МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

Подготовка к сдаче и сдача государственного экзамена

Уровень образования: **высшее образование - специалитет**
Направление подготовки/специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль)/специализация: **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронновычислительных систем**
Курс: 5
Семестр: 10

Учебный план набора 2013, 2014, 2015 года.

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

Томск 2018

Согласована на портале № 38360

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 15 » 5 2018 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа государственного экзамена 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 №1509, рассмотрена и утверждена на заседании кафедры «15» мая 2018 года, протокол № 6.

Разработчик:

Доцент каф. КИБЭВС _____ Е. М. Давыдова

Заведующий каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа согласована с факультетом и экспертами.

Декан ФБ _____ Е. М. Давыдова

Эксперты:

Доцент каф. КИБЭВС _____ А. А. Конев

Доцент каф. КИБЭВС _____ К.С. Сарин

Согласована на портале № 38360

1. Общие положения

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. Цели и задачи проведения государственного экзамена

Целью проведения ГЭ является комплексная оценка полученных за период обучения теоретических знаний и практических навыков выпускника и проверка сформированности компетенций, необходимых в профессиональной деятельности в соответствии с требованиями по направлению подготовки (специальности) 10.05.03.

Задачей проведения государственного экзамена является выявление способностей обучающихся к решению теоретических и практических задач, имеющих определяющее значение для профессиональной деятельности выпускников.

3. место государственного экзамена в структуре ОПОП ВО и его объем

Согласно ФГОС ВО по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем» государственный экзамен в составе ГИА входит в блок 3и относится к базовой части образовательной программы.

Трудоемкость подготовки к сдаче и сдача государственного экзамена составляет 3 з.е.

4. Допуск к государственному экзамену

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

Государственный экзамен является этапом государственной итоговой аттестации и завершается выставлением оценки.

5 Проведение государственного экзамена

5.1 Нормативные требования

Согласно требованиям приказа Министерства образования и науки Российской Федерации от 29.06.2015 г. №636 «Порядок проведения государственной итоговой аттестации по образова-

Согласована на портале № 38360

тельным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры» государственный экзамен проводится по одной или нескольким дисциплинам и (или) модулям образовательной программы, результаты освоения которых имеют определенное значение для профессиональной деятельности выпускников. Государственный экзамен проводится устно или письменно.

Программа государственного экзамена, критерии оценки результатов сдачи государственного экзамена, а также порядок подачи и рассмотрения апелляций доводятся до сведения обучающихся не позднее, чем за шесть месяцев до начала ГИА.

Программа государственного экзамена содержит перечень вопросов, выносимых на государственный экзамен, и рекомендации обучающимся по подготовке к государственному экзамену, в том числе перечень рекомендуемой литературы для подготовки к государственному экзамену.

Перед государственным экзаменом проводятся консультации обучающихся по вопросам, включенным в программу государственного экзамена.

Государственный экзамен, как элемент ГИА, проводятся в форме контактной работы и в форме самостоятельной работы обучающихся. Объем контактной работы при проведении ГЭ, определяется согласно локальному акту «Положению о контактной работе обучающихся в ТУСУРе».

5.2 Процедура проведения государственного экзамена

Государственный экзамен по данному направлению подготовки (специальности) проводится по следующим дисциплинам:

- «Разработка и эксплуатация защищенных автоматизированных систем»,
- «Программно-аппаратные средства обеспечения информационной безопасности»,
- «Управление средствами защиты информации»,
- «Организационное и правовое обеспечение информационной безопасности».
- «Основы программирования»,
- «Безопасность программного обеспечения»,
- «Безопасность систем баз данных»,
- «Технологии и методы программирования».
- «Системный анализ»,
- «Криптографические методы защиты информации»,
- «Нормативная база обеспечения информационной безопасности банковской организации».

Проведение ГЭ осуществляет государственная экзаменационная комиссия, утвержденная приказом по вузу.

Каждый экзаменационный билет ГЭ состоит из 2 задач, выбираемых случайным образом из перечня вопросов (задач) по дисциплинам, включенной в состав ГЭ.

Количество билетов определяется на выпускающей кафедре и должно составлять не менее 110% от количества сдающих ГЭ.

Ежегодно проводиться обновление экзаменационных билетов в частичном объеме, но не менее 25% от общего числа билетов.

Экзаменационные билеты хранятся на выпускающей кафедре в защищенном от свободного доступа месте.

Дата проведения государственного экзамена устанавливается расписанием, которое формирует бюро расписания и согласует с выпускающей кафедрой.

Сдача ГЭ начинается с 09.00 часов. Продолжительность сдачи ГЭ составляет не более 3,5 астрономических часов.

Государственный экзамен проводится в комбинированной форме.

Согласована на портале № 38360

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 обучающийся случайным образом выбирает один экзаменационный билет для выполнения письменного этапа. В билете два задания. На выполнение заданий письменного этапа отводится 3часа 20 минут (часы астрономические). Из них 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». В 12-20 закрывается доступ к разделу государственный экзамен.

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 15-20 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.

Результаты государственного экзамена и общую оценку комплексной подготовки каждого обучающегося государственная экзаменационная комиссия принимает на закрытом совещании. Все заседания и решения ГЭК по приему государственного экзамена протоколируются. Результаты ГЭ заносятся в протокол заседания государственной экзаменационной комиссии и оглашаются в день проведения ГЭ.

В протоколе заседания государственной экзаменационной комиссии по приему государственного экзамена отражаются перечень заданных обучающемуся вопросов и характеристика ответов на них, мнения председателя и членов ГЭК о выявленном в ходе государственного экзамена уровне подготовленности обучающегося к решению профессиональных задач, оценка сформированности компетенций, а также информация о выявленных недостатках в теоретической и практической подготовке обучающегося. Протоколы являются документами строгой отчетности и хранятся в соответствии с номенклатурой ведения дел кафедры.

Оценка по государственному экзамену выставляется по четырех бальной шкале: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Результаты сдачи государственного экзамена записываются в приложение к диплому

5.3. Перечень компетенций, оцениваемых в ходе государственного экзамена

В процессе сдачи ГЭ оценивается степень освоения указанных в РУП компетенций, имеющих определяющее значение для профессиональной деятельности выпускников:

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 разви-

Согласована на портале № 38360

тия 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;

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;

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-

Согласована на портале № 38360

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-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 сис-

Согласована на портале № 38360

темы;

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.

5.4 Показатели, критерии и шкалы оценивания компетенций в ходе ГЭ

Показатели освоения указанных выше компетенций оцениваются путем анализа набора следующих параметров:

- уверенные знания, умения и навыки в рассмотрении всех вопросов и решении задач экзаменационного билета;
- знание производственной ситуации и умение применить правильный научный и методический подход и инструментарий для решения задач;
- умение выделять приоритетные направления в профессиональной области;
- способность устанавливать причинно-следственные связи в изложении материала, делать выводы;
- обоснованность, четкость, полнота изложения ответов;
- общий (культурный) и специальный (профессиональный) язык ответов;
- подготовленность обучающегося к решению профессиональных задач.

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

1. Уверенные знания, умения и навыки в рассмотрении предложенного вопроса:

Шкала оценивания	**5 баллов**	**4 балла**	**3 балла**	**2 балла**
Критерии	Получены полные ответы на все вопросы экзаменационного билета с привлечением математического аппарата, продемонстрировано понимание междисциплинарных связей, имеется целостное представление о процессах и явлениях в природе, показана способность использовать известные методы и модели для количественного и качественного описания процессов и объектов, относящихся к профессиональной деятельности	Получены ответы на все вопросы экзаменационного билета с использованием основных формул и соотношений при ответе на некоторые вопросы, продемонстрировано умение давать ответы на междисциплинарные вопросы и целостное представление о процессах и явлениях в природе при ориентации в вопросах, относящихся к профессиональной деятельности	Получены ответы не менее чем на 50% вопросов экзаменационного билета на удовлетворительном уровне, подтверждена ориентация в вопросах междисциплинарного характера, имеется общее представление об описании процессов и объектов, относящихся к области профессиональной деятельности	при ответах не раскрыта сущность вопросов, нет ориентации в междисциплинарных связях и в вопросах, относящихся к профессиональной деятельности

Согласована на портале № 38360

2. Знание производственной ситуации и умение применить правильный научный и методический подход и инструментарий для решения задач:

Шкала оценивания	5 баллов	4 балла	3 балла	2 балла
Критерии	Обучающийся демонстрирует глубокие знания производственной ситуации и умеет применять правильный научный и методический подход и инструментарий для решения задач, понимает сущности рассматриваемых явлений и закономерностей, принципов и теорий	Обучающийся обнаруживает достаточные знания производственной ситуации и умеет применять основные научные и методические подходы и инструментарии для решения задач, но затрудняется в приведении примеров	Обучающийся обнаруживает посредственные знания производственной ситуации, умеет применять основные научные и методические подходы и инструментарии для решения задач, но раскрывает материал неполно, делает неточности	Обучающийся обнаруживает разрозненные бессистемные знания производственной ситуации и не умеет применять основные научные и методические подходы и инструментарии для решения задач или вообще отказывается от ответа

3. Умение выделять приоритетные направления в профессиональной области:

Шкала оценивания	5 баллов	4 балла	3 балла	2 балла
Критерии	Обучающийся умеет выделять приоритетные направления в профессиональной области, приводит примеры применения данных направлений в различных сферах деятельности.	Обучающийся умеет выделять основные направления в профессиональной области, но затрудняется в приведении примеров	Обучающийся умеет выделять основные направления в профессиональной области, но раскрывает материал неполно, делает неточности.	Обучающийся не умеет выделять основные направления в профессиональной области или вообще отказывается от ответа

4. Способность устанавливать причинно-следственные связи в изложении материала, делать выводы:

Шкала оценивания	5 баллов	4 балла	3 балла	2 балла
Критерии	Обучающийся умеет выделять существенные связи в рассматриваемых явлениях, делает обоснованные выводы	Обучающийся умеет выделять основные связи в рассматриваемых явлениях, но затрудняется с обоснованием выводов	Обучающийся умеет выделять основные связи в рассматриваемых явлениях, совершает существенные ошибки в обосновании выводов	Обучающийся не умеет выделять основные связи в рассматриваемых явлениях, совершает грубые ошибки в обосновании выводов или вообще отказывается от ответа

5. Обоснованность, четкость, полнота изложения ответов:

Шкала оценивания	5 баллов	4 балла	3 балла	2 балла
Критерии	Обучающийся даёт точное, полное определение основным понятиям, связывает теорию с практикой, решает прикладные задачи, грамотно аргументирует свои суждения.	Обучающийся даёт точное, полное определение основным понятиям, связывает теорию с практикой, решает прикладные задачи, но затрудняется в приведении примеров. При ответе допускает отдельные неточности	Обучающийся излагает основное содержание учебного материала, но раскрывает материал неполно, непоследовательно, допускает неточности в определении понятий, не умеет доказательно обосновать свои суждения	Обучающийся демонстрирует разрозненные бессистемные знания, беспорядочно, неуверенно излагает материал или вообще отказывается от ответа

6. Общий (культурный) и специальный (профессиональный) язык ответа:

Шкала оценивания	5 баллов	4 балла	3 балла	2 балла

Согласована на портале № 38360

Критерии	Обучающийся грамотно владеет профессиональной терминологией, связно излагает свой ответ	Обучающийся грамотно владеет профессиональной терминологией, связно излагает свой ответ, но допускает неточности	Обучающийся слабо владеет профессиональной терминологией, допускает неточности, допускает ошибки в изложении ответа	Обучающийся не владеет профессиональной терминологией, бессвязно, неуверенно излагает свой ответ или вообще отказывается от ответа

7. Подготовленность обучающегося к решению профессиональных задач:

Шкала оценивания	**5 баллов**	**4 балла**	**3 балла**	**2 балла**
Критерии	Обучающийся полностью готов к решению профессиональных задач по всем предусмотренным ОПОП видам деятельности	Обучающийся готов к решению профессиональных задач по всем предусмотренным ОПОП видам деятельности, но допускает неточности	Обучающийся готов к решению профессиональных задач но не по всем по видам деятельности, предусмотренным ОПОП	Обучающийся не готов к решению профессиональных задач ни по одному из предусмотренных ОПОП виду деятельности

Каждый член государственной экзаменационной комиссии выставляет по каждому критерию оценку по пятибалльной шкале. Рабочий лист оценки критериев освоения компетенций при проведении ГЭ приведен в ПРИЛОЖЕНИИ А. Сумма оценок по всем критериям для каждого члена ГЭК преобразуется в традиционную пятибалльную оценку, согласно таблице 2.

Таблица 2 – Формирование оценки члена ГЭК

Сумма баллов по критериям	**Оценка члена ГЭК**
32-35	Отлично
25-31	Хорошо
18-24	Удовлетворительно
Ниже 18	Неудовлетворительно

6. Оценочные материалы государственного экзамена

6.1. Материалы для письменного этапа проведения ГЭ

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;

Согласована на портале № 38360

- 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. https://storage.tusur.ru/files/40668/rules_tech_01-2013.pdf .

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).

Основная литература для подготовки к письменному этапу:

1) Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" http://www.consultant.ru/document/cons_doc_LAW_61801/ (Дата доступа 15.05.2018г.);

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 доступа 15.05.2018г.);

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 доступа 15.05.2018г.);

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 доступа 15.05.2018г.);

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 доступа 15.05.2018г.);

6) Государственный реестр сертифицированных средств защиты информации http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-

Согласована на портале № 38360

sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (Дата доступа 15.05.2018г.);

7) Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности" http://www.consultant.ru/document/cons_doc_LAW_113658/ (Дата доступа 15.05.2018г.);

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/ ;

9) Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" http://www.consultant.ru/document/cons_doc_LAW_112701/ (Дата доступа 15.05.2018г.);

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 доступа 15.05.2018г.);

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/ (Дата доступа 15.05.2018г.);

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 доступа 15.05.2018г.);

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 доступа 15.05.2018г.);

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 доступа 15.05.2018г.);

15) Федеральный закон от 07.07.2003 N 126-ФЗ "О связи" http://www.consultant.ru/document/cons_doc_LAW_43224/b819c620a8c698de35861ad4c9d9696ee0c3ee7a/ (Дата доступа 15.05.2018г.);

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 доступа 15.05.2018г.) ;

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 доступа 15.05.2018г.);

Согласована на портале № 38360

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 доступа 15.05.2018г.);

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 доступа 15.05.2018г.);

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.).

Дополнительная литература для подготовки к письменному этапу:

1) Шелупанов, Александр Александрович. Информатика. Базовый курс [Электронный учебник] : учебник. Ч. 3 : Основы алгоритмизации и программирования в среде Visual C++ 2005. - Томск , 2008 on-line ; 216 с. https://edu.tusur.ru/publications/521

2) Давыдов, Владимир Григорьевич. Программирование и основы алгоритмизации : Учебное пособие для вузов. - М. : Высшая школа , 2005. - 448 с. (69 экз.)

3) Култыгин, О. П. Администрирование баз данных. СУБД MS SQL Server [Электронный ресурс] : учеб. пособие / О. П. Култыгин. - М.: МФПА, 2012. - 232 с. - (Университетская серия). - ISBN 978-5-4257-0026-1. http://znanium.com/catalog/product/451114 .

4) Нормативно-правовые акты информационной безопасности : учебное пособие: В 5 ч. / А. А. Шелупанов [и др.] ; Министерство образования и науки Российской Федерации, Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности, Кафедра комплексной информационной безопасности электронно-вычислительных систем, Сибирское региональное отделение учебно-методического объединения вузов России по образованию в области информационной безопасности. - Томск : В-Спектр, 2007 - . - ISBN 978-5-91191-052-7. Ч. 1. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 214[2] с. : табл. - ISBN 978-5-91191-053-5 (81 экз.)

5) Нормативно-правовые акты информационной безопасности : учебное пособие: В 5 ч. / А. А. Шелупанов [и др.] ; Министерство образования и науки Российской Федерации, Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности, Кафедра комплексной информационной безопасности электронно-вычислительных систем, Сибирское региональное отделение учебно-методического объединения вузов России по образованию в области информационной безопасности. - Томск : В-Спектр, 2007 - ISBN 978-5-91191-052-7. Ч. 2. - 3-е изд., перераб. и доп. (81 экз.)

Согласована на портале № 38360

6.2 Список дополнительных вопросов.

Дисциплина «Управление средствами защиты информации»

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.
7. Для чего предназначен механизм контроля целостности?
8. Приведите и поясните несколько категорий регистрации событий?
9. В какой последовательности применяются параметры групповых политик?
10. Для каких устройств может осуществляться теневое копирование?

Основная литература по дисциплине:

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 доступа 15.05.2018г.)
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 доступа 15.05.2018г.)
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 доступа 15.05.2018г.)
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 доступа 15.05.2018г.)
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 доступа 15.05.2018г.)

Дополнительная литература по дисциплине:

1. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2018. — 592 с. — (Высшее образование: Бакалавриат). http://znanium.com/catalog/product/937502 (Дата доступа 15.05.2018г.)

Согласована на портале № 38360

2. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с. http://znanium.com/catalog/product/489084 (Дата доступа 15.05.2018г.)

Дисциплина «Системный анализ»

Вопросы:

1. Представьте и объясните алгоритм анализа проектного 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.
5. Раскройте понятие системы и её элементов.
6. Укажите основные характеристические свойства системы.
7. Сформулируйте понятие цель системы, приведите примеры классификации систем
8. Сформулируйте базовый алгоритм построения дерева целей
9. Приведите примеры методов согласования мнений экспертов
10. Виды шкал и оценивание характеристик систем

Основная литература по дисциплине:

1. Основы системного анализа : Учебное пособие / А. А. Шумский, А. А. Шелупанов ; 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 : Спектр, 2007. - 218[2] с. : ил., табл. - (Приоритетные национальные проекты. Образование). - Библиогр.: с. 183. Доступно в библиотеке: 103 экземпляра.

2. Основы системного анализа : учебник / Ф. И. Перегудов, Ф. П. Тарасенко. - 3-е изд. - Томск : Издательство научно-технической литературы, 2001. - 390 с. : ил. - Библиогр. в конце глав. - ISBN 5-89503-115-3 Доступно в библиотеке: 103 экземпляра.

Дополнительная литература по дисциплине:

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».

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).

Согласована на портале № 38360

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).

Основная литература по дисциплиннам:

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 доступа 15.05.2018г.)

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 доступа 15.05.2018г.)

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 доступа 15.05.2018г.)

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 доступа 15.05.2018г.)

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 доступа 15.05.2018г.)

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 доступа 15.05.2018г.)

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

Согласована на портале № 38360

при Президенте Российской Федерации от 30 марта 1992 г. 29 с. http://fstec.ru/component/attachments/download/296 (Дата доступа 15.05.2018г.)

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 доступа 15.05.2018г.)

9. Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты [Электронный ресурс] // Режим доступа: http://fstec.ru/component/attachments/download/317 (Дата доступа 15.05.2018г.)

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.)

Дополнительная литература по дисциплинам:

1. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-004-7 http://znanium.com/catalog/product/489084 (Дата доступа 15.05.2018г.)

2. Защита информации с использованием смарт-карт и электронных брелоков / Л. К. Бабенко, С. С. Ищуков, О. Б. Макаревич. - М. : "Гелиос АРВ", 2003. - 351[1] с. : ил., табл., портр. - Библиогр.: с. 348-349. Доступно в библиотеке: 29 экземпляров

Дисциплина «Криптографические методы защиты информации».

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?

7. Приведите типовую/возможную структуру инструкции по парольной защите.

8. Приведите типовую/возможную структуру должностной инструкции специалиста по защите информации.

9. Коды аутентичности сообщений. Электронная подпись.

10. Криптография с открытым ключем.

Основная литература по дисциплине:

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.)

Согласована на портале № 38360

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

3. 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.)

4. 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.)

5. 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 доступа 15.05.2018г.)

6. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. — М.: Стандартинформ, 2015. — 21 с. http://docs.cntd.ru/document/1200121984 (Дата доступа 15.05.2018г.)

7. 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 доступа 15.05.2018г.)

8. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. — М.: Стандартинформ, 2012. — 34 с. http://docs.cntd.ru/document/1200095035 (Дата доступа 15.05.2018г.)

9. 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 доступа 15.05.2018г.)

10. "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 доступа 15.05.2018г.)

11. 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 доступа 15.05.2018г.)

12. 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 доступа 15.05.2018г.)

13. 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 доступа 15.05.2018г.).

Дополнительная литература по дисциплине:

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

2. Основы современной криптографии: учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — 2-е изд., перераб. и доп. — М.: Горячая линия-Телеком, 2002. — 176 с. (51 экз.)

Дисциплина «Нормативная база обеспечения информационной безопасности банковской организации»

Вопросы:

1. Опишите комплекс отраслевых стандартов (СТО БР ИББС) и рекомендаций (РС БР ИББС) Центрального Банка Российской Федерации в области информационной безопасности бан-

Согласована на портале № 38360

ковской 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.

5. Опишите программно-аппаратный комплекс автоматизирующий процесс приема платежей в Интернете.

6. Что составляет банковскую тайну.

7. Назовите этапы формирования СОИБ банковской организации.

8. Опишите стандарт PCI DSS/

9. Перечислите основные платежные системы России и их характеристики.

10. Какие функции реализует механизм электронной подписи.

Основная литература по дисциплине:

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 доступа 15.05.2018г.).

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 доступа 15.05.2018г.).

Дополнительная литература по дисциплине:

Информационные системы в банковской деятельности: учебное пособие / С. Ю. Золотов, Е. Б. Грибанова; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра автоматизированных систем управления. – Томск: ТМЦДО, 2008. – 103 с. (20 экз.).

6.3. Методические материалы процедуры оценивания результатов ГЭ

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 доступа 15.05.2018г.)

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] https://regulations.tusur.ru/documents/295 . (Дата доступа 15.05.2018г.)

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 доступа 15.05.2018г.)

Дополнительная литература ГЭ

1. Образовательный стандарт вуза ОС ТУСУР 01-2013. Работы студенческие по направлениям подготовки и специальностям технического профиля. Общие требования и правила оформления.

Согласована на портале № 38360

Введен приказом ректора от 03.12.2013 г. №14103. [Электронный ресурс]. URL: https://storage.tusur.ru/files/40668/rules_tech_01-2013.pdf (Дата доступа 15.05.2018г.).

2. 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 доступа 15.05.2018г.).

7. 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:

–Microsoft Windows;

–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:

–Microsoft Windows;

–MS OFFICE;

–Visual Studio 2012;

–Oracle VM VirtualBox;

–VMware Player;

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

8. Проведение ГЭ для лиц с ограниченными возможностями здоровья

Форма проведения государственного экзамена 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 к сдаче и сдача ГЭ для обучающихся 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.

Согласована на портале № 38360

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. На время сдачи 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 сдачи экзамена.

9.Порядок подачи и рассмотрения апелляций по ГИА

Обучающийся имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению, установленной процедуры проведения государственного аттестационного испытания и (или) несогласии с результатами государственного экзамена.

Апелляция подается **лично** обучающимся в апелляционную комиссию не позднее следующего рабочего дня после объявления результатов государственного аттестационного испытания.

Для рассмотрения апелляции секретарь государственной экзаменационной комиссии направляет в апелляционную комиссию протокол заседания государственной экзаменационной комиссии, заключение председателя государственной экзаменационной комиссии о соблюдении процедурных вопросов при проведении государственного аттестационного испытания, а также письменные ответы обучающегося (при их наличии) (для рассмотрения апелляции по проведению государственного экзамена) либо выпускную квалификационную работу, отзыв и рецензию (рецензии) (для рассмотрения апелляции по проведению защиты выпускной квалификационной работы).

Апелляция рассматривается не позднее 2 рабочих дней со дня подачи апелляции на заседании апелляционной комиссии, на которое приглашаются председатель государственной экзаменационной комиссии и обучающийся, подавший апелляцию.

Решение апелляционной комиссии доводится до сведения обучающегося, подавшего апелля-

Согласована на портале № 38360

цию, в течение 3 рабочих дней со дня заседания апелляционной комиссии. Факт ознакомления обучающегося, подавшего апелляцию, с решением апелляционной комиссии удостоверяется подписью обучающегося.

При рассмотрении апелляции о нарушении порядка проведения государственного аттестационного испытания апелляционная комиссия принимает одно из следующих решений:

• об отклонении апелляции, если изложенные в ней сведения о нарушениях процедуры проведения государственной итоговой аттестации обучающегося не подтвердились и (или) не повлияли на результат государственного аттестационного испытания;

• об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях процедуры проведения государственной итоговой аттестации обучающегося подтвердились и повлияли на результат государственного аттестационного испытания.

В случае удовлетворения апелляции, результат проведения государственного аттестационного испытания подлежит аннулированию, в связи с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в государственную экзаменационную комиссию для реализации решения апелляционной комиссии. Обучающемуся предоставляется возможность пройти государственное аттестационное испытание в сроки, установленные образовательной организацией.

При рассмотрении апелляции о несогласии с результатами государственного аттестационного испытания апелляционная комиссия выносит одно из следующих решений:

• об отклонении апелляции и сохранении результата государственного аттестационного испытания;

• об удовлетворении апелляции и выставлении иного результата государственного аттестационного испытания.

Решение апелляционной комиссии не позднее следующего рабочего дня передается в государственную экзаменационную комиссию. Решение апелляционной комиссии является основанием для аннулирования ранее выставленного результата государственного аттестационного испытания и выставления нового.

Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

Повторное проведение государственного аттестационного испытания осуществляется в присутствии одного из членов апелляционной комиссии не позднее 15 июля.

Апелляция на повторное проведение государственного аттестационного испытания не принимается.

Согласована на портале № 38360

Приложение А
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 и доклада при защите письменной части государственного экзамена														
7	Качество ответов на вопросы устной части экзамена														
	Сумма баллов														
	Итоговая оценка														

Подпись члена ГЭК_____

Согласована на портале №