


Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

«Государственная итоговая аттестация»

по специальности 10.05.03 «Информационная безопасность автоматизированных систем»
специализация «Безопасность открытых информационных систем»

1. Цели и задачи ГИА

Государственная итоговая аттестация проводится государственными экзаменационными комиссиями с целью определения соответствия результатов освоения обучающимися основных образовательных программ соответствующим требованиям федерального государственного образовательного стандарта.

Цель проведения ГИА состоит в проверке знаний и навыков студента, полученных им в процессе обучения, и оценке его профессионального уровня по специальности «Информационная безопасность автоматизированных систем».

Задачи ГИА:

- проверка знания студентом основных теоретико-методологических подходов и уровня освоения базовых предметов специальности, определяющих профессиональные способности выпускника;
- оценка умения студента ориентироваться в текущей ситуации в области информационной безопасности;
- оценка уровня обоснования студентом собственных выводов, грамотности их изложения;
- определение соответствия подготовки выпускников квалификационным требованиям федерального государственного образовательного стандарта высшего образования (далее по тексту ФГОС ВО).

2. Место ГИА в структуре ОПОП ВО


Данный модуль входит в блок «Государственная итоговая аттестация» (БЗ) Основной Профессиональной Образовательной Программы по специальности «Информационная безопасность автоматизированных систем» и включает в себя государственный экзамен и защиту выпускной квалификационной работы (ВКР). Для успешного освоения ГИА используются знания, умения, навыки и компетенции, сформированные в процессе обучения по базовым дисциплинам указанной специальности.

3. Требования к результатам освоения программы

Программа ГИА направлена на определение сформированности у выпускников следующих компетенций:

общекультурными компетенциями:

- способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);
- способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);
- способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		


- способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);
- способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);
- способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);
- способностью к самоорганизации и самообразованию (ОК-8);
- способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

общефессиональными компетенциями:


- способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);
- способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);
- способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);
- способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);
- способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);
- способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6)
- способностью применять приемы первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);
- способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8).

профессиональными компетенциями:

- способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);
- способностью создавать и исследовать модели автоматизированных систем (ПК-2);
- способностью проводить анализ защищенности автоматизированных систем (ПК-3);
- способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);
- способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);
- способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

- профессиональной деятельности (ПК-6);
- способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);
 - способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);
 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);
 - способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);
 - способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);
 - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);
 - способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);
 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
 - способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);
 - способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации (ПК-16);
 - способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);
 - способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);
 - способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);
 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);
 - способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);
 - способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);
 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);
 - способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);
 - способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);
 - способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

- способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);
- способностью управлять информационной безопасностью автоматизированной системы (ПК-28);

профессионально-специализированными компетенциями:

- способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-4.1);
- способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.2);
- способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3);
- способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы (ПСК-4.4);
- способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.5).


Кроме того, студент должен:

Знать:

- основные понятия и методы математического анализа, геометрии, алгебры, теории функций комплексного переменного, теории вероятностей и математической статистики;
- принципы организации информационных систем в соответствии с требованиями информационной защищенности, в том числе в соответствии с требованиями по защите государственной тайны;
- базовый понятийный аппарат в области информационной безопасности и защиты информации;
- виды и состав угроз информационной безопасности;
- конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации, потенциальные каналы утечки информации, характерные для этих устройств, способы их выявления и методы оценки опасности, основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;
- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- принципы построения современных криптографических систем, стандарты в области криптографической защиты информации;
- основные правовые положения в области информационной безопасности и защиты информации;
- виды уязвимости защищаемой информации и формы ее проявления;
- каналы и методы несанкционированного доступа к конфиденциальной информации;
- наиболее уязвимые для атак противника элементы компьютерных систем;

Владеть:

- методами организации и управления деятельностью служб защиты информации на

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

- предприятию;
- технологией проектирования, построения и эксплуатации комплексных систем защиты информации;
 - методами научного исследования уязвимости и защищенности информационных процессов;
 - методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
 - навыками использования типовых криптографических алгоритмов;
 - навыками математического моделирования в криптографии;
 - навыками самостоятельной работы с современными международными стандартами криптографических протоколов;

Применять на практике:

- основные методы математического, комплексного анализа, алгебры и геометрии;
- комплекс мер по информационной безопасности с учетом его правовой обоснованности;
- разработку математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов;
- проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации;
- применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;
- проведение инструментального мониторинга защищенности компьютерных систем;
- организацию работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа (сведений, составляющих государственную тайну и конфиденциальной информации).

4. Общая трудоемкость ГИА

Общая трудоемкость ГИА составляет 324 часа (9 зачетных единиц). Из них:

- 108 часов (3 ЗЕ) отводится на подготовку и сдачу государственного экзамена,
- 216 часов (6 ЗЕ) отводится на подготовку и защиту ВКР.

5. Образовательные технологии

В ходе ГИА используются следующие образовательные технологии: активные (подготовка дипломной работы, подготовка к государственному экзамену).

При организации самостоятельной работы используются следующие образовательные технологии: репродуктивные (работа с книгой), активные (работа с информационными ресурсами), компьютерные технологии.

6. Контроль успеваемости

Программой ГИА виды текущего контроля не предусмотрены.

В блок "Государственная итоговая аттестация" входит

- подготовка к сдаче и сдача государственного экзамена,
- защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.