Федеральное государственное автономное образовательное учреждение
высшего образования
«Волгоградский государственный университет»

Институт приоритетных технологий

УТВЕРЖДАЮ
Проректор по учебной работе
_____ Д.Ю. Ильин
«20» 09 2023 г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙАТТЕСТАЦИИ

для обучающихся
по основной профессиональной образовательной программе
10.05.01 «Компьютерная безопасность»

квалификация выпускника: *специалист по защите информации*

г. Волгоград
2023 год

ЛИСТ СОГЛАСОВАНИЯ

ПРОГРАММЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Программа соответствует:

1. Требованиям ФГОС ВО по специальности 10.05.01 «Компьютерная безопасность» утвержденного приказом Министерства образования и науки РФ от «26» ноября 2020 г., № 1459.

Программа принята на заседании Ученого совета института приоритетных технологий, протокол № 9 от «19 » сентября 2023 г

Руководитель ОПОП 10.05.01 «Компьютерная безопасность»

_____ к.ф.-м.н., доцент, О.А. Какорина

«19» 09 2023 г.

Директор института
приоритетных технологий _____ д.ф.-м.н., профессор И.В. Запороцкова

«19» 09 2023 г.

Зав. кафедрой
информационной безопасности _____ к.ф.-м.н., доцент, О.А. Какорина

«19» 09 2023 г.

Начальник управления
образовательных программ _____ Ю.В. Бутенко

Составитель программы: зав. кафедрой информационной безопасности О.А. Какорина

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Цель государственной итоговой аттестации – установление соответствия уровня профессиональной подготовки выпускников основной профессиональной образовательной программы высшего образования, разработанной в ФГАОУ ВО «Волгоградский государственный университет» с учётом ее профиля и ориентации на конкретные области знания и / или виды профессиональной деятельности выпускника, требованиям федеральных государственных образовательных стандартов высшего образования (далее - ФГОС ВО) по определенному направлению подготовки.

Успешное прохождение государственной итоговой аттестации является основанием для выдачи выпускнику документа о высшем образовании и о квалификации, установленного Министерством образования и науки Российской Федерации.

Для проведения государственной итоговой аттестации и проведения апелляций по результатам государственной итоговой аттестации создаются государственные экзаменационные комиссии и апелляционные комиссии, действующие в течение календарного года. Составы комиссий утверждаются не позднее, чем за 1 месяц до даты начала государственной итоговой аттестации.

2. Структура государственной итоговой аттестации по направлению подготовки 10.05.01 – «Компьютерная безопасность» (специализация №4 Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)):

государственный экзамен*;*

защита выпускной квалификационной работы.

Объем Блока 3 «Государственная итоговая аттестация» - 9 з.е. и включает в себя:

- подготовку к государственному экзамену и государственный экзамен;
- подготовку к процедуре защиты и защиту выпускной квалификационной работы.

3. Особенности прохождения государственных аттестационных испытаний лицами с ОВЗ и инвалидами

При проведении государственной итоговой аттестации обеспечивается соблюдение следующих общих требований:

- проведение государственной итоговой аттестации для инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при прохождении государственной итоговой аттестации;
- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с председателем и членами государственной экзаменационной комиссии);
- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении государственной итоговой аттестации с учетом их индивидуальных особенностей;
- обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных

помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже, наличие специальных кресел и других приспособлений).

По письменному заявлению обучающегося инвалида продолжительность сдачи обучающимся инвалидом государственного аттестационного испытания может быть увеличена по отношению к установленной продолжительности его сдачи: продолжительность сдачи государственного экзамена, проводимого в письменной форме, - не более чем на 90 минут; продолжительность подготовки обучающегося к ответу на государственном экзамене, проводимом в устной форме, - не более чем на 20 минут; продолжительность выступления обучающегося при защите выпускной квалификационной работы - не более чем на 15 минут.

Обучающийся инвалид не позднее чем за 3 месяца до начала проведения государственной итоговой аттестации подает письменное заявление о необходимости создания для него специальных условий при проведении государственных аттестационных испытаний с указанием его индивидуальных особенностей. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в университете). В заявлении обучающийся указывает на необходимость (отсутствие необходимости) присутствия ассистента на государственном аттестационном испытании, необходимость (отсутствие необходимости) увеличения продолжительности сдачи государственного аттестационного испытания по отношению к установленной продолжительности (для каждого государственного аттестационного испытания).

II. ТРЕБОВАНИЯ К СТРУКТУРЕ И СОДЕРЖАНИЮ ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

Государственный экзамен является формой государственной итоговой аттестации, проводится согласно графику учебного процесса после прохождения обучающимся преддипломной практики. Государственный экзамен имеет своей целью определение практической и теоретической подготовленности выпускника к выполнению профессиональных задач, степени освоения компетенций, установленных ФГОС ВО по специальности 10.05.01 «Компьютерная безопасность» (специализация №4 Безопасность компьютерных систем и сетей) и основной профессиональной образовательной программой высшего образования, реализуемой в Волгоградском государственном университете (далее – ОПОП ВолГУ).

1. Цель и задачи государственного экзамена

Цель проведения государственного экзамена	Определение практической и теоретической подготовленности выпускника к выполнению профессиональных задач, степени освоения компетенций установленных федеральным государственным образовательным стандартом высшего образования и ОПОП ВолГУ

Задачи проведения государственного экзамена	продемонстрировать умение применять знания и навыки обеспечения информационной безопасности в профессиональной деятельности; продемонстрировать умение ориентироваться в специальной литературе; проявить навыки практического применения полученных знаний в конкретной ситуации.

2. Требования к уровню подготовки выпускника

В рамках проведения государственного экзамена оценивается степень соответствия практической и теоретической подготовленности выпускника к выполнению профессиональных задач, степени освоения компетенций, установленных ФГОС ВО и ОПОП ВолГУ.

В соответствии с требованиями ФГОС ВО и ОПОП ВолГУ по специальности 10.05.01 «Компьютерная безопасность» выпускник готовятся к решению задач профессиональной деятельности следующих типов:

научно-исследовательский;

проектный;

эксплуатационный.

В рамках проведения государственного экзамена проверятся степень сформированности у выпускника следующих компетенций: УК-2; УК-6; УК-7; УК-8; ОПК-1; ОПК-2; ОПК-3; ОПК-5; ОПК-6; ОПК-10; ОПК-17; ПК-1; ПК-5; ПК-6.

Шифр компетенции	*Расшифровка компетенции*
УК-2	Способен управлять проектом на всех этапах его жизненного цикла
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течении всей жизни
УК-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности
УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-2	Способен применять программные средства системного и прикладного назначений, в том числе, отечественного производства, для решения задач профессиональной деятельности

ОПК-3	Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспертному контролю
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности
ОПК-17	Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе, для формирования гражданской позиции и развития патриотизма
ПК-1	Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей
ПК-5	Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов
ПК-6	Способен проводить анализ безопасности компьютерных систем

3. Перечень дисциплин, формирующих программу государственного экзамена

Для решения заявленных в п. 1 целей и задач в программу государственного экзамена включены вопросы, определяющие содержание следующих дисциплин:

1. Стартап и основы проектной деятельности УК-2, УК-3
2. Управление инновационными технологическими проектами систем защиты информации УК-2, УК-6
3. Прикладная физическая культура УК-7
4. Безопасность жизнедеятельности УК-8
5. Основы информационной безопасности ОПК-1, ОПК-5
6. Программно-аппаратные средства защиты информации ОПК-2
7. Дифференциальные уравнения для решения задач информационной безопасности ОПК-3
8. Организационное и правовое обеспечение информационной безопасности ОПК-5, ОПК-6
9. Управление информационной безопасностью ОПК-5
10. Теория информационной безопасности и методология защиты информации ОПК-6
11. Методы и средства криптографической защиты информации ОПК-10
12. История (история России, всеобщая история) ОПК-17

13. Безопасность виртуальной среды ПК-1
14. Расследование компьютерных инцидентов ПК-5
15. Теоретические основы систем обнаружения, предупреждения компьютерных атак ПК-6
16. Теория массового обслуживания для решения задач информационной безопасности ПК-6

4. Содержание государственного экзамена

№	Тематика вопросов / вопросы и задания для оценки сформированности компетенций	Оцениваемые компетенции
Раздел 1. Стартап и основы проектной деятельности		
1.	Сущность предпринимательской деятельности. Основные подходы и современные требования к созданию бизнеса.	УК-2, УК-3
2.	Специфика технологического предпринимательства	УК-2, УК-3
3.	Бизнес-модель технологического предпринимательства.	УК-2, УК-3
4.	Оценка потенциала рынка для технологического бизнес-проекта.	УК-2, УК-3
5.	Показатели эффективности технологического бизнес-проекта.	УК-2, УК-3
Раздел 2. Управление инновационными технологическими проектами систем защиты информации		
1.	Информационные технологии, как основная платформа инновационного развития проекта.	УК-2, УК-6
2.	Взаимосвязь техногенной экономики и экономики знаний.	УК-2, УК-6
3.	Особенности применяемых санкции, которые следует учитывать при реализации технологических проектов систем защиты информации.	УК-2, УК-6
4.	Требования, предъявляемые к инновационному проекту при установлении отношений с непосредственными системными контрагентами.	УК-2, УК-6
5.	Основные задачи и деятельность подсистем, связанных с информационно-коммуникационным управлением инновационным проектом.	УК-2, УК-6
6.	Критическое состояние инновационного развития страны: характеристики основные направления.	УК-2, УК-6
7.	Рекомендуемые алгоритмы реализации технологического проекта систем защиты информации.	УК-2, УК-6
Раздел 3. Прикладная физическая культура		
1.	Физическое развитие человека и требования к нему.	УК-7
2.	Физическая культура как средство сохранения и укрепления здоровья.	УК-7
3.	Правовые основы физической культуры и спорта.	УК-7
4.	Развитие массовой и оздоровительной физической культуры населения Российской Федерации.	УК-7
Раздел 4. Безопасность жизнедеятельности		

	Качественный и количественный анализ опасностей.	УК-8
	Микроклимат в производственных помещениях, его влияние на организм человека.	УК-8
	Влияние вредных веществ на организм человека. ПДК.	УК-8
	Нормирование производственного освещения	УК-8
	Электромагнитное поле, его характеристики.	УК-8
Раздел 5. Основы информационной безопасности		
1.	Понятие угрозы информационной безопасности.	ОПК-1, ОПК-5
2.	Основные внешние источники угроз информационной безопасности РФ	ОПК-1, ОПК-5
3.	Состояние информационной безопасности РФ и основные задачи по ее обеспечению.	ОПК-1, ОПК-5
4.	Состояние информационной безопасности РФ и основные задачи по ее обеспечению.	ОПК-1, ОПК-5
5.	Особенности обеспечения информационной безопасности в различных сферах общественной жизни.	ОПК-1, ОПК-5
6.	Ограничение доступа к информации.	ОПК-1, ОПК-5
7.	Категории информации в зависимости от порядка ее предоставления или распространения.	ОПК-1, ОПК-5
8.	Значение защиты информации для субъектов информационных отношений государства, общества, личности	ОПК-1, ОПК-5
Раздел 6. Дифференциальные уравнения для решения задач информационной безопасности		
1.	Понятие об обыкновенном дифференциальном уравнении. Поле направлений. Изоклины.	ОПК-3
2.	Задача Коши для дифференциального уравнения первого порядка. Формулировка теоремы существования и единственности решения задачи Коши.	ОПК-3
3.	Интегрирование уравнений с разделяющимися переменными.	ОПК-3
	Линейные дифференциальные уравнения первого порядка. Метод Бернулли.	ОПК-3
4.	Линейные дифференциальные уравнения первого порядка. Метод вариации произвольной постоянной.	ОПК-3
5.	Линейное однородное уравнение (ЛОДУ) n-го порядка. Вронскиан и его свойства. Фундаментальная система и общее решение линейного однородного уравнения n-го порядка.	ОПК-3

Раздел 7. Методы дискретной математики в криптологии		
1.	Основные определения. История криптографии. Операция перестановки. Операция подстановки. Роторные машины.	ОПК-10
2.	Перестановка. Гаммирование. Генераторы псевдослучайной последовательности. Регистр сдвига с линейной обратной связью. Аппаратный генератор случайных чисел.	ОПК-10
3.	Симметричные криптосистемы. Блочные шифры. Сеть Фейстеля. SP-сеть.	ОПК-10
4.	Ассиметричные криптосистемы. Схема Эль-Гамаля. Криптосистема, основанная на проблеме Диффи-Хеллмана.	ОПК-10
5.	Ассиметричные криптосистемы. Криптосистема RSA. Криптосистемы Меркля — Хеллмана и Хора — Ривеста.	ОПК-10
6.	Криптосистемы над группой точек эллиптической кривой. Построение группы точек эллиптической кривой.	ОПК-10
Раздел 8. Безопасность виртуальной среды		
1.	Понятие виртуализации. Подходы к виртуализации. Аппаратная виртуализация. Гипервизор. Современные средства виртуализации.	ПК-1
2.	Угрозы виртуальной среды. Требования по нормативной документации (ФСТЭК, ГОСТ) к защите виртуальной среды. ГОСТ Р 56938-2016. Соотнесение ГОСТ Р 56938-2016 с приказами ФСТЭК №17, 21, 31.	ПК-1
3.	Механизмы защиты виртуальной среды, классификация. Обзор средств защиты виртуальной инфраструктуры. Хостовые и гостевые средства защиты.	ПК-1
Раздел 9. История (история России, всеобщая история)		
1.	Россия в конце XVIII - первой четверти XIX в. и мир. Взаимоотношения со странами Запада. Участие России в коалициях.	ОПК-7
2.	Социально-экономическое и общественно-политическое развитие СССР и стран Запада в 1950-1960-х гг.	ОПК-7
3.	Перестройка. Распад СССР. Становление новой российской государственности.¶Особенности социально-экономического и политического развития в 2000-е гг.	ОПК-7
Раздел 10. Теория информационной безопасности и методология защиты информации		
1.	Методы оценивания угроз безопасности в информационных системах.	ОПК-6
2.	Подходы, принципы, методы и средства обеспечения безопасности.	ОПК-6
3.	Теоретико-графовые модели комплексной оценки защищенности КС. Технико-экономическое обоснование систем обеспечения безопасности.	ОПК-6
4.	Модель Белла-ЛаПадулы и основная теорема безопасности.	ОПК-6
5.	Дискреционные модели распространения прав доступа.	ОПК-6
Раздел 11. Организационное и правовое обеспечение информационной безопасности		

1.	Правовой режим защиты государственной тайны. Правовые режимы защиты информации ограниченного доступа, не составляющей государственную тайну. Правовой режим защиты персональных данных.	ОПК-5, ОПК-6
2.	Система лицензирования РФ. Лицензирование деятельности в области защиты информации. Органы лицензирования и их полномочия. Лицензируемые виды деятельности.	ОПК-5, ОПК-6
3.	Сертификация средств защиты информации в системе сертификации ФСТЭК. Аттестация объектов информатизации по требованиям ФСТЭК.	ОПК-5, ОПК-6
Раздел 12. Управление информационной безопасностью		
1.	Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Модель PDCA.	ОПК-5
2.	Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ.	ОПК-5
3.	Этапы разработки и функционирования СУИБ.	ОПК-5
4.	Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ. Понятие и виды защищаемой информации по законодательству РФ. Примеры политики СУИБ.	ОПК-5
5.	Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Основные положения стандартов в области управления рисками ИБ.	ОПК-5
6.	Модель угроз. Методы оценки ущерба от реализации угроз информационной безопасности.	ОПК-5
7.	Методики анализа рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Использование результатов анализа рисков ИБ.	ОПК-5
8.	Ввод системы в эксплуатацию. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация.	ОПК-5
Раздел 13. Расследование компьютерных инцидентов		
1.	Понятие компьютерного инцидента. Основные термины и определения в области компьютерной криминалистики.	ПК-5
2.	Законодательство РФ в области компьютерных инцидентов.	ПК-5
3.	Угрозы безопасности информации и основные виды атак. Факторы воздействия на информацию и последствия.	ПК-5
4.	Основные предпосылки для возникновения компьютерных инцидентов. Признаки компьютерного инцидента.	ПК-5
5.	Юридические предпосылки и меры для минимизации нанесенного ущерба.	ПК-5
6.	Технические мероприятия. Изъятие и исследование компьютерной техники и носителей информации. Виды документов.	ПК-5

7.	Методы анализа образов жестких дисков. Выявление удаленных данных и шифрованных областей. Инструменты. Методы восстановления.	ПК-5
8.	Анализ файлов-образов виртуальных систем, файлов состояний виртуальных систем. Инструменты.	ПК-5
Раздел 14. Теоретические основы систем обнаружения, предупреждения компьютерных атак		
1.	Типичный сценарий действий нарушителя. Сбор информации. Реализация атаки. Завершение атаки.	ПК-6
2.	Средства обнаружения компьютерных атак. Признаки атак. Повтор определенных событий. Неправильные команды. Использование уязвимостей. Несоответствующие параметры сетевого трафика. Непредвиденные атрибуты. Необъяснимые проблемы. Дополнительные признаки.	ПК-6
3.	Источники информации об атаках. Технологии обнаружения атак. Обнаружение аномальной активности. Обнаружение злоупотреблений. Статистический анализ. Экспертные системы. Нейронные сети.	ПК-6
Раздел 15. Теория массового обслуживания для решения задач информационной безопасности		
1.	Понятие случайного процесса. Цепь Маркова с конечным числом состояний и дискретным временем. Граф состояний. Матрица переходных вероятностей. Стационарное распределение.	ПК-6
2.	Марковские процессы с конечным числом состояний и непрерывным временем. Размеченный граф состояний. Матрица интенсивностей перехода. Система дифференциальных уравнений Колмогорова. Нахождение стационарного распределения.	ПК-6
3.	Основные понятия и классификация систем массового обслуживания (СМО): по поведению заявки (с отказами, с очередью, смешанного типа); по характеру источника заявок (открытого и замкнутого типа); по дисциплине ожидания и обслуживания. Параметры и характеристика СМО: параметры входящего потока; параметры структуры СМО. Показатели эффективности СМО.	ПК-6
4.	Методы исследования СМО с простейшими потоками событий: СМО без потерь, СМО с отказами, СМО с нетерпеливыми заявками, СМО замкнутого типа.	ПК-6
5.	Методы исследования сетей массового обслуживания (СеМО) с простейшими потоками событий. Моделирование систем массового обслуживания.	ПК-6
Раздел 16. Программно-аппаратные средства защиты информации		
1.	Модель построения ПАСЗИ. Концепция диспетчера доступа. Состав подсистемы защиты информации: Подсистема управления доступом, Подсистема криптографической защиты. Подсистема регистрации и учета. Подсистема обеспечения целостности.	ОПК-2
2.	Состав типового комплекса защиты от несанкционированного доступа. Архитектура аппаратного контроллера.	ОПК-2
3.	Разграничение доступа. Дискреционная и мандатная модель разграничения доступа в СЗИ от НСД.	ОПК-2

4.	Электронные идентификаторы. eToken, JaCarta, РуТокен, GuardantID; TouchMemory, iButton, SMART-карты, RFID и Proximity карты. Применение электронных идентификаторов.	ОПК-2

5. Оценочные средства для проведения государственного экзамена

5.1. Процедура оценивания

Экзамен проводится в письменной форме по билетам. Каждый из билетов содержит по три теоретических вопроса, относящихся к одной из дисциплин, перечисленных в п. 3 настоящей программы.

Процедура проведения государственного экзамена в письменной форме предусматривает выбор «вслепую» экзаменационного билета, написание ответа на специальном бланке, проверку письменных работ комиссией, совещание комиссии, составление и подписание протоколов, объявление оценок.

5.2. Критерии оценивания результатов обучения

Уровень сформированности компетенций	Критерии оценивания	Оценка
Повышенный уровень	обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий	**«отлично»**
Базовый уровень	обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий	**«хорошо»**
Пороговый уровень	обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне	**«удовлетворительно»**
Уровень ниже порогового	система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности	**«неудовлетворительно»**

Оценка ответа обучающегося на государственном экзамене определяется в ходе заседания государственной экзаменационной комиссии по приему государственного экзамена (далее – ГЭК).

Члены ГЭК по приему государственного экзамена оценивают результаты сдачи экзамена и вносят их в оценочный лист ГЭК (приложение 1).

6. Общие рекомендации по подготовке к государственному экзамену

Обучающийся должен самостоятельно актуализировать полученные ранее знания, умения, навыки, характеризующие практическую и теоретическую подготовленность по темам, содержание которых составляет предмет государственного экзамена и соответствует требованиям по готовности к видам профессиональной деятельности, решению профессиональных задач и освоению компетенций, перечисленных в п. 2 настоящей программы.

При подготовке к экзамену желательно составлять конспекты, иллюстрируя отдельные прорабатываемые вопросы. Теоретический материал должен быть дополнен практическими примерами из области защиты информации. Материал должен конспектироваться кратко, четко, конкретно в рамках обозначенной темы.

III. ТРЕБОВАНИЯ К СТРУКТУРЕ И СОДЕРЖАНИЮ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Выпускная квалификационная работа (далее – ВКР) является обязательной формой государственной итоговой аттестации и выполняется согласно графику учебного процесса. Выпускная квалификационная работа имеет своей целью систематизацию, обобщение и закрепление теоретических знаний и практических умений выпускника, определение степени освоения компетенций, установленных федеральным государственным образовательным стандартом высшего образования (далее – ФГОС ВО) по специальности 10.05.01 «Компьютерная безопасность» и основной профессиональной образовательной программой высшего образования, реализуемой в Волгоградском государственном университете (далее – ОПОП ВолГУ).

1. Цель и задачи выполнения выпускной квалификационной работы

Цель выполнения выпускной квалификационной работы	Выполнение ВКР является заключительным этапом обучения и имеет своей целью: – систематизацию, закрепление и расширение теоретических знаний по специальности 10.05.01 Компьютерная безопасность (специализация №4 Безопасность компьютерных систем и сетей) и применение этих знаний при решении конкретных практических задач; – развитие навыков ведения самостоятельной работы, овладение методикой исследования и эксперимента при решении разрабатываемых в ВКР проблем и вопросов в соответствии с требованиями ФГОС ВО и ОПОП ВолГУ в

	разделах, характеризующих области, объекты и виды профессиональной деятельности.
Задачи выполнения выпускной квалификационной работы	развитие навыков проведения анализа объектов и процессов в предметной области; развитие навыков разработки математический и функциональных моделей процессов предметной области; развитие навыков разработки программных или программно-аппаратных средств защиты информации; развитие навыков проведения экспериментальных исследований и анализа экспериментальных данных; развитие навыков формирования эргономических требований разрабатываемого проекта; развитие навыков расчета экономической эффективности разрабатываемого проекта

2. Требования к уровню подготовки выпускника

В рамках выполнения выпускной квалификационной работы оценивается степень соответствия практической и теоретической подготовленности выпускника к выполнению профессиональных задач, степени освоения компетенций установленных ФГОС ВО и ОПОП ВолГУ.

В соответствии с требованиями ФГОС ВО и ОПОП ВолГУ по специальности 10.05.01 Компьютерная безопасность (специализация №4 Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности) выпускник должен быть подготовлен к следующим **видам деятельности/типам задач профессиональной деятельности[1]:**

научно-исследовательский;

проектный;

эксплуатационный.

По итогам выполнения выпускной квалификационной работы проверятся степень сформированности у выпускника следующих компетенций: УК-1; УК-3; УК-4; УК-5; УК-9; УК-10; ОПК-3; ОПК-4; ОПК-7; ОПК-8; ОПК-9; ОПК-11; ОПК-12; ОПК-13; ОПК-14; ОПК-15: ОПК-16; ОПК-17; ОПК-4.1, ОПК-4.2, ОПК-4.3., ПК-5; ПК-2; ПК-3; ПК-4; ПК-7; ПК-8.

Шифр компетенции	*Расшифровка компетенции*
Универсальные компетенции (УК)	
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
Общепрофессиональная компетенция (ОПК)	
ОПК-3	Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности
ОПК-4	Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности
ОПК-7	Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ
ОПК-8	Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей
ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации
ОПК-11	Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации
ОПК-12	Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения
ОПК-13	Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности
ОПК-14	Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации
ОПК-15	Способен администрировать компьютерные сети и контролировать корректность их функционирования

ОПК-16	Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях
ОПК-17	Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе, для формирования гражданской позиции и развития патриотизма
ОПК-4.1	Способен организовывать защиту информации в компьютерных системах и сетях (по областям применения)
ОПК-4.2	Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения)
ОПК-4.3	Способен разрабатывать и анализировать корректность политики информационной безопасности компьютерных систем и сетей (по областям применения)
Профессиональные компетенции (ПК)	
ПК-2	Способен участвовать в проведении экспериментально исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы
ПК-3	Способен 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
ПК-4	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
ПК-5	Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов
ПК-7	Способен устранять сбои и отказы сетевых устройств и операционных систем
ПК-8	Способен проектировать системы защиты информации на объектах информатизации

3. Тематика выпускных квалификационных работ

1. Разграничение доступа в операционных системах
2. Защита электронного документооборота
3. Разработка обманной системы
4. Моделирование электродинамических свойств радиопоглощающих материалов
5. Инструментальный анализ защищенности информационной системы
6. Обнаружение несанкционированного трафика

7. Обнаружение атак на IoT-устройства
8. Выявление уязвимостей объектов
9. Аудит информационной безопасности
10. Обнаружение таргетированных атак
11. Мониторинг информационной безопасности
12. Оценка эффективности системы защиты платежных терминалов и банкоматов
13. Анонимизация сетевого трафика
14. Управление информационной безопасностью
15. Стеганоанализ контейнеров-изображений
16. Разработка политики безопасности СУБД
17. Анализ событий в SIEM-системах
18. Оценка защищенности субъекта критической информационной инфраструктуры
19. Прогнозирование надежности субъекта критической информационной инфраструктуры
20. Восстановление данных на жестких дисках

4. Требования к выпускной квалификационной работе и общие рекомендации по ее выполнению

В ВКР выпускник должен показать:

Методы системного анализа и описание предметной области и объектов проектирования.

Формальный аппарат для анализа функциональной, информационной, алгоритмической, программной и аппаратной структур объектов проектирования.

Математические модели и методы анализа, расчетов, оптимизации детерминированных и случайных явлений и процессов в объектах проектирования.

Возможности ЭВМ или вычислительных систем объекта проектирования.

Методы и средства разработки алгоритмов и программ, приемы структурного программирования.

Системные программные средства, операционные системы и оболочки, обслуживающие сервисные программы.

Модели представления знаний и формализации задач при разработке интеллектуальных компонентов автоматизированных систем (в зависимости от тематики работы).

Основные инструментальные средства разработки экспертных систем (в зависимости от тематики работы).

Инструментальные средства компьютерной графики и графического диалога (в зависимости от тематики работы).

Каждая выпускная квалификационная работа должна содержать следующие необходимые элементы:

1. введение к ВКР;
2. четыре главы ВКР;
3. заключение к ВКР;
4. приложение с кодом разработанного программного средства;
5. реферат на русском и английском языке;

6. отзыв научного руководителя;
7. рецензия;
8. акт о внедрении разработанного программного средства;
9. отчет системы антиплагиат.

5. Оценочные средства для процедуры защиты ВКР

5.1. Процедура оценивания

Защита выпускной квалификационной работы предусматривает доклад выпускника, выступление научного руководителя, зачитывание рецензии, дискуссию, заключительное слово выпускника, совещание комиссии, составление и подписание протоколов, объявление оценок.

5.2. Критерии оценивания ВКР

№	Критерии оценивания ВКР
1.	Работа носит исследовательский (рационализаторский, изобретательский) характер
2.	Тема работы актуальна
3.	Четко сформулированы тема, цель и задачи исследования
4.	Работа отличается определенной новизной
5.	Работа выполнена самостоятельно
6.	Работа имеет практическое или теоретическое значение
7.	На основе изученной литературы сделаны обобщения, сравнения с собственными результатами и аргументированные выводы
8.	В тексте имеется ссылки на все литературные источники
9.	Содержание работы полностью соответствует теме, целям и задачам
10.	Выбранные методики исследования целесообразны
11.	В работе использованы средства математической и/или статистической обработки данных
12.	Анализируемый материал имеет достаточный объем и позволяет сделать достоверные выводы
13.	Исследуемая проблема достаточно раскрыта
14.	Выводы четко сформулированы, достоверны, опираются на полученные результаты и соответствуют поставленным задачам
15.	ВКР написана с соблюдением требований к структуре, содержанию и оформлению
16.	Работа написана научным языком, текст работы соответствует нормам русского литературного языка, работа вычитана и не содержит опечаток
17.	Список литературы отражает информацию по теме исследования, оформлен в соответствии с требованиями
18.	Работа содержит достаточный иллюстративный материал, в том числе выполненный автором самостоятельно на основе результатов исследования
19.	Доклад четко структурирован, логичен, полностью отражает суть работы
20.	На защите докладчик показал знание исследуемой проблемы и умение вести научную дискуссию, обладает культурой речи
21.	Докладчик активно работает со слайдами презентации, комментирует их
22.	Аргументированность и полнота ответов на вопросы в процессе защиты ВКР
23.	Проведен всесторонний анализ предметной области
24.	Определена модель угроз для предметной области

5.3. Критерии оценивания результатов обучения

Уровень сформированности компетенций	Критерии оценивания	Оценка
Повышенный уровень	обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий	**«отлично»**
Базовый уровень	обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий	**«хорошо»**
Пороговый уровень	обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне	**«удовлетворительно»**
Уровень ниже порогового	система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности	**«неудовлетворительно»**

Оценка защиты выпускной квалификационной работы обучающимся определяется в ходе заседания государственной экзаменационной комиссии (далее – ГЭК) по защите ВКР.

Члены ГЭК по защите ВКР оценивают результаты защиты и вносят их в оценочный лист ГЭК (приложение 1).

При необходимости (в случае отсутствия в составе государственных аттестационных испытаний государственного экзамена), по решению учебно-методической комиссии института, оценка сформированности некоторых компетенций может осуществляться в процессе предзащиты выпускной квалификационной работы (приложение 2). Оценочный лист с оценкой уровня сформированности проверяемых компетенций вместе с отзывом научного руководителя представляются в государственную экзаменационную комиссию до начала проведения итоговых аттестационных испытаний.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ ДЛЯ ПОДГОТОВКИ К ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

1. Основная литература

1. Осипова Виктория Аркадьевна Основы дискретной математики [Электронный ресурс]: учебное - Издание доп. - ФОРУМ, 2017. - 157 с. - Режим доступа: http://znanium.com/go.php?id=534886
2. Канцедал Сергей Андреевич Дискретная математика [Электронный ресурс]: учебное - ФОРУМ, 2019. - 222 с. - Режим доступа: http://znanium.com/go.php?id=978416
3. Гусева Анна Ивановна Дискретная математика [Электронный ресурс]: учебное - КУРС, 2019. - 208 с. - Режим доступа: http://znanium.com/go.php?id=978936
4. Шевелев Ю. П. Дискретная математика [Электронный ресурс]: учебное - Издание 4-е изд., стер. - Лань, 2019. - 592 с. - Режим доступа: https://e.lanbook.com/book/118616
5. Математика и информатика : учебное пособие / К.В. Балдин, В.Н. Башлыков, А.В. Рукосуев, В.Б. Уткин. — Москва :КноРус, 2017. — 361 с. — Бакалавриат. — ISBN 978-5-406-00864-5.
6. Введение в математику : курс лекций / В.М. Казиев. — Москва :Интуит НОУ, 2016. — 206 с. — ISBN 978-5-9556-0105-2.
7. Дискретная математика. Краткий курс : учебное пособие / А.А. Казанский. — Москва : Проспект, 2016. — 317 с. — ISBN 978-5-392-19545-9.
8. Основы дискретной математики : курс лекций / М.И. Дехтярь. — Москва :Интуит НОУ, 2016. — 184 с. — ISBN 978-5-9556-0110-6.
9. Математическая логика и теория алгоритмов для программистов : учебное пособие / Д.В. Гринченков, С.И. Потоцкий. — Москва :КноРус, 2017. — 206 с. — ISBN 978-5-406-05421-5.
10. Математический анализ. Краткий курс : учебное пособие / Р.М. Асланов, О.В. Ли, Т.Р. Мурадов. — Москва : Прометей, 2014. — 284 с. — ISBN 978-5-9905886-5-3.
11. Теория информации для бакалавров. Учебное пособие Павлов Ю., Смирнова Е., Тихомирова Е. М.: МГТУ им. Н. Э. Баумана, 2016, 176 с.
12. Теория информации. Учебное пособие Осокин А., Мальчуков А. Юрайт, 2016, 206 с.
13. Хохлов Г.И. Комбинаторная теория информации (информационная теория детерминированных процессов). Москва : Русайнс, 2018
14. Теория информации и кодирование. Задачник. Учебное пособие Цымбал В.: Ленанд, 2014, 280 с.
15. Лаврищева Е.М. Программная инженерия и технологии программирования сложных систем 2-е изд., испр. и доп., МФТИ, 2018 – 342 с.
16. Павловская Т.А. C#. Программирование на языке высокого уровня: Учебник для вузов Санкт-Петербург: Питер, 2012, 432 с.
17. Вайсфельд Мэтт Объектно-ориентированное мышление Санкт-Петербург: Питер, 2014, 304 с.
18. Васильев А.Н. C#. Объектно-ориентированное программирование. Учебный курс Санкт-Петербург: Питер, 2012, 320 с.
19. Афанасьев А.М. Методы расчета электрических цепей постоянного тока. – Волгоград: Изд-во ВолГУ, 2016. – 64 с.

20. Сети и системы передачи информации. Телекоммуникационные сети. Учебник и практикум Самуйлов К., Шалимов И., Кулябов Д. и др. Юрайт, 2016, 364 с.
21. Коньков К.А., Карпов В.Е. Основы операционных систем // Интуит НОУ, 2016
22. Коньков К.А. Основы организации операционных систем MicrosoftWindows // Интуит НОУ, 2016
23. Сафонов В.О. Основы современных операционных систем // Интуит НОУ, 2016
24. Верещагина Е.А. Операционные системы // Проспект, 2015
25. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft // Интуит НОУ, 2016
26. Проскурин В.Г. Защита в операционных системах, Горячая линия - Телеком, 2014
27. Котельников Е.В. Введение во внутреннее устройство Windows, Интернет-Университет Информационных Технологий (ИНТУИТ), 2013
28. Разработка и эксплуатация удаленных баз данных. Учебник. Фуфаев Э.В., Фуфаев Д.Э. Academia, 2014, 256 с.
29. Лапонина О.Р. Криптографические основы безопасности // Интуит НОУ, 2016
30. Бехроуз А. Фороузан Математика криптографии и теория шифрования // Интуит НОУ, 2016
31. Басалова Г.В. Основы криптографии // Интуит НОУ, 2016
32. Федеральный закон Российской Федерации "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г. N 149-ФЗ.
33. Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1.
34. Скрипник Д. А. Общие вопросы технической защиты информации. Национальный Открытый Университет «ИНТУИТ». - 2016 г. - 425 с.
35. Инструментальный контроль и защита информации: учебное пособие. ВГУИТ. - 2013 г. - 192 с.
36. Сагдеев К. М., Петренко В. И., Чипига А. Ф. Физические основы защиты информации: учебное пособие. - СКФУ 2015 г. - 394 с.
37. Зайцев, А.П. Технические средства и методы защиты информации. [Электронный ресурс] / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 442 с. — Режим доступа: http://e. Программные средства защиты информации lanbook.com/book/5155
38. Долозов Н. Л., Гультяева Т. А.: конспект лекций. НГТУ – 2015 г. – 63 с.
39. Степанов-Егиянц В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации: монография. Статут – 2016 г. 190 страниц
40. Курило А.П.., Милославская Н.Г., Толстой А.И., Сенаторов М.Ю. Основы управления информационной безопасностью. М.:Горячаялиния-Телеком, 2014.
41. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. - М.: ГТК - 1992 г. - 13с.
42. Гостехкомиссия России. Руководящий документ: Средства вычислительной техники. Межсетевые экраны. Показатели защищенности от несанкционированного доступа. - М.: ГТК - 1997 г. - 17с.
43. Платунова, С.М. Построение корпоративной сети с применением коммутационного оборудования и настройкой безопасности. Учебное пособие по дисциплине

«Корпоративные сети». [Электронный ресурс] — Электрон. дан. — СПб. : НИУ ИТМО, 2012. — 85 с.
44. МэйволдЭ.Безопасность сетей. Национальный Открытый Университет «ИНТУИТ» Национальный Открытый Университет «ИНТУИТ» – 2016 г. – 572 с.
45. Брэгг Р., Родс-Оусли М., СтрассбергК.Безопасность сетей. Полноеруководство
46. Советов, Б. Я. Моделирование систем : учебник для академического бакалавриата / Б. Я. Советов, С. А. Яковлев. — 7-е изд. — М. : Издательство Юрайт, 2017. — 343 с. — (Серия : Бакалавр. Академическийкурс). — ISBN 978-5-9916-3916-3.
47. Петров, А.В. Моделирование процессов и систем [Электронный ресурс] : учеб. пособие — Электрон. дан. — Санкт-Петербург : Лань, 2015. — 288 с. — Режим доступа: https://e.lanbook.com/book/68472. — Загл. с экрана.
48. Акопов, А. С. Имитационное моделирование : учебник и практикум для академического бакалавриата / А. С. Акопов. — М. : Издательство Юрайт, 2018. — 389 с. — (Серия : Бакалавр. Академическийкурс). — ISBN 978-5-534-02528-6.
49. Закон РФ «О государственной тайне» от 21 июля 1993 г. № 5485-1
50. Рембовский, А.М. Радиомониторинг: задачи, методы, средства. [Электронный ресурс] / А.М. Рембовский, А.В. Ашихмин, В.А. Козьмин. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 624 с.
51. Дятлов, А.П. Корреляционная обработка широкополосных сигналов в автоматизированных комплексах радиомониторинга. [Электронный ресурс] / А.П. Дятлов, Б.Х. Кульбикаян. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 332 с.
52. Кирсанов, Э.А. Обработка информации в пространственно-распределенных системах радиомониторинга: статистический и нейросетевой подходы. [Электронный ресурс] / Э.А. Кирсанов, А.А. Сирота. — Электрон. дан. — М. : Физматлит, 2012. — 344 с.
53. Сагдеев К. М., Петренко В. И., Чипига А. Ф. Физические основы защиты информации: учебное пособие. - СКФУ 2015 г. - 394 с.Зайцев, А.П. Технические средства и методы защиты информации. [Электронный ресурс] / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 442 с. — Режим доступа: http://e.lanbook.com/book/5155
54. ГОСТ Р 51320-99. Совместимость технических средств электромагнитная. Радиопомехииндустриальные. Методыиспытанийтехническихсредств - источниковиндустриальныхрадиопомех.
55. Сакалема Д.Ж., Филинова А.С., Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) // Учебное пособие для вузов / М.: Горячая линия– Телеком, 2013. – 220 с.
56. О.И.Шелухин, А.Н.Руднев, А.В.Савелов Системы обнаружения вторжений в компьютерные сети // Учебное пособие. МТУСИ, Москва, 2013 г, 97 стр.
57. Богомолова О.Б., Усенков Д.Ю. Защита компьютера от вредоносных воздействий: практикум // М.: БИНОМ. Лабораториязнаний, 2012.— 175 с.
58. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: учебное пособие // Омск: Омский государственный университет, 2013.— 160 с.
59. Милославская. Н.Г. Вопросы управление информационной безопасностью Москва : Горячая линия-Телеком, 2013.

60. Сакалема Д.Ж., Филинова А.С., Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) // Учебное пособие для вузов / М.: Горячая линия–Телеком, 2015. – 220 с.
61. О.И. Шелухин, А.Н.Руднев, А.В.Савелов Системы обнаружения вторжений в компьютерные сети // Учебное пособие. МТУСИ, Москва, 2015 г, 97 стр.
62. Курячий Г.В. Операционная система UNIX // Интуит НОУ, 2016
63. Курячий Г.В., Маслинский К.А. Операционная система Linux // Интуит НОУ, 2016
64. Мошков М.Е. Введение в системное администрирование Unix // Интуит НОУ, 2016
65. Костромин В.А. Основы работы в ОС Linux // Интуит НОУ, 2016
66. Бражук А.И. Сетевые средства Linux // Интуит НОУ, 2016
67. Харрис Дэвид М., Харрис Сара Л. Цифровая схемотехника и архитектура компьютера. Morgan Kaufman, 2013 (перевод: февраль 2015) – 1622 с.
68. Таненбаум Э., Остин Т. Архитектура компьютера. 6-е издание. СПб.: Питер, 2013 – 816 с.

2. Дополнительная литература

1. Основы математического анализа [Электронный ресурс] : учебное пособие / О. В. Савченко ; Себряк. фил. Волгогр. гос. архит.-строит. ун-та. - Волгоград : Изд-во ВолГУ, 2013. - 76 с. - ISBN 978-5-9669-1130-0.
2. Математическая логика и теория алгоритмов [Электронный ресурс] : учебно-методическое пособие : в 2 ч. Ч. 2 : Алгебра логики предикатов / Т. В. Штельмах ; ВолГУ. - Волгоград : Изд-во ВолГУ, 2014. - 54 с. - Список лит.: с. 53-54. - ISBN 978-5-9669-1304-5.
3. Основы теории графов [Электронный ресурс] : учебно-методическое пособие / В. В. Попов ; ВолГУ. - : Изд-во ВолГУ, 2014. - 48 с.
4. Дискретно-непрерывная математика [Электронный ресурс] . Кн. 4, ч. 4 : Алгебры и дифференциалы / А. Е. Кононюк. - Киев : ОсвітаУкраіни, 2015. - 690 с. - (Парадигма развития науки. Методологическое обеспечение). - ISBN 978-966-373-693-8. - ISBN 978-966-373-694-5.
5. Дискретно-непрерывная математика [Электронный ресурс] . Кн. 7, ч. 2 : Графы / А. Е. Кононюк. - Киев : ОсвітаУкраіни, 2015. - 512 с. - (Парадигма развития науки. Методологическое обеспечение). - ISBN 978-966-373-693-8. - ISBN 978-966-373-694-5.
6. Дискретно-непрерывная математика [Электронный ресурс] . Кн. 3, ч. 1 : Отношения. Четкие / А. Е. Кононюк. - Киев : ОсвітаУкраіни, 2013. - 506 с. - (Парадигма развития науки. Методологическое обеспечение). - ISBN 978-966-373-693-8. - ISBN 978-966-373-694-5.
7. Дискретно-непрерывная математика [Электронный ресурс] . Кн. 6, ч. 1 : Поверхности / А. Е. Кононюк. - Киев : ОсвітаУкраіни, 2013. - 564 с. - (Парадигма развития науки. Методологическое обеспечение). - ISBN 978-966-373-693-8. - ISBN 978-966-373-694-5.
8. . Баскаков С.И. Радиотехнические цепи и сигналы. – М.: Высшая школа, 1983. – 535 с.
9. Компьютерные сети. 5-е изд. : Таненбаум Э. С., Уэзеролл Д. СПб. : Питер, 2011, 960 с
10. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. Олифер В. Г., Олифер Н. А. СПб. : Питер, 2012, 944 с., МО РФ
11. И.Ф. Астахова Компьютерные науки. Деревья, операционные системы, сети, ФИЗМАТЛИТ, 2013
12. Журавлева Т.Ю. Практикум по дисциплине «Операционные системы», Вузовское образование, 2014

13. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками, Горячая линия - Телеком, 2013
14. Руководящий документ. ФСТЭК. Режим доступа: http://fstec.ru/component/tags/tag/7-rukovodyashchij-dokument
15. Дж. Фостер, В. Лю. Разработка средств безопасности и эксплойтов / Перевод с английского. – М.: Издательство "Русская Редакция"; СПб.: Питер, 2007.
16. Ерофеев А.А. Теория автоматического управления. Учеб. для вузов. СПб: Политехника, 2001, 302 с.
17. Цыпкин Я.З. Основы теории автоматических систем. М.: Наука, 1977, 560 с.
18. Богомолова О.Б., Усенков Д.Ю. Защита компьютера от вредоносных воздействий: практикум // М.: БИНОМ. Лаборатория знаний, 2014.— 175 с.
19. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: учебное пособие // Омск: Омский государственный университет, 2015.— 160 с.
20. Варлатая С.К., Шаханова М.В. Криптографические методы и средства обеспечения информационной безопасности // Проспект, 2015
21. Бабаш А.В., Баранова Е.К. Криптографические методы защиты информации (для бакалавров и магистров) // КноРус, 2018
22. Никишова А.В., Македонский С.А., Оладько В.С. Лабораторный практикум по защите операционных систем // Издательство ВолГУ, 2017
23. Карпов В.Е., Коньков К.А. Основы операционных систем. Практикум // Интуит НОУ, 2016
24. Назаров С.В., Широков А.И. Современные операционные системы // Интуит НОУ, 2016
25. Никишова А.В., Македонский С.А., Оладько В.С. Лабораторный практикум по защите операционных систем // Издательство ВолГУ, 2017
26. Администрирование ОС Unix // Интуит НОУ, 2016
27. Гончарук С.В. Администрирование ОС Linux // Интуит НОУ, 2016
28. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М., 2008, 31 с.
29. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2014, 106 с
30. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. М., 2014, 58 с.
31. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011, 51 с
32. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

33. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности
34. ГОСТ Р ИСО/МЭК 27013-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1
35. ГОСТ Р ИСО/МЭК 27031-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса.
36. Шелухин, О.И. Моделирование информационных систем [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 536 с. — Режим доступа: https://e.lanbook.com/book/5204. — Загл. с экрана.
37. Афонин, В.В. Моделирование систем [Электронный ресурс] : учеб. пособие / В.В. Афонин, С.А. Федосин. — Электрон. дан. — Москва : , 2016. — 269 с. — Режим доступа: https://e.lanbook.com/book/100659. — Загл. с экрана.
38. Колесов, Ю.Б. Математическое моделирование гибридных динамических систем: учеб. пособие [Электронный ресурс] : учеб. пособие / Ю.Б. Колесов, Ю.Б. Сениченков. — Электрон. дан. — Санкт-Петербург : СПбГПУ, 2014. — 236 с. — Режим доступа: https://e.lanbook.com/book/64806. — Загл. с экрана.
39. Лаврищева Е.М. Программная инженерия. Парадигмы, технологии и case-средства 2-е изд., МФТИ, 2018 - 280 с.
40. Кубенский А.А. Функциональное программирование, 2018 - 348 с.

V. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

В рамках освоения образовательной программы каждому обучающемуся предоставляется неограниченный доступ к электронной информационно-образовательной среде (ЭИОС) университета.

ЭИОС, разработанная на платформе Русский Moodle, обеспечивает доступ к рабочим программам дисциплин (модулей), практик, электронным учебным изданиям и электронным образовательным ресурсам.

Для подготовки к государственной итоговой аттестации используется:

- MS Office;
- MS Visual Studio;
- Oracle VM VirtualBox.

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Учебные аудитории для проведения аттестационных испытаний, оснащенные мультимедийным оборудованием: 2-24бК

ОЦЕНКА УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

оценочный лист государственной экзаменационной комиссии

по приему государственного экзамена/по защите выпускной квалификационной работе

Направление подготовки 10.05.03 «Компьютерная безопасность» специализация: "Безопасность компьютерных систем и сетей" (по отрасли или в сфере профессиональной деятельности)

Уровень сформированности: повышенный – 5 баллов; базовый – 4 балла, пороговый – 3 балла, ниже порогового – 2 балла

№	ФИО выпускника	Индекс компетенции																												Среднее значение оценки уровня сформированности компетенций
		Оценка уровня сформированности																												
1																														

Председатель ГЭК _____ /_____/

Члены ГЭК:

_____ /_____/ _____ /_____/ _____ /_____/

_____ /_____/ _____ /_____/ _____ /_____/

«___»_____ 20__ г.

Приложение к оценочному листу ГЭК

(справочно для комиссии)

Критерии сформированности компетенций

Уровень сформированности компетенций	Критерии оценивания
Повышенный уровень	обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий
Базовый уровень	обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий
Пороговый уровень	обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне
Уровень ниже порогового	система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности