшурованном виде подлежит обязательному рецензированию. Список рецензентов выпускных квалификационных работ готовит выпускающая кафедра, затем список утверждается директором института.

Рецензирование выпускных квалификационных работ осуществляется ведущими специалистами в соответствующей области профессиональной деятельности.

Рецензия оформляется в рукописном или печатном варианте на бланке, в которой дает характеристику всем ее компонентам и предлагает оценку для работы в целом («отлично», «хорошо», «удовлетворительно», «неудовлетворительно). Оценка рецензента учитывается государственной экзаменационной комиссией при определении окончательной оценки защиты ВКР. Получение отрицательной рецензии не является препятствием к принятию ВКР к защите.

В целях повышения контроля степени самостоятельности выполнения обучающимися работ, а также соблюдения ими прав интеллектуальной собственности руководителем осуществляется проверка текстов ВКР на объем заимствований с использованием программы «Платформа ВКР ВУЗ – размещение, хранение материалов и поиск на заимствования». Справка о заимствовании в выпускной квалификационной работе обязательно прилагается.

Ответственное лицо выпускающей кафедры не позднее, чем за 2 дня до защиты выпускной квалификационной работы обеспечивает ознакомление обучающегося с отзывом и рецензией (рецензиями).

Перед защитой ВКР отзыв руководителя, рецензия (рецензии) и справка о заимствовании передается секретарю государственной экзаменационной комиссии выпускающей кафедры.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Перечень оценочных средств выпускной квалификационной работы

Примерная тематика выпускных квалификационных работ

1. Разработка межсетевого экрана, скрытого от нарушителя, действующего по сети.
2. Комплексная система предотвращения утечки конфиденциальной информации с мобильных устройств: сервер управления доступом к конфиденциальной информации и предотвращение утечек данных.
3. Система контроля и защиты мобильных устройств.
4. Система централизованного управления учетными записями пользователей.
5. Разработка программно-аппаратного комплекса биометрической идентификации по рисунку вен ладони.
6. Система распознавания идентификационных номеров и контроля доступа транспортных средств на охраняемую территорию.
7. Система биометрической аутентификации пользователя персонального компьютера.
8. Система защиты канала передачи информации.
9. Программно-аппаратное средство защиты пользовательских фалов на основе ключевого flash-носителя.
10. Разработка системы контроля действий пользователя, на основе заданной внутренней политики.
11. Система определения тематики web ресурса.
12. Программный комплекс по обеспечению аутсорсинга IT-систем.
13. Контроль целостности информации ограниченного доступа.
14. Разработка системы контроля доступа к информационной системе с использованием мобильного телефона.
15. Разработка методических указаний по проведения аудита информационной безопасности PCI DSS в банковских системах.
16. Разработка системы определения актуальных угроз информационных систем персональных данных.
17. Оценка эмоционального состояния работника как возможность определения потенциального нарушителя.
18. Автоматизированная система защиты речевого трафика.
19. Комплексная система контроля физического доступа к защищаемому объекту на основе GSM-сигнализации.
20. Защищенная система физической безопасности объекта.
21. Система контроля и анализа внешних и внутренних информационных ресурсов.
22. Программный комплекс идентификации, аутентификации и аудита внешних запоминающих устройств с интерфейсом USB.
23. Распределенная система предотвращения утечек конфиденциальной информации через устройства вывода на печать.

5.2. Процедура оценивания результатов защиты ВКР

Результаты защиты выпускной квалификационной работы оценивает Государственная экзаменационная комиссия, которая утверждается приказом ректора университета. Оценивается уровень освоения соответствующих компетенций. Для оценки результатов защиты ВКР применяют четырехбалльную шкалу: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно». Результаты защиты выпускной квалификационной работы определяются выведением средне-арифметической оценки членов государственной экзаменационной комиссии, руководителя работы и рецензента.

Результаты защиты объявляются всей группе выпускников немедленно после оформления протокола закрытого заседания государственной экзаменационной комиссии, на котором проводилось обсуждение защит выпускных квалификационных работ.

Оценка по результатам защиты выпускной квалификационной работы заносится в протокол заседания Государственной экзаменационной комиссии и зачетную книжку, в которой ставят свои подписи председатель и члены комиссии. У обучающегося есть право не согласиться с оценкой и подать апелляцию в соответствии с Порядком проведения итоговой государственной аттестации выпускников Курганского государственного университета.

5.3. Полный фонд оценочных средств

Полный перечень тем выпускных квалификационных работ, описание показателей и критериев оценивания компетенций, а также шкал оценивания содержится в учебно-методическом комплексе государственной итоговой аттестации образовательной программы.

6. РЕКОМЕНДАЦИИ ВЫПУСКНИКАМ ПО ПОДГОТОВКЕ К ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

В период подготовки выпускной квалификационной работы предусмотрены консультации преподавателей кафедры. График консультации утверждает заведующий выпускающей кафедрой и вывешивается на доске объявлений кафедры.

При выполнении ВКР рекомендуется соблюдать ритмичность работы и согласовывать законченные разделы с руководителем с целью обеспечения соответствия требованиям содержания и задания на ВКР.

При оформлении ВКР следует придерживаться методических рекомендаций, изложенных в учебном пособии «Дипломное проектирование» по выполнению и оформлению выпускных квалификационных работ для студентов образовательной программы высшего образования: программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем».

В период подготовки к процедуре защиты работы выпускникам рекомендуется составить текст доклада, учитывая установленные временные

ограничения на доклад, согласовать его с руководителем и подготовить ответы на замечания в отзыве и рецензии на ВКР.

7. ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ ИНТЕРНЕТ

7.1 ОСНОВНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

1 Мэйволд, Э. Безопасность сетей [Электронный ресурс] : учебное пособие / Э. Мэйволд; Интернет-университет информационных технологий. – Электрон. дан. – М.: Интернет-Университет информационных технологий, 2005. – Режим доступа: https://www.intuit.ru/studies/courses/102/102/info, свободный. – Загл. с экрана.

2 Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей. Учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2018. — 416 с.

3 Шопырин Д.Г. Управление проектами разработки ПО: Учебно-методическое пособие по дисциплине "Гибкие технологии разработки программного обеспечения" / Д.Г. Шопырин. – СПб: СПбГУ ИТМО, 2007. – 131 с. – Режим доступа: http://window.edu.ru/resource/ 373/60373, свободный. – Загл. с экрана.

4 Комагоров, В.П. Архитектура сетей и систем телекоммуникации [Электронный ресурс] : учебное пособие / В.П. Комагоров; Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2011. – 154 с – Режим доступа: http://window.edu.ru/resource/074/79074, свободный. – Загл. с экрана.

5 Миков, А.И. Распределенные системы и алгоритмы [Электронный ресурс]: Курс лекций / А.И.Миков, Е.Б.Замятина. – 2007. – 118 с. – Режим доступа: http://window.edu.ru/resource/466/57466, свободный. – Загл. с экрана.

6 Соколов, А. В. Защита информации в распределенных корпоративных сетях и системах [Электронный ресурс] / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК, 2002. – 656 с. – Режим доступа: http://window.edu.ru/ .

7 Хорев П.Б., Методы и средства защиты информации в компьютерных системах. Учеб. пособие для студ. высш. учеб. заведений. — М.: Академия, 2005. — 256 с.

8 Проскурин В.Г. Защита программ и данных. Учебное пособие 2-е изд., стер. – М.: «Академия», 2012 – 208 с.

9 Галатенко В.А. Стандарты информационной безопасности: курс лекций / В.А. Галатенко. — Москва : Интуит НОУ, 2016. - 308 с.

10 А.Ю. Щербаков. Современная компьютерная безопасностью. Теоретические основы. Практические аспекты. [Электронный ресурс]: Учебное пособие. - М.: Книжный мир, 2009. – Доступ из ЭБС «Консультант студента».

11 Галатенко В.А. Основы информационной безопасности: Курс лекций – М.: Интернет-Университет Информационных технологий, 2004. - 208с.

12 Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей:

Учебное пособие: В.Ф. Шаньгин. – М.: ИНФРА-М, 2017 - 416. – Доступ из ЭБС: http://znanium.com/catalog.php?bookinfo=945331

13 Сети связи и системы коммутации: Учебное пособие/ Паринов А.В. и (др.) Воронеж: Научная книга, 2016 – 178. – Доступ из ЭБС: http://znanium.com/bookread2.php?book=923309

14 Заботина Н.Н. Проектирование информационных систем: Учебное пособие/ Н.Н. Заботина – М.,НИЦ ИНФРА – М,2014 – 331с., Доступ из ЭБС: http://znanium.com/bookread2.php?book=454282

7.2 ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

1. Научно-исследовательские работы (курсовые, дипломные, диссертации): общая методология, методика подготовки и оформления/ Учебное пособие – М, Издательство АСВ, 2015 – 120с – Доступ из ЭБС: http:entlibrary.ru/book ISBN9785930934007.html

2 Основы построения автоматизированных информационных систем: Учебник В.А. Гвоздева, И.Ю. Лаврентьева – М: ИД ФОРУМ: НИЦ ИНФРА – М, 2013 – 320с Доступ из ЭБС: http://znanium.com/bookread2.php?book=392285

8. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

Информационно-справочная система «Консультант-Плюс».

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, Libre Office.

ПРИЛОЖЕНИЕ 1

Аннотация к программе
государственной итоговой аттестации
образовательной программы высшего образования –
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Направленность: (специализация №7) **Обеспечение информационной безопасности распределенных информационных систем**

Трудоемкость: 9 зачетных единиц (324 академических часа)
Семестр: 10 (очная форма обучения)
Форма государственной итоговой аттестации: подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы.

Содержание программы государственной итоговой аттестации:

Характеристика профессиональной деятельности выпускника, планируемые результаты обучения, описание процедур проведения государственной итоговой аттестации, фонд оценочных средств, рекомендации выпускникам по подготовке к государственной итоговой аттестации, перечень рекомендуемой литературы и ресурсов сети интернет, минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, Libre Office.