МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА и
ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ
(Государственного экзамена)

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль**): Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**

Учебный план набора 2012 года и последующих лет.

Трудоемкость ГЭ_____3_____з.е.
Количество зачетных единиц на ГЭ по плану

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 15 » 6 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «15» июня 2017 года, протокол №6.

Разработчик:

доцент каф. КИБЭВС	_____	Е. М. Давыдова
Заведующий обеспечивающей каф. КИБЭВС	_____	А. А. Шелупанов

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан ФБ	_____	Е. М. Давыдова
Заведующий выпускающей каф. КИБЭВС	_____	А. А. Шелупанов

Эксперт:

Директор Центр системного проектирования	_____	А. А. Конев

1. Цель государственной итоговой аттестации и ее состав

Согласно требованиям закона «Об образовании в РФ» ФЗ-273 (статья 59) и соответствующего федерального государственного образовательного стандарта высшего образования (ФГОС ВО), итоговая аттестация, завершающая освоение основных профессиональных образовательных программ, является обязательной и представляет собой форму оценки степени и уровня освоения обучающимися образовательной программы. Итоговая аттестация, завершающая освоение имеющих государственную аккредитацию основных образовательных программ, является **государственной итоговой аттестацией (ГИА)**.

Целью ГИА является определение соответствия результатов освоения обучающимися основных образовательных программ соответствующим требованиям федерального государственного образовательного стандарта высшего образования.

Согласно требованиям ФГОС ВО 10.05.03, в процедуру ГИА входит защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, а также подготовка к сдаче и сдача государственного экзамена (если организация включила государственный экзамен в состав государственной итоговой аттестации).

Государственный экзамен в состав ГИА по решению выпускающей кафедры по данному направлению подготовки включен.

2. Место ГИА в структуре ОПОП ВО и ее объем

Согласно ФГОС ВО по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем» государственная итоговая аттестация входит в блок 3, который в полном объеме относится к базовой части образовательной программы.

Согласно требованиям соответствующего ФГОС ВО трудоемкость ГИА должна быть предусмотрена в объеме 6 - 9 з.е. По данному направлению подготовки трудоемкость ГИА составляет 9 з.е. Трудоемкость ГЭ составляет 3 з.е.

3. Допуск к ГЭ

К государственному экзамену допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план.

4 Порядок проведения ГЭ

4.1 Нормативные требования

Требования к процедуре ГЭ, порядок проведения итоговой аттестации соответствуют положениям приказа МОН от 29 июня 2015 г. N 636 (с изменениями) «Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры».

4.2 Требования к государственному экзамену

Государственный экзамен проводится в виде междисциплинарного экзамена по нескольким общепрофессиональным дисциплинам и дисциплинам специализации, включая дисциплины специальности.

Междисциплинарный государственный экзамен проводится по окончании теоретического обучения по специальности.

Сдача итогового междисциплинарного экзамена осуществляется в сроки итоговой государственной аттестации, которые определяются учебным планом и приказом ректора.

Форма проведения государственного экзамена смешанная, в два этапа: письменного и устного.

Студенты обеспечиваются программой государственного экзамена за не менее чем за 2 месяца до сдачи. За 10 дней до начала сдачи по желанию студентов проводятся консультации по ГЭ. Оценка объявляется выпускникам в день сдачи экзамена после оформления в установленном порядке протоколов заседания Государственной экзаменационной комиссии.

4.3 Порядок проведения государственного экзамена

Государственный экзамен по направлению Информационная безопасность, специальность 10.05.03 – «Информационная безопасность автоматизированных систем: проводится в два этапа: письменный этап и устный этап.

В день государственного экзамена в 9-00 студенты получают билет для выполнения письменного этапа. В билете два задания. На выполнение заданий письменного этапа отводится 4 академических часа. 20 минут отводится на перерыв. Студентам предоставляется рабочее место и ЭВМ в учебном классе. Для сдающих экзамен, открывается доступ к разделу государственный экзамен в единой образовательной среде MOODLe для «выкладывания решений». Доступ к разделу закрывается в 12-20.

Начиная с 12 - 20 до 14 - 00 члены комиссии проводят предварительную экспертизу решений в системе MOODLe .

Защита письменного этапа назначается на 14 - 00 в тот же день. Решения на письменные задания государственного экзамена докладываются публично на заседании Государственной экзаменационной комиссии (ГЭК). Студент получает доступ к системе MOODLe. Отображает решение на экране. Делает доклад.

Для защиты письменного задания отводится не более 20 минут для каждого студента. По ходу защиты задаются вопросы, подтверждающие овладение соответствующими компетенциями.

На заключительном этапе защиты студенту задаются дополнительные вопросы из списка. Вопросы, предоставляются студентам заранее.

После защиты всех работ студентами, объявляется закрытое заседание государственной экзаменационной комиссии для подведения итогов и определения профессиональной объективной оценки научных знаний и практических навыков (компетенций) выпускников на основании экспертизы ответов на задания и поставленные вопросы, и оценки умения студента представлять и защищать их.

5. Фонды оценочных средств государственного экзамена

5.1 Основные требования к ФОС государственного экзамена

Согласно приказу МОН от 19.12.2013 N 1367, фонд оценочных средств государственной итоговой аттестации включает в себя:

- перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы;
- описание показателей и критериев оценивания компетенций, а также шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы.

5.2 Перечень компетенций ГЭ

После полного освоения ОПОП ВО специалитета по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем» выпускник должен обладать следующими компетенциями, перечисленными в таблице 1:

Таблица 1 - Перечень компетенций, формируемых по направлению подготовки

Номер компе-тенции	Содержание компетенции
Выпускник должен обладать общекультурными компетенциями (ОК)	
ОК-1	способностью использовать основы философских знаний для формирования

	мировоззренческой позиции;
ОК-2	способностью использовать основы экономических знаний в различных сферах деятельности;
ОК-3	способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма;
ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности;
ОК-5	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-6	способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;
ОК-7	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-8	способностью к самоорганизации и самообразованию;
ОК-9	способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности;
Выпускник должен обладать общепрофессиональными компетенциями (ОПК)	
ОПК-1	способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач;
ОПК-2	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-3	способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности;
ОПК-4	способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах;
ОПК-5	способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;
ОПК-6	способностью применять нормативные правовые акты в профессиональной деятельности;
ОПК-7	способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций;
ОПК-8	способностью к освоению новых образцов программных, технических средств и информационных технологий;
Выпускник должен обладать профессиональными компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована образовательная программа	
	научно-исследовательская деятельность:
ПК-1	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-2	способностью создавать и исследовать модели автоматизированных систем;
ПК-3	способностью проводить анализ защищенности автоматизированных систем;
ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной

	безопасности автоматизированной системы;
ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы;
ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;
ПК-7	способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;
	проектно-конструкторская деятельность:
ПК-8	способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;
ПК-9	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности;
ПК-10	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-11	способностью разрабатывать политику информационной безопасности автоматизированной системы;
ПК-12	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;
ПК-13	способностью участвовать в проектировании средств защиты информации автоматизированной системы;
	контрольно-аналитическая деятельность:
ПК-14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
ПК-15	способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем;
ПК-16	способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации;
ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;
	организационно-управленческая деятельность:
ПК-18	способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности;
ПК-19	способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;
ПК-20	способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;
ПК-21	способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем;
ПК-22	способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;
ПК-23	способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;
	эксплуатационная деятельность:
ПК-24	способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;

ПК-25	способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;
ПК-26	способностью администрировать подсистему информационной безопасности автоматизированной системы;
ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы;
ПК-28	способностью управлять информационной безопасностью автоматизированной системы;
	Выпускник должен обладать профессиональными компетенциями, соответствующими видам специальной профессиональной деятельности, на которые ориентирована образовательная программа
ПСК-5.1	способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем
ПСК-5.2	способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем
ПСК-5.3	способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью автоматизированных банковских систем
ПСК-5.4	способностью участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных банковских систем
ПСК-5.5	способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы

В ходе теоретического обучения, при прохождении учебной и производственной практик были полностью сформированы и оценены по степени освоения все общекультурные компетенции от ОК-1 до ОК-9, ряд общепрофессиональных компетенций (ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-7).

В процессе государственной итоговой аттестации (ГЭ) по данному направлению подготовки завершается формирование и оценивается степень освоения комплекса компетенций, содержащих наиболее важные общепрофессиональные (ОПК-6, ОПК-8, все профессиональные компетенции и специальные профессиональные компетенции, согласно выбранным видам деятельности (см. таблицу 2)).

Таблица 2 - Перечень компетенций, оцениваемых в ходе процедуры ГЭ

Номер компетенции	Содержание компетенции
ОПК-6	способностью применять нормативные правовые акты в профессиональной деятельности ;
ОПК-8	способностью к освоению новых образцов программных, технических средств и информационных технологий;
ПК-1	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-2	способностью создавать и исследовать модели автоматизированных систем;
ПК-3	способностью проводить анализ защищенности автоматизированных систем;
ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы ;
ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы;
ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере

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

ПК-26	способностью администрировать подсистему информационной безопасности автоматизированной системы;
ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы;
ПК-28	способностью управлять информационной безопасностью автоматизированной системы;
ПСК-5.1	способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем
ПСК-5.2	способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем
ПСК-5.3	способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью автоматизированных банковских систем
ПСК-5.4	способностью участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных банковских систем
ПСК-5.5	способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы

5.3 Показатели, критерии и шкалы оценивания компетенций в ходе ГЭ

Показатели, характеризующие освоение компетенций (ОПК-6, ОПК-8, ПК-1, ПК-2, ПК-3,ПК-4,ПК-5,ПК-6, ПК-7,ПК-8, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16, ПК-17, ПК-18, ПК-19, ПК-20, ПК-21, ПК-22, ПК-23, ПК-24, ПК-25, ПК-26, ПК-27, ПК-28, ПСК-5.1, ПСК-5.2, ПСК-5.3, ПСК-5.4, ПСК-5.5), составляющих комплекс компетенций, определение степени освоения которого позволяет дать общую интегральную оценку сформированности компетенций всей ОПОП ВО, связаны с подготовкой к государственному экзамену и его сдачей. Эти показатели оцениваются путем анализа набора следующих параметров.

1. Соответствие содержания письменной части ответов государственного экзамена заданию, четкость формулировки ответов;
2. Полнота выполнения задания;
3. Владение знаниями нормативных документов;
4. Стиль изложения ответов на письменное задание;
5. Соблюдение стандартов вуза при оформлении ответов на письменную часть;
6. Качество доклада при защите письменной части государственного экзамена;
7. Качество ответов на вопросы устной части экзамена.

Критерии оценивания степени достижения вышеуказанных компетенций и шкала, по которой оценивается степень их освоения, ниже расшифрованы по каждому показателю.

1. ***Соответствие содержания ответов письменной части государственного экзамена заданию, четкость формулировки ответов.***

Шкала оценивания	**5 баллов**	**4 балла**	**3 балла**	**2 балла**
Критерии	Полное соответствие содержания ответов письменной части государственного экзамена заданию, четкость формулировки ответов.	Ответ имеет не значительное несоответствие заданию. Формулировки недостаточно четкие.	К ответу предъявляются существенные замечания. Нет четкого представления о методах решения задания.	Ответы не соответствуют поставленному заданию

2. Полнота выполнения задания.

Шкала оценивания	5 баллов	4 балла	3 балла	2 балла
Критерии	Задания выполнены полностью, с хорошим качеством	Ответ на задание имеет незначительные «огрехи», которые были устранены в ходе устной защиты полученных решений.	Результаты ответа вызывают серьезные замечания.	Ответ на задания неверный.

3. Владение знаниями нормативных документов.

Шкала оценивания	5 баллов	4 балла	3 балла	2 балла
Критерии	В ответах на вопросы продемонстрировано уверенное знание нормативных документов необходимых для решения поставленных задач.	В ответах на вопросы присутствовали незначительные, непринципиальные оговорки, связанные со знанием нормативных документов необходимых для решения поставленных задач.	При ответе использовался неполный комплект необходимых документов или использовались не актуальные нормативные документы.	Незнание нормативных документов, необходимых для решения поставленных задач.

4. Стиль изложения ответов на письменное задание

Шкала оценивания	5 баллов	4 балла	3 балла	2 балла
Критерии	Отмечается научный стиль изложения результатов решения задания.	Имеются незначительные замечания к стилю изложения результатов решения задания	Имеются серьезные замечания к стилю изложения результатов решения.	Стиль изложения не соответствует научному.

5. Соблюдение стандартов вуза при оформлении письменной части государственного экзамена.

Шкала оценивания	5 баллов	4 балла	3 балла	2 балла
Критерии	Оформление решения письменного задания полностью соответствует требованиям ОС ТУСУР 01-2013	Оформление решения письменного задания с незначительными замечаниями соответствует требованиям ОС ТУСУР 01- 2013	Оформление решения письменного задания имеет значительные замечания по соответствию требованиям ОС ТУСУР 01-2013	Оформление решения письменного задания не соответствует требованиям ОС ТУСУР 01-2013

6. Качество доклада при защите письменной части государственного экзамена.

Шкала оценивания	5 баллов	4 балла	3 балла	2 балла
Критерии	Доклад в полной мере отражают содержание решение поставленных задач, продемонстрировано хорошее владение материалом.	Имеются незначительные замечания к докладу. Были допущены незначительные неточности при изложении результатов решения задания.	Имеются существенные замечания к качеству доклада. Были допущены значительные неточности при изложении материала, влияющие на суть понимания решения.	Доклад не отражает сути решения заданий.

7. Качество ответов на вопросы устной части экзамена.

Шкала оценивания	5 баллов	4 балла	3 балла	2 балла

Критерии	Ответы на вопросы даны в полном объеме	ответы даны не полностью и/или с небольшими погрешностями	ответы на вопросы являются неполными, с серьезными погрешностями	ответы на вопросы не даны

Каждый член государственной экзаменационной комиссии выставляет по каждому критерию оценку по пятибалльной шкале. Сумма оценок по всем критериям для каждого члена ГЭК преобразуется в традиционную пятибалльную оценку, согласно таб.3.

Таблица 3 – Формирование оценки члена ГЭК

Сумма баллов по критериям	Оценка члена ГЭК
35-32	Отлично
25-31	Хорошо
21-24	Удовлетворительно
Ниже 21	Неудовлетворительно

Для эффективности и удобства работы членов ГЭК используется вспомогательный документ «Рабочий лист оценки критериев освоения компетенций при проведении ГЭ», рекомендованная форма которого приведена в приложении.

Итоговая оценка сформированности указанных компетенций является оценкой, выставляемой по итогам сдачи ГЭ. Для определения итоговой оценки необходимо вычислить и округлить среднее арифметическое от оценок, выставленных всеми членами государственной комиссии. При возникновении спорных вопросов председатель ГЭК имеет право решающего голоса.

5.4 Типовые контрольные задания

Государственный экзамен в рамках ГИА является комплексным и проводится по следующим дисциплинам:

«Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Управление информационной безопасностью» «Системный анализ», «Криптографические методы защиты информации», «Нормативная база обеспечения информационной безопасности банковской организации», «Моделирование автоматизированных информационных систем», «Распределенные автоматизированные информационные системы».

Требования к письменному этапу экзамена

В ответе на первое задание билета студент должен показать знания, умения и навыки, освоенные в дисциплинах: «Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности», «Управление средствами защиты информации», «Организационное и правовое обеспечение информационной безопасности».

В отчете по первому заданию следует обратить внимание на:

- определение основных законодательных требований к ведению деятельности организации, связанные с обеспечением информационной безопасности. Особое внимание уделить вопросам лицензирования и сертификации;
- выбор средств защиты информации (провести анализ с объяснением причины выбора);
- список нормативно-правовых актов, применяемых в области деятельности организации.

Второе задание связано с дисциплинами: «Основы программирования», «Безопасность программного обеспечения», «Безопасность систем баз данных», «Технологии и методы программирования».

При подготовке к решению второго задания необходимо проработать вопросы, связанные с:

- реляционными моделями баз данных, проектированием реляционной базы данных, нормализацией структуры базы данных, безопасностью баз данных;
- объектно-ориентированным анализом и проектированием;

- функциональным тестированием программного обеспечения, процедурным программированием, рекурсивными функциями;

- видами и способами представления алгоритмов, процедурным программированием, функциями, рекурсивными функциями.

Письменное задание должно быть оформлено с использованием текстового редактора в соответствии с ОС ТУСУР 01-2013 г. http://www.tusur.ru/export/sites/ru.tusur.new/ru/education/documents/inside/tech_01-2013_new.pdf.

Письменное задание направлено на выявления способностей по следующим компетенциям:

способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);

способностью разрабатывать и исследовать модели автоматизированных систем (ПК-2);.

способностью проводить синтез и анализ проектных решений по обеспечению информационной безопасности автоматизированных банковских систем (ПК-8).

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 управлять информационной безопасностью автоматизированной системы (ПК-28).

В письменном задании студенты должны дополнительно показать освоение следующих компетенций:

№	Номер	Компетенция	Примечание
1.	ОПК-5	способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.	Необходимо обосновать решение в письменном задании в соответствии с общенаучными методами.
	ПК-1	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	Обосновать применение соответствующего физико-математического аппарата.
	ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Необходимо обосновать решение в письменном задании в соответствии со одним из методов: анализ; синтез; сравнение; абстрагирование; конкретизация; обобщение; формализация; индукция; дедукция; идеализация; аналогия; моделирование; мысленный эксперимент; воображение.
	ПК-7	способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Правильно оформленное письменное задание в соответствии с ГОСТ 34.XXX, 19.XXX

Для защиты решения письменного задания отводится не более 20 минут. По ходу защиты задаются вопросы, в соответствии с решенными задачами письменного этапа и подтверждающие степень овладения компетенциями:

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 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 документов по защите информации (ПК-16);

способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

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

способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью автоматизированных банковских систем (ПСК-5.3);

способностью участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных банковских систем (ПСК-5.4).

Пример билета письменного этапа государственного экзамена:

Задание 1

Вы участвуете в создании банковской организации. Определите необходимый набор лицензий и документов, необходимых для начала ведения деятельности данным юридическим лицом. Предоставьте базовый набор мер защиты информации, с учетом обрабатываемых в банковской организации персональных данных. Составить рекомендацию по использованию средств защиты информации, сертифицированных по требованиям безопасности информации.

Задание 2

Исследовать заданную предметную область. Выбрать объекты, существенные атрибуты, установить связи между объектами. Задать первичные и внешние ключи. Провести нормализацию базы данный по нормальной форме Бойса-Кодда. Представить структуру нормализованной БД согласно IDEF1X. Представить результаты в виде отчета о проектировании схема базы данных.

Предметная область: Работа с банковскими картами. Карты выдаются только клиентам банка. У клиента при этом должен быть открыт счет. Счет открывается только на одного клиента. У клиента может быть несколько счетов. Карты выдаются по работе с определенным счетом клиента. На один и тот же счет может быть выписано несколько карт. Важно учитывать поступление и снятие денежных средств (где, когда, во сколько и какова сумма операции).

Список источников

1) Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 20.05.2017)

2) Постановление Правительства РФ от 01.11.2012 N1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" http://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения 20.05.2017)

3) Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691 (дата обращения 20.05.2017)

4) Приказ ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности" https://rg.ru/2014/09/17/zashita-dok.html (дата обращения 20.05.2017);

5) Приказ ФСТЭК России от 11.02.2013 N17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения 20.05.2017);

6) Государственный реестр сертифицированных средств защиты информации http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (дата обращения 20.05.2017);

7) Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности" http://legalacts.ru/doc/postanovlenie-pravitelstva-rf-ot-26062013-n-536/ (дата обращения 20.05.2017);

8) Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 20.05.2017);

9) Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения 20.05.2017);

10) Федеральный закон от 02.12.1990 N 395-1 "О банках и банковской деятельности" http://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения 20.05.2017);

11) Инструкция Банка России от 02.04.2010 N 135-И "О порядке принятия Банком России решения о государственной регистрации кредитных организаций и выдаче лицензий на осуществление банковских операций" http://www.consultant.ru/document/cons_doc_LAW_99865/ ;

12) Положение ЦБР от 9 июня 2005 г. N 271-П "О рассмотрении документов, представляемых в территориальное учреждение Банка России для принятия решения о государственной регистрации кредитных организаций, выдаче лицензий на осуществление банковских операций" http://www.consultant.ru/document/cons_doc_LAW_54571/eeb5679e3c5ccae487c71b3bcf35b0463a558df9/ (дата обращения 20.05.2017);

13) Постановление Правительства РФ от 16.04.2012 N 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)" http://www.consultant.ru/document/cons_doc_LAW_128739/ (дата обращения 20.05.2017);

14) Приказ ФСБ РФ от 09.02.2005 N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" http://www.consultant.ru/document/cons_doc_LAW_52098/ (дата обращения 20.05.2017);

15) Федеральный закон от 07.07.2003 N 126-ФЗ "О связи"

http://www.consultant.ru/document/cons_doc_LAW_43224/b819c620a8c698de35861ad4c9d9696ee0c3ee7a/ (дата обращения 20.05.2017);

16) Постановление Правительства РФ от 16.03.2009 N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" (вместе с "Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций") http://www.consultant.ru/document/cons_doc_LAW_85889/ (дата обращения 20.05.2017);

17) Постановление Правительства РФ от 03.02.2012 N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" http://www.consultant.ru/document/cons_doc_LAW_125798/ (дата обращения 20.05.2017);

18) Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г. http://fstec.ru/component/attachments/download/288 (дата обращения 20.05.2017);

19) Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне" http://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения 20.05.2017);

20) Базы данных : Учебное пособие / Е. М. Давыдова, Н. А. Новгородова ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : ТУСУР, 2005. - 127 с. : ил. - Библиогр.: с. 114 (26 экз.);

21) Орлов Сергей Александрович. Технологии разработки программного обеспечения. Разработка сложных программных систем : Учебное пособие для вузов / Сергей Александрович Орлов. - СПб. : Питер, 2002. - 464 с. : ил. - (Учебник для вузов). - Библиогр.: с. 454-457 (25 экз.);

22). Основы программирования на языке С++ : учебное пособие / В. Н. Кирнос ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - 2-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 129[1] с. : ил. - Библиогр.: с. 109 (51 экз.);

23) Страуструп, Бьерн. Язык программирования Си++ : пер. с англ. / Б. Страуструп ; пер.: М. Г. Пиголкин, В. А. Яницкий. - М. : Радио и связь, 1991. - 348, [4] с. - **ISBN** 5-256-00454-9 (в пер.) (31 экз.).

Список дополнительных вопросов.

Дисциплина «Управление средствами защиты информации». Оцениваемые компетенции:

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 управлять информационной безопасностью автоматизированной системы (ПК-28).

Вопросы:

1. Перечислите требования к описанию условий создания и использования защищаемой информации и приведите примеры информационно-технологических ресурсов, подлежащих защите.

2. Приведите перечень направлений классификации угроз информационной безопасности, на основании которых составляются частные модели угроз персональным данным.

3. Охарактеризуйте категории нарушителей в зависимости от наличия доступа, способа доступа и полномочий доступа к автоматизированной системе.

4. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем.

5. Приведите примеры источников информации об инцидентах информационной безопасности и перечислите аспекты анализа этих инцидентов, направленные на совершенствование системы управления информационной безопасностью..

6. Приведите требования к формированию политики информационной безопасности организации и учитываемые в ней категории безопасности.

Список источников

1. Методические рекомендации по обеспечению с помощью криптосредст в безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утв. ФСБ РФ 21.02.2008 N 149/54-144. http://www.consultant.ru/document/cons_doc_LAW_126992/ (дата обращения 20.05.2017)

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утв. ФСТЭК РФ 15.02.2008. http://fstec.ru/component/attachments/download/289 (дата обращения 20.05.2017)

3. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Утв. приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. N 632-ст. http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010 (дата обращения 20.05.2017)

4. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. N 513-ст. http://docs.cntd.ru/document/1200068822 (дата обращения 20.05.2017)

5. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Утв. приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. N 423-ст. http://docs.cntd.ru/document/1200103619 (дата обращения 20.05.2017)

Дисциплина «Системный анализ». Оцениваемые компетенции:

способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);

способностью создавать и исследовать модели автоматизированных систем (ПК-2).

Вопросы:

1. Представьте и объясните алгоритм анализа проекторного решения.

2. Какие модели порождает процедура анализа проектного решения. Их место и назначение в процедуре анализа проектного решения.

3. Представьте и объясните алгоритм синтеза проекторного решения.

4. Какие модели порождает процедура синтеза проектного решения. Их место и назначение в процедуре синтеза проектного решения.

Список источников

1.Прикладной системный анализ : учебное пособие / Ф.П. Тарасенко. — М. : КНОРУС, 2010. — 224 с. , с. 59-61. (61 экз.)

Дисциплины «Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности».

Оцениваемые компетенции:

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 участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

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);

способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

Вопросы:

1. Обоснуйте необходимость использования систем обнаружения вторжений. Приведите примеры, проанализируйте и коротко опишите существующие решения.
2. Обоснуйте необходимость использования средств защиты информации от несанкционированного доступа. Приведите примеры, проанализируйте и коротко опишите существующие решения.
3. Опишите модель разработки защищенных автоматизированных систем в соответствии с ГОСТ Р ИСО/МЭК 15408-1-2012 "Критерии оценки безопасности информационных технологий" ("Общие критерии").
4. Дайте определение понятию "Профиль защиты". Опишите назначение профиля защиты с точки зрения разработки защищенных автоматизированных систем (ГОСТ Р ИСО/МЭК 15408-1-2012).
5. Перечислите и кратко опишите разделы технического задания на создание автоматизированной системы (ГОСТ 34.602-89).
6. Перечислите классы функциональных требований безопасности ГОСТ Р ИСО/МЭК 15408-2-2012. Опишите один из классов на примере базового профиля защиты операционных систем общего назначения.
7. Перечислите и опишите этапы разработки системы управления информационной безопасностью (ГОСТ Р ИСО/МЭК 27001).
8. Перечислите и опишите основные варианты стратегии анализа рисков организации (ГОСТ Р ИСО/МЭК 27005-2010).
9. Сформулируйте стадии проектирования средств защиты информации и средств контроля защищенности автоматизированной системы.
10. Опишите многоуровневый подход к построению компьютерных сетей. Модели OSI, TCP/IP.
11. Планирование и управление сетевой безопасностью. Кратко изложите общий процесс достижения и поддержки необходимой сетевой безопасности (ГОСТ Р ИСО/МЭК 27033-1-2011).
12. Перечислите основные этапы, исходные данные и критерии отнесения автоматизированной системы к классам защищенности от НСД к информации (РД АС. Защита от НСД к информации. Классификация АС и требования по ЗИ).

Список источников

1. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства

обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель [Текст]. - Введ. 2012-11-15. - М.: Стандартинформ, 2014. http://docs.cntd.ru/document/1200101777 (дата обращения 20.05.2017)

2. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности [Текст]. - Введ. 2013-11-08. - М.: Стандартинформ, 2014. http://docs.cntd.ru/document/1200105710 (дата обращения 20.05.2017)

3. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы [Текст]. - Введ. 1990-01-01. - М.: ИПК ИЗДАТЕЛЬСТВО СТАНДАРТОВ, 2004. http://docs.cntd.ru/document/1200006924 (дата обращения 20.05.2017)

4. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования [Текст]. - Введ. 2006-12-27. - М.: Стандартинформ, 2008. http://docs.cntd.ru/document/gost-r-iso-mek-27001-2006 (дата обращения 20.05.2017)

5. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности [Текст]. - Введ. 2011-12-01. - М.: Стандартинформ, 2011. http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010 (дата обращения 20.05.2017)

6. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции [Текст]. - Введ. 2012-01-01. - М.: Стандартинформ, 2012. http://docs.cntd.ru/document/1200089172 (дата обращения 20.05.2017)

7. Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации [Текст]: . Утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. 29 с. http://fstec.ru/component/attachments/download/296

8. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания [Текст]. - Введ. 1992-01-01. - М.: Стандартинформ, 2009. http://docs.cntd.ru/document/1200006921 (дата обращения 20.05.2017)

9. Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты [Электронный ресурс] // Режим доступа: http://fstec.ru/component/attachments/download/317 (дата обращения 20.05.2017)

10. Олифер, Виктор Григорьевич. Компьютерные сети: Принципы, технологии, протоколы : Учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. - 3-е изд. - СПб. : Питер, 2007. - 957[3] с. : ил. - (Учебник для вузов). - Библиогр.: с. 919-921. - **ISBN** 978-5-469-00504-9 (40 экз.)

11. Комплексная защита информации в корпоративных системах [Текст] : учебное пособие для вузов / В. Ф. Шаньгин. - М. : ФОРУМ, 2012 ; М. : ИНФРА-М, 2012. - 592 с. : ил. (30 экз.)

Дисциплина «Криптографические методы защиты информации». Оцениваемые компетенции:

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).

Вопросы:

1. Каким образом может быть проведен анализ автоматизированной системы на предмет возможности утечки права доступа?

2. Каким образом может быть формализована политика разграничения прав доступа в

автоматизированной системе?

3. Для обеспечения свойств конфиденциальности и целостности информации в автоматизированной банковской системе используется протокол, основанный на использовании отечественных криптографических стандартов. Предложите формат пакета данных для такого протокола.

4. Перечислите и охарактеризуйте задачи информационной безопасности, для решения которых предназначен стандарт ГОСТ 28147-89?

5. Укажите, каким образом связаны между собой криптографические стандарты ГОСТ Р 34.10 и ГОСТ Р 34.11.

6. Каким образом пользователь может удостовериться в аутентичности открытого ключа другого пользователя, который содержится в сертификате, выданном центром сертификации, неизвестным первому пользователю?

Список источников

1. Мещеряков Р.В. Теоретические основы компьютерной безопасности: учебное пособие для студентов специальности 075500 / Р. В. Мещеряков, Г. А. Праскурин. — 2-е изд., перераб. и доп. — Томск: В-Спектр, 2007. — 343 с. (52 экз.)

2. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах.— М.: Радио и связь, 2006. — 175 с. (60 экз.)

1. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 479 с. (30 экз.)

2. Рябко, Борис Яковлевич. Криптографические методы защиты информации : Учебное пособие для вузов / Б. Я. Рябко, А. Н. Фионов. - М. : Горячая линия-Телеком, 2005. - 229[3] с. - (Специальность для высших учебных заведений). - (30 экз.)

3. Смарт Н. Криптография: учебник для вузов. — М.: Техносфера, 2005. — 525 с. (11 экз.)

4. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — М.: ИПК Издательство стандартов, 1996. — 26 с. http://docs.cntd.ru/document/1200007350 (дата обращения 20.05.2017)

5. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. — М.: Стандартинформ, 2015. — 21 с. http://docs.cntd.ru/document/1200121984 (дата обращения 20.05.2017)

6. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. — М.: Стандартинформ, 2015. — 38 с. http://docs.cntd.ru/document/1200121984 (дата обращения 20.05.2017)

7. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. — М.: Стандартинформ, 2012. — 34 с. http://docs.cntd.ru/document/1200095035 (дата обращения 20.05.2017)

8. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М.: Стандартинформ, 2012. — 29 с. http://docs.cntd.ru/document/1200095034 (дата обращения 20.05.2017)

Дисциплина «Организационное и правовое обеспечение информационной безопасности». Оцениваемые компетенция:

способностью создавать и исследовать модели автоматизированных систем (ПК-2);

способностью проводить анализ защищенности автоматизированных систем (ПК-3);

способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

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).

Вопросы:

1. Приведите типовую/возможную структуру инструкции по парольной защите.
2. Приведите типовую/возможную структуру должностной инструкции специалиста по защите информации.

Список источников

1) "Квалификационный справочник должностей руководителей, специалистов и других служащих" (утв. Постановлением Минтруда России от 21.08.1998 N 37) (ред. От 12.02.2014). http://base.garant.ru/180422/ (дата обращения 20.05.2017)

2) Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - М.: Горячая линия — Телеком, 2009. - 552 с.: ил.

3)Приказ Роспатента от 14.07.2015 N 97 "Об утверждении Положения по организации парольной защиты в Федеральной службе по интеллектуальной собственности". http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=633381#0 (дата обращения 20.05.2017)

4)Приказ ФАС России от 23.10.2012 N 654 "Об утверждении Положения по организации парольной защиты автоматизированных систем Федеральной антимонопольной службы". http://lawru.info/dok/2012/10/23/n164349.htm (дата обращения 20.05.2017)

5)Приказ Роспатента от 05.07.2013 N 82 "Об утверждении инструкций по обеспечению режима секретности при обработке секретной информации с использованием компьютерной системы в режимно-секретном подразделении Роспатента". http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=565173#0 (дата обращения 20.05.2017)

Дисциплина «Нормативная база обеспечения информационной безопасности банковской организации». Оцениваемые компетенции:

способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем (ПСК-5.1);

способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем (ПСК-5.2);

способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы (ПСК-5.5);

Вопросы:

1. Опишите комплекс отраслевых стандартов (СТО БР ИББС) и рекомендаций (РС БР ИББС) Центрального Банка Российской Федерации в области информационной безопасности банковской системы Российской Федерации.
2. Какова общая политика информационной безопасности банковской организации.
3. Поясните назначение РАБИС-НП в банковской системе РФ
4. Какие средства и методы технической защиты информации, используются в банковской системе РФ.

Список источников

1. "Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" СТО БР ИББС-1.0-2014" (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399). http://www.cbr.ru/credit/gubzi_docs/st-10-14.pdf (дата обращения 20.05.2017)

2. "Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной

безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014" СТО БР ИББС-1.2-2014" (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399). http://www.cbr.ru/credit/gubzi_docs/st-10-14.pdf (дата обращения 20.05.2017)

Дисциплина «Распределенные автоматизированные информационные системы». Оцениваемые компетенции:

способностью проводить анализ защищенности автоматизированных систем (ПК-3);

способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26).

Вопросы:

1. Опишите комплекс мер для обеспечения информационной безопасности автоматизированной системы на базе автоматизированного рабочего места без подключения к вычислительной сети. Какие нормативные документы регламентируют состав и содержание мер для обеспечения информационной безопасности?
2. Опишите различие в подходах к обеспечению информационной безопасности для локальных и распределенных информационных систем. Какие дополнительные меры обеспечения информационной безопасности необходимо применять для защиты распределенных информационных систем?

Список источников

1. Федеральный закон от 27.07.206 №149 «Об информации, информационных технологиях и о защите информации»; http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 20.05.2017)
2. Федеральный закон от 27.07.2006 №152 «О персональных данных»; http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 20.05.2017)
3. Постановление Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; http://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения 20.05.2017)
4. Приказ ФСТЭК от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»; http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения 20.05.2017);
5. Приказ ФСТЭК от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691(дата обращения 20.05.2017)
6. Приказ ФСБ от 10.07.2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности». https://rg.ru/2014/09/17/zashita-dok.html (дата обращения 20.05.2017)

Дисциплина «Моделирование автоматизированных информационных систем». Оцениваемые компетенции:

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 методы научных исследований в профессиональной

деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);

способностью создавать и исследовать модели автоматизированных систем (ПК-2).

Вопросы:

1. С каких работ следует начинать разработку модели автоматизированной системы?
2. Какие методы исследования модели применяются для автоматизированных систем?

Список источников

1 Решетникова, Г.Н. Моделирование систем : Учебное пособие / Г. Н. Решетникова; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники. - 2-е изд., перераб. и доп. - Томск : ТУСУР, 2007. - 440 с. (70 экз.)

2 Серафинович Л.П. Основы теории подобия и моделирования : учебное пособие / Л. П. Серафинович; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск: ТУСУР, 2005. - 202 с. (131 экз.)

5.5 Методические материалы процедуры оценивания результатов ГЭ

5.5.1. Основная литература ГЭ

1 ФЕДЕРАЛЬНЫЙ ЗАКОН ОБ ОБРАЗОВАНИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ от 29.12.2012 N 273-ФЗ. [Электронный ресурс]. URL: http://fgosvo.ru/support/downloads/1102/?f=uploadfiles/zakony/273_02_2015.pdf (дата обращения 22.05.2017)

2 Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры. Приказ Минобрнауки России от 29.06.2015 № 636 (в ред. от 28.04.2016 №502) [Электронный ресурс] http://old.tusur.ru/export/sites/ru.tusur.new/ru/education/documents/federal/9-1_2016.doc . (дата обращения 22.05.2017)

3 Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета) Утвержден приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. N 1509 [электронный ресурс]. http://fgosvo.ru/uploadfiles/fgosvospec/100503.pdf (дата обращения 23.05.2017)

5.5.2 Учебно-методические пособия ГЭ

1 Образовательный стандарт вуза ОС ТУСУР 01-2013. Работы студенческие по направлениям подготовки и специальностям технического профиля. Общие требования и правила оформления. Введен приказом ректора от 03.12.2013 г. №14103. [Электронный ресурс]. URL: http://old.tusur.ru/export/sites/ru.tusur.new/ru/education/documents/inside/tech_01-2013_new.pdf (дата обращения 23.05.2017)

2 Положение о проверке самостоятельности выполнения письменных работ бакалавров, специалистов и магистров в ТУСУРе. Введено в действие распоряжением ректора от 26.05.2016 №77. [Электронный ресурс]. URL: http://old.tusur.ru/export/sites/ru.tusur.new/ru/education/documents/inside/14.12_2016_1.doc (дата обращения 22.05.2017)

4 Давыдова Е.М. Методические указания к госэкзамену по специальности ИБАС http://kibevs.tusur.ru/sites/default/files/files/upload/notes/2017.05.12/metodicheskie_ukazaniya_k_gosekzamenu_ibas_2017.pdf 2017г. 22с. (дата обращения 22.05.2017)

6. Необходимая материально-техническая база проведения ГЭ

Для подготовки к процедуре сдачи ГЭ работы необходимо помещение, в котором рабочие места имеют площадь не менее 3 $м^2$ и оборудованы:

- наличием компьютерного класса, подключенного к сети Интернет, оснащенного лицензионным программным обеспечением, в состав которого входит:
- MS OFFICE;
- Visual Studio 2012;
- Oracle VM VirtualBox;
- VMware Player.

Для проведения процедуры сдачи ГЭ работы необходимо помещение, вместимостью от 20 и более человек, в котором оборудованы рабочие места для всех членов ГЭК, с возможностью выслушивать доклады, просматривать публичные презентации выступающих, вести записи и протоколы, имеются места для слушателей, желающих присутствовать на процедуре сдачи ГЭ. В состав необходимого оборудования помещения входит:

- аппаратура для публичных презентаций результатов ГЭ, содержащая экран, проектор,
- доска для иллюстрации ответов на вопросы.

7. Проведение ГЭ для лиц с ограниченными возможностями здоровья

Форма проведения государственной итоговой аттестации (ГЭ) для обучающихся из числа лиц с ограниченными возможностями здоровья (инвалидностью) устанавливается с учетом индивидуальных психофизических особенностей в формах, адаптированных к ограничениям их здоровья и восприятия информации (устно, письменно на бумаге, письменно на компьютере и т.п.).

Подготовка и сдача ГЭ для студентов из числа лиц с ограниченными возможностями здоровья осуществляется с использованием средств общего и специального назначения. Перечень используемого материально-технического обеспечения:

- учебные аудитории, оборудованные компьютерами с выходом в интернет, видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном;
- библиотека, имеющая рабочие места для студентов, оборудованные доступом к базам данных и интернетом;
- компьютерные классы;
- аудитория Центра сопровождения студентов с инвалидностью с компьютером, оснащенная специализированным программным обеспечением для студентов с нарушениями зрения, устройствами для ввода и вывода голосовой информации.

Для лиц с нарушениями зрения материалы предоставляются:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в печатной форме;
- в форме электронного документа.

Для лиц с нарушением опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа.

Сдача ГЭ для лиц с нарушениями зрения проводится в устной форме без предоставления студентом решения на экране. На время защиты в аудитории должна быть обеспечена полная тишина, продолжительность защиты увеличивается до 1 часа (при необходимости). Гарантируется допуск в аудиторию, где проходит сдача ГЭ, собаки-проводника при наличии документа, подтверждающего ее специальное обучение, выданного по форме и в порядке, утвержденных приказом Министерства труда и социальной защиты Российской Федерации 21 июля 2015г.,

регистрационный номер 38115).

Для лиц с нарушениями слуха сдача ГЭ проводится без предоставления устного доклада. Вопросы комиссии и ответы на них представляются в письменной форме. В случае необходимости, вуз обеспечивает предоставление услуг сурдопереводчика.

Для студентов с нарушениями опорно-двигательного аппарата сдача ГЭ проводится в аудитории, оборудованной в соответствии с требованиями доступности. Помещения, где могут находиться люди на креслах-колясках, должны размещаться на уровне доступного входа или предусматривать пандусы, подъемные платформы для людей с ограниченными возможностями или лифты. В аудитории должно быть предусмотрено место для размещения студента на коляске.

Дополнительные требования к материально-технической базе, необходимой для сдачи ГЭ лицом с ограниченными возможностями здоровья, студент должен предоставить на кафедру не позднее, чем за два месяца до проведения процедуры защиты.

Приложение
Рабочий лист оценки критериев освоения компетенций при проведении ГЭ

Член ГЭК _____ Кафедра _____ Группа _____ Направление _____

ФИО члена ГЭК **Выпускающая кафедра** **Номер группы** **Код направления подготовки, и профиль**

	ФИО студента / **Критерий** / **(Оценки от 2 до 5)**														
1	Соответствие содержания письменной части ответов государственного экзамена заданию, четкость формулировки ответов														
2	Полнота выполнения задания														
3	Владение знаниями нормативных документов														
4	Стиль изложения ответов на письменное задание														
5	Соблюдение стандартов вуза при оформлении ответов на письменную часть														
6	Качество доклада при защите письменной части государственного экзамена														
7	Качество ответов на вопросы устной части экзамена														
	Сумма баллов														
	Итоговая оценка														

Подпись члена ГЭК_____