Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Романчук Иван Сергеевич
Должность: Ректор
Дата подписания: 31.10.2023 10:29:17
Уникальный программный ключ:
6319edc2b582ffdacea443f01d5779368d0957ac34f5cd074d8118153045324f9

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
и.о. заместителя директора Института
математики и компьютерных наук
_____/М.Н. Перевалова/
"01" июня 2020 г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ
10.05.01 «Компьютерная безопасность»
специализации «Безопасность распределенных компьютерных систем»
квалификации «Специалист по защите информации»
форма обучения очная

Нестерова О.А. Ниссенбаум О.В. Программа государственной итоговой аттестации специальности 10.05.01 «Компьютерная безопасность», специализация «Безопасность распределенных компьютерных систем», форма обучения очная. Тюмень, 2020.

Программа государственной итоговой аттестации опубликована на сайте ТюмГУ: Государственная итоговая аттестация [электронный ресурс] / Режим доступа: http://www.utmn.ru/sveden/education/#.

© Тюменский государственный университет, 2020.
© Нестерова О. А., Ниссенбаум О.В., 2020.

1. Цели государственной итоговой аттестации

Государственная итоговая аттестация осуществляется с целью установления уровня подготовленности выпускника высшего учебного заведения к выполнению профессиональных задач и соответствия его подготовки требованиям ФГОС ВО и основной образовательной программы по специальности высшего образования.

2. Задачи государственной итоговой аттестации

Задачи:

• установление уровня подготовки выпускника к выполнению профессиональных задач;

• установление соответствия теоретической и практической подготовки требованиям государственного образовательного стандарта высшего образования (включая базовые и вариативные блоки);

• установление уровня сформированности общекультурных компетенций на примере умений работать с литературой, находить необходимую информацию, уметь перерабатывать ее, систематизировать результаты информационного поиска, использовать при ответе на вопрос;

• оценка подготовленности студента к практической деятельности в современных условиях;

• презентация умений публичной дискуссии;

Результаты государственного экзамена учитываются вузом при рекомендации выпускника к продолжению образования.

Итоговые государственные аттестационные испытания, входящие в перечень обязательных итоговых аттестационных испытаний, не могут быть заменены оценкой качества освоения ООП путем осуществления текущего контроля успеваемости и промежуточной аттестации студента.

3. Форма проведения государственной итоговой аттестации

Государственный экзамен принимается государственной аттестационной комиссией, сформированной в Институте и утвержденной в соответствии с Положением об итоговой государственной аттестации выпускников высших учебных заведений в РФ. Государственный экзамен может проводиться только при наличии необходимого кворума в присутствии председателя комиссии или его заместителя.

4. Перечень компетенций, которыми должен овладеть обучающийся в результате освоения образовательной программы

Код компетенции	Наименование компетенции	Форма ГИА (государственный экзамен/ВКР) *при наличии 2 форм*
Универсальные компетенции / Общекультурные компетенции (УК/ОК)		
ОК-1	способностью использовать основы философских знаний для формирования мировоззренческой позиции	Государственный экзамен и ВКР

ОК-2	способностью использовать основы экономических знаний в различных сферах деятельности	Государственный экзамен и ВКР
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	Государственный экзамен и ВКР
ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности	Государственный экзамен и ВКР
ОК-5	способностью понимать социальную значимость своей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Государственный экзамен и ВКР
ОК-6	способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Государственный экзамен и ВКР
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	Государственный экзамен и ВКР
ОК-8	способностью к самоорганизации и самообразованию	Государственный экзамен и ВКР
ОК-9	способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	Государственный экзамен и ВКР
Общепрофессиональные компетенции (ОПК)		
ОПК-1	способностью анализировать физические явления и процессы при решении профессиональных задач	Государственный экзамен и ВКР
ОПК-2	способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Государственный экзамен и ВКР
ОПК-3	способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	Государственный экзамен и ВКР

ОПК-4	способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Государственный экзамен и ВКР
ОПК-5	способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Государственный экзамен и ВКР
ОПК-6	способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций	Государственный экзамен и ВКР
ОПК-7	способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Государственный экзамен и ВКР
ОПК-8	способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Государственный экзамен и ВКР
ОПК-9	способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Государственный экзамен и ВКР
ОПК-10	способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Государственный экзамен и ВКР
Профессиональные компетенции (ПК)		
ПК-1	способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	Государственный экзамен и ВКР
ПК-2	способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	Государственный экзамен и ВКР
ПК-3	способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Государственный экзамен и ВКР
ПК-4	способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Государственный экзамен и ВКР
ПК-5	способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Государственный экзамен и ВКР

ПК-6	способностью участвовать в разработке проектной и технической документации	Государственный экзамен и ВКР
ПК-7	способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем	Государственный экзамен и ВКР
ПК-8	способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы	Государственный экзамен и ВКР
ПК-9	способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	Государственный экзамен и ВКР
ПК-10	способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Государственный экзамен и ВКР
ПК-11	способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	Государственный экзамен и ВКР
ПК-12	способностью проводить инструментальный мониторинг защищенности компьютерных систем	Государственный экзамен и ВКР
ПК-13	способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности	Государственный экзамен и ВКР
ПК-14	способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Государственный экзамен и ВКР
ПК-15	способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Государственный экзамен и ВКР
ПК-16	способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	Государственный экзамен и ВКР
ПК-17	способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	Государственный экзамен и ВКР

ПК-18	способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Государственный экзамен и ВКР
ПК-19	способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Государственный экзамен и ВКР
ПК-20	способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	Государственный экзамен и ВКР
Специализированные компетенции		
ПСК-3.1	способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем	Государственный экзамен и ВКР
ПСК-3.2	способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем	Государственный экзамен и ВКР
ПСК-3.3	способностью использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности	Государственный экзамен и ВКР
ПСК-3.4	способностью организовывать защиту информации в распределенных компьютерных системах	Государственный экзамен и ВКР
ПСК-3.5	способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем	Государственный экзамен и ВКР
Вид профессиональной деятельности		
научно-исследовательская, проектная, контрольно-аналитическая, организационно-управленческая, эксплуатационная, научно-исследовательская, организационно-управленческая, проектная		
Дополнительные профессиональные компетенции, установленные в образовательной программе (ДПК)		

5. Общие требования к проведению государственной итоговой аттестации

5.1. Требования к проведению государственного экзамена (при наличии экзамена)

Экзамен проводится в аудитории, где оборудуются места для экзаменационной комиссии, секретаря комиссии и индивидуальные места для студентов. К началу экзамена в аудитории должны быть подготовлены:

• приказ о составе государственной экзаменационной комиссии;
• приказ о допуске к государственному экзамену;
• программа сдачи государственного итогового экзамена;
• экзаменационные билеты в запечатанном конверте;
• список студентов, сдающих экзамен;
• сведения о выпускниках, сдающих экзамены;
• зачетные книжки;
• протоколы сдачи экзамена;
• бумага для письменного ответа со штампом Института;
• экзаменационная ведомость для выставления комиссией оценок за ответ на государственном экзамене.

В день работы ГАК перед началом экзамена студенты – выпускники приглашаются в аудиторию, где председатель ГАК:

• знакомит присутствующих и экзаменующихся с приказом о создании ГАК, зачитывает его и представляет экзаменующимся состав комиссии персонально;
• вскрывает конверт с экзаменационными билетами, проверяет их количество и раскладывает на специально выделенном для этого столе;
• дает общие рекомендации экзаменующимся при подготовке ответов и изложении вопросов билета, а также при ответах на дополнительные вопросы.

Во время экзамена члены комиссии наблюдают за самостоятельной подготовкой студентов к ответу на вопросы билета, дают пояснения, если в этом возникает необходимость. На экзамене студенты могут пользоваться программами изучения дисциплин, включенных в билеты.

Во время ответа на вопросы билета (в устной или письменной форме) студент должен четко и ясно формулировать (излагать) ответ на вопрос билета. Ответивший (закончивший письменный ответ на вопросы билета) студент сдает листы своего ответа по билету и сам билет секретарю ГАК. Члены ГАК могут задавать уточняющие вопросы выступающему студенту.

После ответа последнего студента под руководством председателя ГАК проводится обсуждение и выставление оценок. По каждому студенту решение о выставляемой оценке должно быть единогласным. Члены комиссии имеют право на особое мнение по оценке ответа отдельных студентов. Оно должно быть мотивированно и записано в протокол. Одновременно формулируется общая оценка уровня теоретических и практических знаний экзаменующихся, выделяются наиболее грамотные и компетентные ответы. Оценки по каждому студенту заносятся в протоколы и зачетные книжки, комиссия подписывает эти документы.

5.2. Требования к процедуре защиты выпускной квалификационной работы (при наличии ВКР)

Для проведения защиты ВКР используется аудитория, оборудованная мультимедиа проектором и персональным компьютером.

Для подготовки текста ВКР, презентации и доклада студенту предоставляется компьютер с пакетом офисных программ в классе, выделенном для самостоятельной работы студента.

В случае выполнения выпускной квалификационной работы на базе ТюмГУ, студенту предоставляется оборудование одной из лабораторий Института математики и компьютерных наук или иного подразделения Университета в зависимости от темы работы.

6. Оценочные материалы и критерии для проведения государственной итоговой аттестации

6.1. Оценочные критерии государственного экзамена (при наличии экзамена)

Критерии оценки вопросов, выносимых на экзамен, разработаны с учетом требований Государственного образовательного стандарта и должны быть доведены до выпускников. Ответы на вопросы, выносимые на итоговый междисциплинарный экзамен, оцениваются по шкале «отлично», «хорошо», «удовлетворительно» и
«неудовлетворительно».

Оценка «отлично»: Студент глубоко, осмысленно, в полном объеме усвоил программный материал, излагает его на высоком научном уровне, способен к самостоятельному анализу и оценке проблемных ситуаций. Умеет творчески применять теоретические знания при решении практических ситуаций. Показывает способность самостоятельно пополнять и обновлять знания в процессе повышения квалификации и профессиональной деятельности.

Оценка «хорошо»: Студент полно раскрыл материал, предусмотренный программой, изучил обязательную литературу. Владеет понятиями, определениями, терминами, методами исследования в области компьютерной безопасности, умеет установить взаимосвязь изученных дисциплин с другими областями знаний. Применяет теоретические знания на практике. Допустил незначительные неточности при изложении материала, не искажающие содержание ответа по существу вопроса.

Оценка «удовлетворительно»: Студент владеет материалом в пределах программы, знает основные понятия и определения в области компьютерной безопасности. Обладает достаточными знаниями для профессиональной деятельности. Способен разобраться в конкретной практической ситуации.

Оценка «неудовлетворительно». Студент показал пробелы в знании основного учебного материала, не может дать четких определений, понятий в области информационной безопасности. Не может разобраться в конкретной практической ситуации. Не обладает достаточными знаниями и практическими навыками для профессиональной деятельности.

Результат государственного итогового экзамена определяется дифференцированно оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», которые объявляются в тот же день после оформления в установленном порядке протоколов заседаний аттестационной комиссии. Результаты государственного экзамена вносятся в зачетную книжку студента и заверяются подписями всех членов экзаменационной комиссии, присутствующих на заседании.

Председатель комиссии подводит итоги сдачи государственного экзамена и сообщает, что в результате обсуждения и совещания оценки выставлены и оглашает их студентам, отмечает лучших студентов, высказывает общие замечания, обращается к студентам с вопросом, нет ли не согласных с решением комиссии ГАК по выставленным оценкам. В случае устного заявления экзаменующегося о занижении оценки его ответа, с ним проводится собеседование в присутствии всего состава комиссии. Целью такого собеседования является разъяснение качества ответов и обоснование итоговой оценки. Пересдача экзамена на повышенную оценку запрещается.

Студент, не сдавший государственный итоговый экзамен, допускается к нему повторно один раз в течение пяти лет после окончания ТюмГУ и не ранее, чем через один год на основании личного заявления и представления учебной части. Срок повторной сдачи устанавливает ректор университета по согласованию с председателем ГАК в период очередной работы ГАК. Выпускник, не явившийся по уважительной причине (по медицинским показаниям, документально подтвержденным) имеет право пройти итоговую аттестацию в течение месяца с момента подачи заявления о готовности пройти соответствующие государственные аттестационные испытания.

Студент, имеющий неудовлетворительную оценку по государственному экзамену, не допускается к следующему виду аттестационных испытаний – защите выпускной квалификационной работы.

Подведение итогов работы ГАК осуществляется в письменном отчете, в котором приводится статистика о количестве сдававших экзамен, уровне знаний и формулируются предложения по совершенствованию преподавания отдельных дисциплин.

6.2. Оценочные критерии выпускной квалификационной работы (при наличии ВКР)

«Государственная итоговая аттестация», в виде выпускной квалификационной работы, оценивается по итогам её защиты перед членами ГАК, в полном объеме относится к базовой части программы и завершается присвоением квалификации, указанной в перечне направлений подготовки высшего образования, утвержденном Министерством образования и науки Российской Федерации".

Предусматриваются индивидуальная и групповая формы выполнения выпускной квалификационной работы. При любой форме работы студентом(ами) к защитепредставляется тест дипломной работы (один на группу в случае групповой формы), отзыв научного руководителя (на каждого студента), аннотация. В случае наличия — рецензия. Призащите работы, выполненной в групповой форме, каждый студент в своем докладе должен отразить личный вклад в выполненную работу, вопросы комиссией каждому студенту задаются индивидуально.

Выпускник по итогам защиты, учитывающим качество текста ВКР, доклада, полноты и качества решения студентом поставленных в работе задач, ответов на вопросы, заданные членами ГАК, получает оценку «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно». Оценка отражает уровень сформированности компетенций студента.

6.3. Оценочные материалы государственной итоговой аттестации

Государственная экзаменационная комиссия дает оценку сформированности у обучающегося всех компетенций, предусмотренных ФГОС ВО по специальности (в том числе способности к самоорганизации и самообразованию, использования методов и средств физической культуры для обеспечения полноценной социальной и профессиональной деятельности), используя оценочные средства (выпускная квалификационная работа, отзыв руководителя, устный ответ студента), либо посредством дополнительных вопросов студенту на государственном экзамене/защите ВКР.

6.3.1. Вопросы (и задачи) государственного экзамена (при наличии экзамена)

Раздел «Математика»

1. Системы линейного уравнения над кольцом и полем. Системы линейных уравнений над коммутативным кольцом с единицей. Равносильность систем. Системы уравнений над кольцом. Однородные уравнения и функциональная система решений.
2. Сравнения и вычеты. Кольцо вычетов. Малая теорема Ферма. Сравнения первой степени. Китайская теорема об остатках.
3. Кольца матриц. Матрицы над кольцом и операции над ними. Кольцо квадратных матриц. Определители квадратных матриц над коммутативным кольцом с единицей. Критерии обратимости матрицы над коммутативным кольцом с единицей.
4. Многочлены. Кольцо многочленов над кольцом с единицей. Делимость многочленов, теорема о делении с остатком. Значение и корень многочлена. Теорема Безу.
5. Линейные пространства. Определение, примеры, простейшие свойства. Единственность нейтрального, единственность противоположного элемента. Линейная зависимость. Координаты векторов и их связь при переходе к другому базису.

6. Основные типы статистических гипотез. Общая логическая схема статистического критерия. Примеры для ИБ.
7. Статистики, статистические оценки и их свойства. Статистические оценки параметров распределения. Статистические оценки и процедуры оценивания. Примеры для ИБ.
8. Дискретные случайные величины. Ряд распределения дискретной случайной величины. Функция распределения дискретной случайной величины. Способы задания. Примеры. Примеры для ИБ.
9. Формула полной вероятности. Формула Байеса. Априорные и апостериорные вероятности. Коэффициенты регрессии и корреляции случайных событий. Примеры для ИБ.
10. Нормальное распределение, гамма-распределение, бета-распределение, распределение хи-квадрат, распределение Стьюдента, распределение Фишера. Примеры для ИБ.
11. Теоремы сложения и умножения вероятностей. Теоремы сложения вероятностей для несовместных и совместных событий. Независимые и зависимые случайные события. Условная вероятность. Примеры для ИБ.
12. Функция распределения случайной величины и ее свойства. Математическое ожидание и дисперсия случайных величин: определение и свойства. Примеры для ИБ.
13. Основные понятия теории вероятности, классификация событий. Классические определения вероятности. Теоремы сложения и умножения вероятностей. Примеры для ИБ.
14. Первообразная и неопределенный интеграл. Определение первообразной. Определение неопределенного интеграла и его свойства. Определение интеграла по Риману. Необходимые и достаточные условия интегрируемости. Формула Ньютона- Лейбница.
15. Непрерывность действительной функции одного действительного переменного. Свойства функций, непрерывных на отрезке: теорема Вейерштрасса, Больцано-Коши; непрерывность многочленной и рациональной функции.

Раздел «Криптографические методы защиты информации»

16. Блочные шифры. Математическая модель. Разновидности блочных шифров. ГОСТ Р 34.12-2015.
17. Эллиптические кривые над конечным полем. Сложение точек, порядок точки, образующая точка. Теорема Хассе. Подпись Эль-Гамаля на эллиптической кривой. ГОСТ Р 34.10-2012.
18. Цифровая подпись, атаки и угрозы. Подписи RSA и Эль-Гамаля. Национальные стандарты DSA и ГОСТ Р 34.10-94.
19. Асимметричные криптосистемы. Понятие односторонней функции. Проблемы факторизации и дискретного логарифмирования. Криптосистемы RSA и Эль-Гамаля.
20. Функции хэширования, требования к ним. Схема Меркла-Дамгарда. Хэш-функции на основе блочных шифров. ГОСТ Р 34.11-2012.
21. Управление ключами в асимметричных криптосистемах. Инфраструктура открытых ключей. Сертификаты. Стандарт X.509.
22. Ключи симметричной криптосистемы. Жизненный цикл ключей. Требования к обеспечению безопасности жизненного цикла ключей. Управление ключами в криптографических системах. Примеры для ИБ.
23. Идентификация и аутентификация. Парольные схемы. Протоколы рукопожатия. Интерактивные системы доказательства.

24. Криптографические протоколы – основные виды и типы, область применения. Разделение секрета. Идеальность и совершенность схем разделения секрета.
25. Совершенные и идеальные шифры по Клоду Шеннону. Избыточность языка на букву сообщения. Ложные ключи и расстояние единственности.
26. Основные понятия криптографии. Модели шифров. Блочные и поточные шифры. Ключевая системы шифра. Атаки и угрозы шифрам. Вычислительная и теоретическая стойкость.

Раздел «Безопасность операционных систем, баз данных и вычислительных сетей»

27. Основные сетевые стандарты, протоколы взаимодействия в сетях. Модели OSI и TCP/IP. Сетевое оборудование на 2 и 3 уровнях модели OSI. Пример.
28. Аутентификация и защита канала в сетях VPN – семейства протоколов IPSec и SSL\TLS. Пример.
29. Понятие процесса, потока. Жизненный цикл процесса. Основные цели и алгоритмы планирования процессов. Пример.
30. Средства обеспечения защиты данных от несанкционированного доступа, средства идентификации и аутентификации объектов БД, языковые средства разграничения доступа, организация аудита в системах БД. Задачи и средства администратора безопасности БД. Пример.
31. Безопасность баз данных – механизмы управления (разграничения) доступом пользователей к данным. Пример.
32. Безопасность баз данных – механизмы восстановления данных после программных и\или аппаратных сбоев, откат транзакций. На своем примере.
33. Безопасность баз данных - использование шифрования и криптографических протоколов. Пример.
34. Типовые функциональные дефекты ОС, приводящие к созданию каналов утечки данных.
35. Контроль доступа к данным в ОС: основные понятия, модели доступа.
36. Основные сервисы безопасности ОС.
37. Основные угрозы безопасности в ОС. Меры противодействия (на своем примере).
38. Формализованные требования к защите ОС.
39. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа пользователей к ресурсам сети. Монитор безопасности. На своем примере.
40. Протоколы IP v4 и IP v6. Совместное использование в рамках одной корпоративной сети.
41. Технологии обеспечения безопасности корпоративной сети с использованием оборудования 2-го уровня модели OSI. На своем примере.
42. Технологии обеспечения безопасности корпоративной сети с использованием оборудования 3-го уровня модели OSI. На своем примере.
43. Понятие неразделяемого ресурса. Гонки. Методы взаимного исключения с активным ожиданием (метод блокирующей переменной, строгое чередование, алгоритм Деккера, алгоритм Петерсона).
44. Технологии обеспечения безопасности беспроводных сетей. На своем примере.

Раздел «Алгоритмы, теория языков программирования, базы данных»

45. Задачи о кратчайших расстояниях на графах. Основные алгоритмы для решения задач о кратчайших расстояниях.
46. Алгоритмы поиска. Использование деревьев в задачах поиска: бинарные, сбалансированные, красно-черные деревья поиска.

47. Алгоритмы сортировки. Постановка задачи, классификация, анализ эффективности. Основные алгоритмы (обмен, выбор, вставка, шейкер, метод Шелла, быстрая, поразрядная, пирамидальная).
48. Абстрактные типы данных. Классы. Инкапсуляция. Наследование. Полиморфизм. Спецификация и реализация в разных языках программирования.
49. Процессы и потоки. Объекты межпроцессной синхронизации. Понятие гонок и взаимной блокировки
50. Общие понятия реляционного подхода к организации БД. Основные понятия реляционной теории: домен, атрибут, кортеж, первичный ключ, отношение. Фундаментальные свойства отношений. Нормализация. На своем примере для небольшой базы.
51. Синтаксис оператора SELECT. Обзор его подразделов (списка выборки, секций FROM, WHERE, GROUP BY, HAVING, OREDER BY).. Способы упорядочивания итогового набора в секции OREDER BY. Модификация данных с использованием Data Manipulation Language (DML). Операторы INSERT, UPDATE, DELETE. На примере своей небольшой базы.

Раздел «Технические средства и методы защиты информации»

52. Технические каналы утечки информации, классификация и характеристика. На своем примере.
53. Радиоэлектронные каналы утечки информации. На своем примере.
54. Способы и средства инженерной защиты и технической охраны объектов. На своем примере.
55. Видеокамеры. Организация охраны объекта с помощью видеокамер. На своем примере.
56. Способы и средства информационного скрытия речевой информации от подслушивания. Энергетическое скрытие акустического сигнала. На своем примере.
57. Принцип действия активных средств поиска прослушивающих устройств. Метод нелинейной локации. На своем примере.
58. Принцип действия пассивных средств поиска прослушивающих устройств. На своем примере.

Раздел «Основы защиты информации»

59. Положения ФЗ-149 "Об информации, информационных технологиях и защите информации". Основные понятия. Виды информации в соответствии с ФЗ-149. Виды конфиденциальной информации. Требования по защите информации.
60. Основные положения Руководящих документов ФСТЭК в области защиты конфиденциальной информации: Приказ № 21 Об утверждении состава и содержания организационных мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. На своих примерах.
61. Основные положения Руководящих документов ФСТЭК в области защиты конфиденциальной информации: Приказ № 17 Об утверждении требований о защите информации, на составляющей государственную тайну, содержащейся в государственных информационных системах. На своих примерах.
62. Классификация автоматизированных систем согласно РД Гостехкомисии "Автоматизированные системы. Защита от несанкционированного дступа к информации", их отличительные особенности. На своих примерах. Состав подсистем защиты информации для каждого класса.
63. Мандатное управление доступом. Модель Белла-ЛаПадулы и модель Биба: основные положения и принципы разграничения прав доступа в системе. Базовая теорема безопасности (BST).

64. Расширенное понятие информационной безопасности. Субъекты и объекты защиты. Защищаемые свойства безопасности. Информационная безопасность как часть обеспечения национальной безопасности Российской Федерации.
65. Сравнительный обзор методик анализа рисков информационной безопасности: OCTAVE, COBRA, CRAMM, RiskWatch.
66. Процессный подход к построению СУИБ и циклическая модель PDCA. Цели и задачи, решаемые СУИБ. На примере своей ИС.
67. Библиотека инфраструктуры информационных технологий (ITIL). Управление IT- сервисами (ITSM). ITIL и управление ИБ.
68. Математические модели систем защиты информации: обобщенные модели систем защиты, вероятностные модели СЗИ, модели, построенные с использованием теории автоматов, модели СЗИ, построенные с использованием теории графов. Примеры.
69. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования). На своем примере.
70. Определения конфиденциальности, целостности, доступности информации. Понятия уязвимости и угрозы. Базовая и частная модели угроз. Политика информационной безопасности.
71. Дискреционное разграничение прав доступа. Модель Харрисона-Руззо-Ульмана (ХРУ), модель типизированной матрицы доступа (ТМД), классическая и расширенная модели Take-Grant.
72. Атрибутная и ролевая модели разграничения прав доступа: основные положения и принципы. Сравнительный анализ атрибутной и ролевой моделей доступа.

Раздел «Организационные и правовые основы обеспечения информационной безопасности»

73. Аудит системы информационной безопасности на объекте как основание для подготовки организационных и правовых мероприятий. Его критерии, формы и методы. На примере своей ИС.
74. Управление непрерывностью деятельности: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ. На примере своей ИС.
75. Требования доктрины информационной безопасности РФ и ее реализация в существующих системах информационной безопасности. На примере своей ИС.
76. Область действия и основные понятия ФЗ-152. Принципы обработки ПДн. Условия обработки ПДн. Согласие на обработку ПДн. Пример согласия. Порядок отправления запросов к оператору ПДн и ответов на них. Пример запроса.
77. Порядок сертификации средств защиты информации. Основные участники процесса. Необходимость сертификации. Виды и схемы сертификации средств защиты информации. Понятия техническое условие, задание по безопасности и профиль защиты.
78. Основные положения ПП-1119. Классификация ИСПДн. Определение уровня защищенности. Основные характеристики ИСПДн. Перечень мер в зависимости от уровня защищенности. На примере своей ИСПДн.
79. Условия обработки биометрических и специальных ПДн. Виды ИСПДн. Условия трансграничной передачи ПДн
80. Понятие средства защиты информации. Классификации средств защиты информации с примерами. Типы сертифицированных средств защиты информации с примерами.
81. Основные положения ФЗ 5485-1 "О государственной тайне". Перечень сведений, отнесенных к гостайне. Порядок отнесения сведений к гостайне. Уровни допуска к гостайне и их особенности. Ответственность за разглашение гостайны

82. Основные положения ФЗ 98 "О коммерческой тайне". Перечень сведений, составляющих коммерческую тайну. Порядок отнесения сведений к коммерческой тайне. Введение режима коммерческой тайны в организации. На своем примере. Ответственность за нарушение закона.
83. Определение СКЗИ. Виды СКЗИ. Основные понятия. Условия эксплуатации СКЗИ
84. Этапы разработки, внедрения и эксплуатации системы защиты информации на своем примере. Техническое задание и технический проект на создание системы защиты информации. Порядок аттестации информационной системы.
85. Методы и средства защиты информации. Классификация и взаимосвязи. На своих примерах
86. Защита ИСПДн в зависимости от уровня защищенности в соответствии с требованиями приказа ФСБ России № 378
87. Построение модели нарушителя и модели угроз безопасности персональных данных в соответствии с требовании документов ФСБ России и ФСТЭК России. На своем примере.

Раздел «Общие вопросы»

88. Понятие здоровье, его основные компоненты и факторы, определяющие здоровье.
89. Применение средств физической культуры для оптимизации работоспособности и
90. профилактики утомления студентов.
91. Методы коррекции состояния зрительного анализатора.
92. Формы и содержание самостоятельных занятий физическими упражнениями.
93. Методы саморегуляции психоэмоциональных состояний.
94. Требования безопасности, предъявляемые к рабочему месту.
95. Безопасность в экстремальных ситуациях в быту.

6.3.2. Примерная тематика выпускных квалификационных работ

- Разработка защищенной системы веб-трекинга
- Разработка интерактивной обучающей платформы по дисциплинам специальности
- Голосовая аутентификация и авторизация на основе машинного обучения
- Разработка риск-ориентированной системы управления непрерывным процессом сканирования уязвимостей
- Разработка прототипа конструктора смарт-контрактов
- Разработка веб-приложения для проведения кибербразведки на основе открытых источников
- Разработка модуля для анализа входящих писем на наличие потенциально нежелательного контента
- Анализ текста на наличие буллинга в социальных сетях
- Разработка универсальной защищенной образовательной веб-платформы

7. Учебно-методическое обеспечение государственной итоговой аттестации

7.1. Литература

1. **Фихтенгольц, Г. М.** Основы математического анализа : учебник / Г. М. Фихтенгольц. — 12-е изд., стер. — Санкт-Петербург : Лань, 2020 — Часть 1 — 2020. — 444 с. — ISBN 978-5-8114-5338-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/139261 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

2. **Фихтенгольц, Г. М.** Основы математического анализа : учебник / Г. М. Фихтенгольц. — 11-е изд., стер. — Санкт-Петербург : Лань, 2020 — Часть 2 — 2020. — 464 с. — ISBN 978-5-8114-5339-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/139262 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

3. **Маньшин, М. Е.** Математическая логика и теория алгоритмов : учебное пособие / М. Е. Маньшин. — Волгоград : Волгоградский институт бизнеса, 2009. — 106 с. — ISBN 978-5-9061-7260-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/11334.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей.

4. **Климов, Г. П.** Теория вероятностей и математическая статистика : учебник / Г. П. Климов. — Москва : Московский государственный университет имени М.В. Ломоносова, 2011. — 368 с. — ISBN 978-5-211-05846-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/13115.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

5. **Демидович, Б. П.** Сборник задач и упражнений по математическому анализу : учебное пособие / Б. П. Демидович. — 22-е изд., стер. — Санкт-Петербург : Лань, 2020. — 624 с. — ISBN 978-5-8114-4874-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126716 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

6. **Мартынов, Л. М.** Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140740 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

7. **Кнауб, Л. В.** Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/441493 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

8. **Крамаров С.О. Криптографическая защита информации**: учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — М.: РИОР: ИНФРА-М, 2018. — 321 с. — (Высшее образование). — DOI: https://doi.org/ 10.12737/1716-6 [Электронный ресурс]. - URL: https://znanium.com/catalog/document?id=361143 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

9. **Золотарев, В. В.** Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс]: учеб. пособие/ В. В. Золотарев, Е. А. Данило- ва. - Красноярск: Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. Режим доступа – URL: http://znanium.com/catalog/product/463037 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

10. **Жукова, М. Н.** Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс]: учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск: Сиб. гос. аэрокосмич. ун-т, 2012. -100 с. . Режим доступа – URL: http://znanium.com/catalog/product/463061 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

11. **Агальцов В.П. Базы данных**. В 2-х кн. Книга 2. Распределенные и удаленные базы данных: учебник / В.П. Агальцов. — М.: ИД «ФОРУМ»: ИНФРА-М, 2017. — 271 с. http://znanium.com/catalog/product/652917 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

12. **Агальцов В.П. Базы данных**. В 2-х кн.Кн. 1. Локальные базы данных: учебник / В.П. Агальцов. - 2-е изд., перераб. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 352 с. http://znanium.com/catalog/product/326451 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

13. **Сафонов, В. О.** Основы современных операционных систем : учебное пособие / В. О. Сафонов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 868 с. — ISBN 978-5-9963-0495-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100347 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

14. **Бабаш А.В**. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.: 60x88 1/8. - (Высшее образование: Бакалавриат). ISBN 978-5-369-01304-5. [Электронный ресурс]. – URL: http://znanium.com/catalog/product/432654 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

15. **Душкин А.В.** Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. - 198 с. http://znanium.com/catalog/product/977192 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

16. **Гринберг, А. С.** Информационные технологии управления : учебное пособие для вузов / А. С. Гринберг, Н. Н. Горбачев, А. С. Бондаренко. — Москва : ЮНИТИ-ДАНА, 2017. — 478 с. — ISBN 5-238-00725-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/71234.html (дата обращения: 15.05.2020). — Режим доступа: для авторизир. пользователей

7.2. Интернет-ресурсы

Базы данных научно-технической информации, научных трудов, статей, материалов, доступных в Тюменском государственном университете https://www.utmn.ru/upload/medialibrary/fc5/Perechen-podpisnykh-litsenzionnykh-baz-dannykh-i-baz-dannykh-dostupnykh-v-ramkakh-natsionalnoy-podpiski.doc (дата обращения: 15.05.2020).

8. Материально-техническое обеспечение государственной итоговой аттестации

Аудитория, в которой проводится защита выпускной квалификационной работы должна быть оснащена мультимедийным оборудованием (компьютер с доступом в интернет, проектор, колонки). В аудитории должны быть установлены камеры для видео фиксации процедуры защиты ВКР.