Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования «Самарский национальный исследовательский
университет имени академика С.П. Королева»

САМАРСКИЙ УНИВЕРСИТЕТ
SAMARA UNIVERSITY

УТВЕРЖДЕН
21 февраля 2020 года, протокол ученого совета университета №7
Сертификат №: 2a f4 e3 1f 00 01 00 00 02 19
Срок действия: с 08.03.19г. по 08.03.20г.
Владелец: проректор по учебной работе
А.В. Гаврилов

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Код плана	100501.65-2020-О-ПП-5г06м-02
Основная профессиональная образовательная программа высшего образования по направлению подготовки (специальности)	10.05.01 Компьютерная безопасность
Профиль (программа, специализация)	специализация N 7 "Информационно-аналитическая и техническая экспертиза компьютерных систем":
Квалификация (степень)	Специалист по защите информации
Блок, в рамках которого проводится государственная итоговая аттестация	Б3
Институт (факультет)	Факультет математики
Кафедра	безопасности информационных систем
Форма обучения	очная
Курс, семестр	6 курс, 11 семестр
Форма (формы) государственной итоговой аттестации	Государственный итоговый экзамен, защита выпускной квалификационной работы

Самара, 2020

Настоящая программа государственной итоговой аттестации является составной частью основной профессиональной образовательной программы высшего образования Информационно-аналитическая и техническая экспертиза компьютерных систем по специальности 10.05.01 Компьютерная безопасность, обеспечивающей реализацию федерального государственного образовательного стандарта высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета), утвержденного приказом Минобрнауки России от 01.12.2016 №1512 (Зарегистрировано в Минюсте России 20.12.2016 №44825)

Составители:

Заведующий
Кафедрой геоинформатики и информационной безопасности /*В.В. Сергеев*/

Заведующий
кафедрой безопасности информационных систем /*М.Н. Осипов*/

Заведующий
кафедрой безопасности информационных систем /*М.Н. Осипов*/

«_13__»___01____ 20_20_ г.

Программа государственной итоговой аттестации обсуждена на заседании кафедры
безопасности информационных систем

Протокол № 08 от «13» января 2020 г.

Руководитель основной профессиональной образовательной программы высшего образования Информационно-аналитическая и техническая экспертиза компьютерных систем по специальности 10.05.01 Компьютерная безопасность
_____ /*М.Н. Осипов*/

1. ОБЩАЯ ХАРАКТЕРИСТИКА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ)

Государственная итоговая аттестация (далее – ГИА) представляет собой форму оценки степени и уровня освоения обучающимися образовательной программы. ГИА проводится на основе принципов объективности и независимости оценки качества подготовки обучающихся.

ГИА проводится государственными экзаменационными комиссиями (далее – ГЭК). Для рассмотрения апелляций по результатам ГИА в Самарском университете (далее - университет) создаются апелляционные комиссии. Регламенты работы государственной экзаменационной комиссии, экзаменационной комиссии и апелляционной комиссии (далее вместе – комиссии) установлены локальными нормативными актами университета.

ГИА проводится в целях определения соответствия результатов освоения обучающимися основной профессиональной образовательной программы высшего образования Информационно-аналитическая и техническая экспертиза компьютерных систем по специальности 10.05.01 Компьютерная безопасность, соответствующим требованиям федерального государственного образовательного стандарта высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета) (далее – ФГОС ВО).

ГИА, завершающая освоение настоящей основной профессиональной образовательной программы высшего образования (далее – ОПОП ВО), является обязательной и проводится в порядке и в форме, которые установлены законодательством об образовании, настоящей программой и иными локальными нормативными актами университета, регулирующими вопросы организации и проведения ГИА.

Содержание и характеристика формы (вида) государственных итоговых аттестационных испытаний приведены в таблице 1.

Таблица 1. Содержание и характеристика формы (вида) итоговых аттестационных испытаний

Форма проведения ГИА	**Содержание ГИА**	**Характеристика формы (вида) ГИА**
Государственный экзамен	подготовка к сдаче и сдача государственного экзамена	устный
Защита выпускной квалификационной работы	защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	выпускная квалификационная работа

Настоящая программа ГИА, включая программу государственного экзамена и требования к выпускным квалификационным работам (далее – ВКР) и порядку их выполнения, критерии оценки результатов сдачи государственного экзамена и защиты ВКР, утвержденные университетом, а также порядок подачи и рассмотрения апелляций доводятся до сведения обучающихся не позднее чем за шесть месяцев до начала ГИА.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОПОП ВО В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФГОС ВО И ОПОП ВО

Планируемые результаты освоения ОПОП ВО – это компетенции, установленные ФГОС ВО.

Перечень планируемых результатов освоения ОПОП ВО приведен в таблице 2.

Таблица 2. Перечень планируемых результатов освоения ОПОП ВО

Код компетенции	Содержание компетенции
Общекультурные компетенции (ОК)	
ОК-1	Способность использовать основы философских знаний для формирования мировоззренческой позиции
ОК-2	Способность использовать основы экономических знаний в различных сферах деятельности
ОК-3	Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма
ОК-4	Способность использовать основы правовых знаний в различных сферах деятельности
ОК-5	Способность 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
ОК-6	Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия
ОК-7	Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности
ОК-8	Способность к самоорганизации и самообразованию
ОК-9	Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности
Общепрофессиональные компетенции (ОПК)	
ОПК-1	Способность анализировать физические явления и процессы при решении профессиональных задач
ОПК-2	Способность 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
ОПК-3	Способность 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
ОПК-4	Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
ОПК-5	Способность использовать нормативные правовые акты в своей профессиональной деятельности
ОПК-6	Способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций
ОПК-7	Способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения

Код компетенции	Содержание компетенции
ОПК-8	Способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач
ОПК-9	Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации
ОПК-10	Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах
Профессиональные компетенции (ПК)	
ПК-1	Способность 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
ПК-2	Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований
ПК-3	Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности
ПК-4	Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем
ПК-5	Способность 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
ПК-6	Способность участвовать в разработке проектной и технической документации
ПК-7	Способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем
ПК-8	Способность участвовать в разработке подсистемы информационной безопасности компьютерной системы
ПК-9	Способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы
ПК-10	Способность 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
ПК-11	Способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации
ПК-12	Способность проводить инструментальный мониторинг защищенности компьютерных систем

Код компетенции	Содержание компетенции
ПК-13	Способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности
ПК-14	Способность организовать работы по выполнению режима защиты информации, в том числе ограниченного доступа
ПК-15	Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы
ПК-16	Способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующих работу по обеспечению информационной безопасности компьютерных систем
ПК-17	Способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение
ПК-18	Способность 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-19	Способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации
ПК-20	Способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций
Профессионально-специализированные компетенции (ПСК)	
ПСК-7.1	Способность использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов
ПСК-7.2	Способность проводить экспертизу вычислительной техники и носителей компьютерной информации
ПСК-7.3	Способность руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий
ПСК-7.4	Способность подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем
ПСК-7.5	Способность разрабатывать программное обеспечение, предназначенное для выявления следов компьютерных преступлений и инцидентов

3. УКАЗАНИЕ ОБЪЕМА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ В ЗАЧЕТНЫХ ЕДИНИЦАХ И ЕЕ ПРОДОЛЖИТЕЛЬНОСТИ В НЕДЕЛЯХ И В АКАДЕМИЧЕСКИХ ЧАСАХ

Объем ГИА и продолжительность ее проведения приведены в таблице 3.

Таблица 3. Объем государственной итоговой аттестации в зачетных единицах и ее продолжительность

Наименования показателей, характеризующих объем и продолжительность ГИА	**Значение показателей объема и продолжительности ГИА**
Семестр	11
Количество зачетных единиц	9
Количество недель	6
Количество академических часов на подготовку к сдаче и сдачу государственного экзамена	108
в том числе: лекция (предэкзаменационная консультация)	2
самостоятельная работа (подготовка к сдаче государственного экзамена по вопросам, включенным в программу государственного экзамена), академических часов	70
контроль (сдача экзамена, включая подготовку к процедуре сдачи государственного экзамена), академических часов	36
Количество академических часов на защиту выпускной квалификационной работы, включая подготовку к защите и процедуру защиты:	216
контролируемая самостоятельная работа (контроль готовности ВКР просмотровой комиссией кафедры), академических часов	2
самостоятельная работа (подготовка к защите ВКР), академических часов	178
контроль (защита ВКР, включая подготовку к процедуре защиты), академических часов	36

4. СТРУКТУРА И СОДЕРЖАНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

ГИА включает ряд этапов, необходимых для организации и проведения государственных аттестационных испытаний, предусмотренных ОПОП ВО в соответствии с ФГОС ВО. Структура и содержание этапов ГИА приведены в таблице 5.

Таблица 4. Структура и содержание этапов ГИА

Этапы подготовки и проведения ГИА	**Содержание этапа**
1. Подготовительный (организационный) этап к процедуре ГИА	Утверждение председателя ГЭК. Утверждение составов комиссий. Утверждение программы ГИА по ОПОП ВО. Утверждение перечня тем ВКР по ОПОП ВО. Доведение до сведения обучающихся программы ГИА и утвержденного перечня тем ВКР по ОПОП ВО не позднее чем за шесть месяцев до начала ГИА. Закрепление за обучающимися тем ВКР (на основании их личных заявлений), руководителей ВКР и при необходимости консультанта (консультантов) приказом ректора или уполномоченного им лица. Утверждение распорядительным актом расписания государ-

Этапы подготовки и проведения ГИА	Содержание этапа
	ственных аттестационных испытаний не позднее, чем за 30 календарных дней до дня проведения первого государственного аттестационного испытания. Доведение расписания государственных аттестационных испытаний до сведения обучающегося, председателя и членов комиссий, секретарей ГЭК, руководителей и консультантов ВКР. Организация работы комиссий.
2. Подготовка к сдаче государственного экзамена	Самостоятельная работа обучающихся по подготовке к государственному экзамену в соответствии с перечнем вопросов, выносимых на государственный экзамен, рекомендациями обучающимся по подготовке к государственному экзамену и перечнем рекомендуемой литературы для подготовки к государственному экзамену. Изучение рекомендуемой литературы. Самоконтроль результатов обучения по ОПОП ВО.
3. Предэкзаменационная консультация	Дополнительное рассмотрение вопросов, вызвавших трудности на этапе подготовке к государственному экзамену. Доведение информации до обучающихся о регламенте проведения государственного экзамена. Распределение обучающихся на группы для сдачи государственного экзамена.
4. Сдача государственного экзамена	Подготовка ответов на вопросы выбранного экзаменационного билета. Ответ на вопросы билета на заседании ГЭК. Ответы на дополнительные вопросы членов ГЭК.
5. Подготовка к защите ВКР	Представление руководителю для проверки полного текста ВКР. Устранение замечаний (при необходимости).
	Подготовка доклада о результатах ВКР и раздаточного материала, иллюстрирующего содержание доклада о результатах ВКР. Предоставление доклада и раздаточного материала руководителю ВКР. Устранение замечаний (при необходимости).
	Оформление текста ВКР. Нормоконтроль оформления текста ВКР. Проверка текста ВКР на объём заимствования.
	Ознакомление обучающегося с отзывом руководителя на ВКР и рецензией (рецензиями) на ВКР не позднее чем за 5 календарных дней до дня защиты ВКР. Предварительный просмотр ВКР на кафедре. Получение допуска комиссии выпускающей кафедры к защите ВКР по результатам просмотра. Устранение замечаний (при необходимости). Размещение текстов ВКР в электронно-библиотечной системе университета через личный кабинет обучающегося. Передача в ГЭК ВКР, отзыва и рецензии (рецензий) не позднее чем за 2 календарных дня до дня защиты ВКР.
6. Процедура защиты ВКР	Процедура защиты ВКР включает в себя: – открытие заседания ГЭК председателем ГЭК; – доклад обучающегося; – вопросы членов ГЭК; – заслушивание отзыва руководителя ВКР; – заслушивание рецензии; – заключительное слово обучающегося.

Этапы подготовки и проведения ГИА	Содержание этапа
7. Заключительный (организационный) этап процедуры ГИА	Оформление протоколов заседаний ГЭК по результатам каждого заседания ГЭК в соответствии с утвержденным расписанием государственных аттестационных испытаний. Оформление книг протоколов заседаний ГЭК. Сдача протоколов заседаний ГЭК на хранение в архив университета.

5. ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

5.1 Перечень вопросов, выносимых на государственный экзамен

1. Непрерывность действительных функций одной действительной переменной. Классификация точек разрыва. Свойства функций непрерывных на отрезке. Доказательство теоремы о промежуточном значении непрерывной функции.
2. Дифференцируемость функций одной и нескольких действительных переменных. Дифференциал функции. Достаточные условия дифференцируемости (без доказательства). Основные теоремы дифференциального исчисления функций одной переменной: теорема Ферма (с доказательством), теоремы Роля, Лагранжа, Коши (без доказательства).
3. Вывод формулы Тейлора для функций одной действительной переменной. Экстремумы функций одной переменной. Достаточное условие существования экстремума (с доказательством).
4. Абсолютно и условно сходящиеся числовые ряды: признаки сравнения и Даламбера (с доказательством), признаки Коши и Лейбница (без доказательства.)
5. Степенные ряды: теорема Абеля (без доказательства). Область и радиус сходимости степенного ряда. Ряды Тейлора и Маклорена. Достаточное условие разложимости функции в ряд Тейлора (с доказательством).
6. Первообразная и неопределенный интеграл. Определенный интеграл и его свойства. Существование первообразной для непрерывной функции (без доказательства). Интеграл с переменным верхним пределом, формула Ньютона-Лейбница (с доказательством).
7. Ряды Фурье. Признак Дини поточечной сходимости рядов Фурье (с доказательством).
8. Матрицы и операции над ними. Определители матриц и их свойства. Ранг матрицы. Критерий обратимости матриц (с доказательством). Способы вычисления обратной матрицы.
9. Системы линейных уравнений. Критерий Кронекера–Капелли (с доказательством). Теорема о структуре общего решения системы линейных уравнений (без доказательства).
10. Кольцо вычетов. Сравнения и их основные свойства. Малая теорема Ферма (с доказательством).
11. Кольцо многочленов. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида.
12. Группы и их основные свойства. Примеры: циклические группы, конечные абелевые группы. Смежные классы по подгруппе. Теорема Лагранжа (с доказательством).
13. Векторные пространства их базисы и размерность. Координаты векторов в базисе и их изменение при переходе к другому базису.
14. Линейные преобразования векторного пространства и их матрицы. Характеристический многочлен линейного преобразования. Собственные значения и собственные векторы.
15. Квадратичные формы, их матрицы и ранг. Эквивалентность квадратичных форм, приведение к каноническому виду (с доказательством). Положительно определенные квадратичные формы, критерий Сильвестра (без доказательства).

16. Конечные поля. Характеристика поля. Построение конечного поля с заданным числом элементов.
17. Вероятностное пространство. Аксиоматика А.Н. Колмогорова. Свойства вероятностной меры. Классическое определение вероятности.
18. Условные вероятности. Независимость событий. Формула полной вероятности и формула Байеса.
19. Случайные величины. Функции распределения случайных величин и их свойства. Плотности распределения. Типовые распределения: биномиальное, пуассоновское, равномерное, гауссовское (нормальное). Многомерные функции распределения. Многомерное нормальное Распределение. Независимые случайные величины.
20. Определение математического ожидания случайной величины, как интеграла Лебега по вероятностной мере. Формулы вычисления математических ожидания для дискретных и абсолютно непрерывных случайных величин. Дисперсия случайной величины и ее свойства. Коэффициент ковариации случайных величин. Вычисление математических ожиданий и дисперсий случайных величин имеющих типовые распределения.
21. Неравенство П.Л. Чебышева (с доказательством). Закон больших чисел в форме Чебышева (с доказательством).
22. Определение характеристических функций случайных величин. Вычисление характеристических функций случайных величин имеющих типовые распределения. Свойства характеристических функций (без доказательства). Метод характеристических функций в доказательстве предельных теорем. Центральная предельная теорема для независимых одинаково распределенных случайных величин с ограниченной дисперсией (с доказательством). Следствие: теорема Муавра-Лапласа.
23. Дифференцируемость функции комплексного переменного. Вывод условий Коши-Римана.
24. Интеграл от функции комплексного переменного. Теорема Коши об интеграле от аналитической функции по замкнутому контуру (с доказательством). Интегральная формула Коши (с доказательством).
25. Основные типы дифференциальных уравнений первого порядка и методы их решения. Теорема существования и единственности решения дифференциального уравнения первого порядка (без доказательства).
26. Линейные дифференциальные уравнения n-го порядка, структура общего решения (без доказательства). Решение линейных дифференциальных уравнений n-го порядка с постоянными коэффициентами.
27. Алгебра множеств и отношений. Представление алгебр множеств и отношений матричными алгебрами.
28. Функциональные отношения. Отношения эквивалентности и порядка на конечных множествах, свойства их матриц.
29. Универсальные алгебры с конечным носителем. Представление операций многомерными двоичными массивами.
30. Булевы функции. Представление булевых функций формулами алгебры.
31. Исчисления высказываний и предикатов, их полнота и непротиворечивость.
32. Мера количества информации. Энтропия и ее свойства.
33. Теорема Шеннона о пропускной способности канала связи.
34. Линейные блоковые коды. Корректирующие свойства кодов. Код Хемминга.
35. Определение циклического кода. Сверточный код. Алгоритм Витерби.
36. Виды атак в IP сетях. Причины уязвимости IP сетей.
37. Модель информационной безопасности систем. Типовые виды угроз безопасности.
38. Классификация способов и средств защиты информации в сетях.
39. Защита от вирусов.
40. Стандартные методы защиты сетей, МСЭ. Защита доверительной сети, VPN.

41. Требования к системе безопасности сетей. Принципы построения системы обеспечения безопасности корпоративной сети.
42. Понятие базы данных и СУБД. Основные функции СУБД. Архитектура многопользовательских СУБД
43. Базы данных. Реляционная модель и нормализация.
44. Алгоритмы на графах. Алгоритм Крускала. Алгоритм Дейкстры. Оценка сложности.
45. Алгоритмы поиска в последовательно организованных файлах. Оценка трудоемкости.
46. Алгоритмы поиска в деревьях.
47. Основные понятия защиты информации. Построение защищенной автоматизированной системы.
48. Угрозы безопасности информации. Понятие политики безопасности.
49. Модели системы безопасности, примеры моделей.
50. Основные положения Руководящих документов ФСТЭК в области защиты информации.
51. Основное содержание ГОСТ в области защиты информации.
52. Криптография и криптоанализ. Конфиденциальность, целостность, имитостойкость. Теоретическая и практическая стойкость шифра.
53. Классификация криптографических систем. Шифры простой и сложной замены, перестановки, гаммирования.
54. Криптосистемы с секретным ключом. Поточные криптосистемы. Шифрование методом гаммирования.
55. Криптосистемы с секретным ключом. Блочные шифры. Сеть Фейстеля. Стандарт шифрования DES. Российский стандарт шифрования ГОСТ 28147-89. Основные режимы работы блочных шифров.
56. Криптосистемы с открытым ключом. Односторонние функции, односторонние функции с секретом. Криптосистема RSA. Криптосистема Эль Гамаля.
57. Криптографические хэш-функции. Однонаправленные хэш-функции. Алгоритм безопасного хеширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции ГОСТ Р 34.11-94.
58. Электронная подпись. Схемы ЭП
59. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.
60. Правовые основы защиты информации с использованием технических средств.
61. Организация и обеспечение режима секретности.
62. Лицензирование и сертификация в области защиты информации.
63. Проблемы компьютерной безопасности на современном этапе.
64. Экономическая эффективность объектов информационной безопасности.
65. Основные этапы и закономерности исторического развития России, история развития информационной безопасности.
66. Социальная значимость профессии в сфере информационной безопасности. Ее роль в жизни современного общества.
67. Основные методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности в области компьютерной безопасности.
68. Основные приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций

5.2. Рекомендации обучающимся по подготовке к государственному экзамену

Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к государственному экзамену, обучающиеся ликвидируют имеющиеся пробелы в знаниях, углубляют, систематизируют и упорядочивают свои умения, навыки. На государственном экзамене обучающиеся демонстрируют то, что они приобрели в процессе обучения.

В период подготовки к государственному экзамену обучающиеся вновь обращаются к учебно-методическому материалу и закрепляют знания, умения, навыки. Целесообразно использовать материалы лекций, учебно-методические комплексы, справочники, основную и дополнительную литературу.

Вопросы, выносимые на государственный экзамен, составлены по дисциплинам, результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников: Математический анализ, Алгебра, Теория вероятностей и математическая статистика, Теория функций комплексного переменного, Дифференциальные уравнения, Дискретная математика, Математическая логика и теория алгоритмов, Теория информации, Алгоритмы кодирования и сжатия информации, Системы управления базами данных, Защита программ и данных, Основы построения защищенных баз данных, Методы программирования, Операционные системы, Защита в операционных системах, Компьютерные сети, Модели безопасности компьютерных систем, Основы построения защищенных компьютерных сетей, Методы и стандарты оценки защищенности компьютерных систем, Криптографические методы защиты информации, Криптографические протоколы, Организационное и правовое обеспечение информационной безопасности, Информационно-аналитическая деятельность по обеспечению защиты информации, Программно-аппаратные средства обеспечения информационной безопасности, Теоретико-числовые методы в криптографии, Модели угроз и нарушителей информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении, Экспертиза носителей компьютерной информации, Системы обнаружения компьютерных атак, Анализ уязвимостей программного обеспечения, Инструментальные средства проведения расследования компьютерных инцидентов.

Формулировка вопросов экзаменационного билета совпадает с формулировкой перечня рекомендованных для подготовки вопросов государственного экзамена, доведенного до сведения обучающихся за 6 месяцев до экзаменационной сессии.

Представляется крайне важным посещение обучающимися проводимой перед государственным экзаменом консультации. Здесь есть возможность задать вопросы преподавателю по тем разделам и темам, которые недостаточно или противоречиво освещены в учебной, научной литературе или вызывают затруднение в восприятии. Подобного рода консультации весьма эффективны и с психологической точки зрения.

Важно, чтобы обучающийся грамотно распределил время, отведенное для подготовки к государственному экзамену. В этой связи целесообразно составить календарный план подготовки к экзамену, в котором в определенной последовательности отражается изучение или повторение всех экзаменационных вопросов.

Экзамен проводится в форме устного ответа на вопросы экзаменационного билета. За отведенное для подготовки время обучающийся должен сформулировать четкий ответ по каждому вопросу билета. При ответе на экзамене допускается многообразие мнений. Это означает, что обучающийся вправе выбирать любую точку зрения по дискуссионной проблеме, но с условием достаточной аргументации своей позиции. Приветствуется, если обучающийся не читает с листа, а свободно излагает материал.

К выступлению на государственном экзамене предъявляются следующие требования:

- ответ должен строго соответствовать объему вопросов билета;
- ответ должен полностью исчерпывать содержание вопросов билета;
- выступление на экзамене должно соответствовать нормам и правилам публичной речи, быть четким, обоснованным, логичным.

Обучающийся должен быть готов и к дополнительным (уточняющим) вопросам, которые могут быть заданы в рамках билета и связаны, как правило, с неполным ответом. Уточняющие вопросы задаются, чтобы либо конкретизировать ответ на вопрос билета, либо чтобы обучающийся подкрепил те или иные теоретические положения практикой. Полный ответ на уточняющие вопросы лишь усиливает эффект общего ответа.

5.3. Перечень рекомендуемой литературы для подготовки к государственному экзамену

5.3.1. Основная литература

1. Ильин, В. А. Математический анализ. - Ч. 1, кн. 1 . - 2017. Ч. 1, кн. 1 . - 331 с.
2. Ильин, В. А. Математический анализ. - Ч. 1, кн. 2 . - 2017. Ч. 1, кн. 2 . - 328 с
3. Ильин, В. А. Математический анализ. - Ч. 2 . - 2017. Ч. 2. - 357 с.
4. Беклемишев, Д.В. Курс аналитической геометрии и линейной алгебры: учебник / Д.В. Беклемишев. - 12-е изд., испр. - Москва: Физматлит, 2009. - 309 с [Электронный ресурс] – Режим доступа: http://biblioclub.ru/index.php?page=book&id=83040
5. Кострикин, А.И. Введение в алгебру : учебник / А.И. Кострикин. - Москва: МЦНМО, 2009. - Ч. 1. Основы алгебры. 273 с. [Электронный ресурс] – Режим доступа: http://biblioclub.ru/index.php?page=book&id=63140.
6. Кадомцев, С.Б. Аналитическая геометрия и линейная алгебра / С.Б. Кадомцев. - 2-е изд., испр. и доп. - Москва: Физматлит, 2011. - 168 с. [Электронный ресурс]– Режим доступа: http://biblioclub.ru/index.php?page=book&id=69319.
7. Карасев, И.П. Теория функций комплексного переменного: учебное пособие / И.П. Карасев. - Москва: Физматлит, 2008. - 215 с. - ISBN 978-5-9221-0960-4; [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=68139.
8. Малышева, Н.Б. Функции комплексного переменного: учебник / Н.Б. Малышева, Э.Р. Розендорн. - Москва: Физматлит, 2010. - 168 с. - ISBN 978-5-9221-0977-2; [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=68367.
9. Треногин, В.А. Обыкновенные дифференциальные уравнения: учебник / В.А. Треногин. - Москва: Физматлит, 2009. - 312 с. - ISBN 978-5-9221-1063-1; [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=82614.
10. Асташова, И.В. Дифференциальные уравнения / И.В. Асташова, В.А. Никишкин. - Москва: Евразийский открытый институт, 2011. - Ч. 2. - 108 с. - ISBN 978-5-374-00487-8; [Электронный ресурс] – Режим доступа: http://biblioclub.ru/index.php?page=book&id=90342.
11. Треногин, В.А. Функциональный анализ: Учеб. для вузов. - М.: Физматлит, 2007. - 488 с.
12. Асташкин, С. В. Функциональный анализ : учеб. пособие для вузов. - Самара.: Самарский университет, 2009. - 44 с.
13. Ширяев, А.Н. Вероятность-1: Элементарная теория вероятностей. Математические основания. Предельные теоремы: учебник : в 2-х кн. / А.Н. Ширяев. - Изд. 4-е, перераб. и доп. - Москва : МЦНМО, 2007. - 552 с. - ISBN 978-5-94057-105-6; [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/index.php?page=book_red&id=63256.
14. Чистяков, В.П. Курс теории вероятностей [Текст]: [учеб. для вузов по направлениям подгот. и специальностям в обл. техники и технологии]. - М.: Дрофа, 2007. - 253 с.
15. Белов, А.А. Теория вероятностей и математическая статистика: учеб. для вузов. - Ростов н/Д.: Феникс, 2008. - 318 с.
16. Владимиров, В.С. Уравнения математической физики: учебник для вузов [с повыш. мат. подготовкой]. - М..: Физ. 1981. — 512 с.
17. Архитектура современных операционных систем [Электронный ресурс]: электрон. учеб.-метод. комплекс по дисциплине в LMS Moodle. - Самара, 2,013. - on-line.
18. Бабаш, А.В. Криптографические методы защиты информации. - Т. 1 . - 2016. Т. 1 . - 413 с.
19. Безопасность сетей ЭВМ [Электронный ресурс]: электрон. учеб.-метод. комплекс по дисциплине в LMS Moodle. - Самара, 2,012. - on-line.

20. Галатенко, В.А. Стандарты информационной безопасности [Текст]: курс лекций : учеб. пособие : [для вузов по специальностям в обл. информ. технологий]. - М.: ИНТУИТ. ру, 2006. - 263 с.
21. Девянин, П.Н. Модели безопасности компьютерных систем [Текст]: [учеб. пособие для вузов по специальностям 075200 "Компьютер. безопасность" и 075500 "Комплекс. обес. - М.: Academia, 2,005. - 143 с.
22. Еленев, Д. В. Компьютерные сети [Текст]: [учеб. пособие. - Самара: Изд-во СГАУ, 2010. - 78 с.
23. Защита информации [Текст]: учеб. пособие: [для вузов]. - М..: РИОР : ИНФРА-М, 2017. - 392 с.
24. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях. - М.: КУДИЦ-Образ, 2001. - 368с.
25. Крутов, А.Н. Методы программирования : учебное пособие [для студентов специальности 10.05.01 - Компьютерная безопасность]. - Самара.: Самарский университет, 2014. - 46 с.
26. Малюк, А.А. Введение в защиту информации в автоматизированных системах [Текст]: [учеб. пособие по специальностям в обл. информ. безопасности]. - М.: Горячая линия - Телеком, 2005. - 146 с.
27. Мельников, В.П. Методы и средства хранения и защиты компьютерной информации [Текст]: [учеб. пособие для вузов]. - Старый Оскол.: ТНТ, 2016. - 399 с.
28. Моисеев, А.И. Информационная безопасность распределенных информационных систем [Электронный ресурс]: [учеб. по специальности "Информ. безопасность автоматизир. сис. - Самара.: [Изд-во СГАУ], 2,013. - on-line
29. Основы криптографии [Текст]: учеб. пособие для вузов. - М.: Гелиос АРВ, 2005. - 480 с.
30. Основы организационного обеспечения информационной безопасности объектов информатизации [Текст]: [учеб. пособие]. - М.: Гелиос АРВ, 2005. - 186 с.
31. Основы программирования [Электронный ресурс]: метод. указания. - Самара, 2015. - on-line.
32. Пятибратов, А.П. Вычислительные системы, сети и телекоммуникации [Текст]: учеб. пособие для вузов. - М.: КНОРУС, 2019. - 372 с.
33. Родичев, Ю.А. Информационная безопасность: нормативно-правовые аспекты : учеб. пособие для вузов. - СПб.: Питер, 2008. - 272 с.
34. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности [Текст]: [учеб. пособие по направлению подгот. 10.00.00 "Информ. безопасность"]. - СПб. ; М. ; Екатеринбург: Питер, 2017. - 254 с.
35. Смарт, Н. Криптография: [Учебник для вузов] : Пер. с англ.. - М.: Техносфера, 2005. - 224с.
36. Соболева, Т.С. Дискретная математика: учебник для вузов. - М.: Академия, 2006. - 256 с.
37. Теоретические основы компьютерной безопасности: Учеб. пособ. для вузов. - М.: Радио и связь, 2000. - 192с.
38. Цветов, В.П. Дискретная математика: (Курс лекций), Ч. 1. Множества. - Самара.: Универс-групп, 2005. Ч. 1. - 63 с.
39. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей [Текст]: учеб. пособие. - М..: Форум : Инфра-М, 2,017. - 415 с.

5.3.2. Дополнительная литература

1. Тер-Крикоров, А.М. Курс математического анализа [Текст]: [учеб. пособие для вузов]. - М.: Лаб. знаний, 2017. - 672 с.
2. Горлач, Б.А. Математический анализ [Текст]: учеб. пособие. - СПб. ; М. ; Краснодар.: Лань, 2013. - 600 с.
3. Курош, А.Г. Лекции по общей алгебре / А.Г. Курош. - Москва: Гос. изд-во физико-математической лит., 1962. - 399 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=220855
4. Гантмахер, Ф.Р. Теория матриц / Ф.Р. Гантмахер. - 5-е изд. - Москва: Физматлит, 2010. - 560 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=83224
5. Алгебра и аналитическая геометрия в примерах и задачах : учебное пособие / Р.Ф. Ахвердиев, М.Г. Ахмадеев, Н.А. Газизуллин и др.; Федеральное агентство по образованию, ГОУ ВПО Казанский государственный технологический университет. - Казань: КГТУ, 2008. - 87 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=258942.
6. Шабат, Б.В. Введение в комплексный анализ [Текст]: учеб. пособие для мех.-мат. фак. ун-тов. - М.: Наука, 1969. - 576 с.
7. Геворкян, Э.А. Теория функций комплексной переменной: учебное пособие университет экономики, статистики и информатики, / Э.А. Геворкян, А.С. Фокст. - Москва: Московский государственный 2004. - 164 с.; [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=90747.
8. Федорюк, М.В. Обыкновенные дифференциальные уравнения [Текст]: [учеб. пособие для втузов]. - М.: URSS: Либроком, 2015. - 447 с.
9. Егоров, А.И. Теорема Коши и особые решения дифференциальных уравнений / А.И. Егоров. - Москва: Физматлит, 2008. - 254 с. - ISBN 978-5-9221-0942-0; [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=68444.
10. Садовничий, В.А. Теория операторов [Текст]: [учеб. по направлениям и специальностям физ.-мат. профиля]. - М.: Дрофа, Изд-во Моск. ун-та, 2004. – 381 с.
11. Севастьянов, Б.А. Курс теории вероятностей и математической статистики [Текст]: [для специальностей "Математика" и "Механика"]. - М.: Наука, 1982. - 255 с.
12. Боровков, А.А. Математическая статистика: учебник. - М.: Физматлит, 2007. - 704 с.
13. Гнеденко, Б.В. Курс теории вероятностей [Текст]: [учеб для мат. специальностей ун-тов]. - М.: URSS, Кн. дом "Либроком", 2011. - 485 с.
14. Сборник задач по уравнениям математической физики: учебное пособие / В.С. Владимиров, В.П. Михайлов, Т.В. Михайлова, М.И. Шабунин. - 4-е изд., перераб. и доп. - Москва: Физматлит, 2016. - 518 с.: граф. - Библиогр. в кн. - ISBN 978-5-9221-1692-3; [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=485543.
15. Буслаев, В.С. Вариационное исчисление: Учеб. пособ. - Л.: Изд-во ЛГУ, 1980. - 286с.
16. Численные методы. Сборник задач: учеб. пособие для вузов. - М.: Дрофа, 2007. - 144 с.
17. Турчак, Л.И. Основы численных методов: учебное пособие / Л.И. Турчак, П.В. Плотников. - 2-е изд., перераб. и доп. - Москва: Физматлит, 2002. - 304 с. - ISBN 5-9221-0153-6; [Электронный ресурс]. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=69329.
18. Автоматизированные системы контроля и управления РЭС [Электронный ресурс]: науч.-образоват. модуль в системе дистанц. обучения MOODLE. - Самара, 2012. - on-line.
19. Бачило, И.Л. Информационное право: Учебник для вузов: [спец. курс]. - М.: Высшее образование, Юрайт-Издат, 2009. - 454 с.

20. Бузов, Г.А. Защита от утечки информации по техническим каналам [Текст]: [учеб. пособие для экспертов системы Гостехкомиссии России]. - М.: Горячая линия - Телеком, 2005. - 414 с.
21. Владимирский, Б.М. Математика. Общий курс.: Учеб. для вузов. - М.: Лань, 2002. - 960с.
22. Вехов А.М. Компьютерные преступления: Способы совершения и методики расследования. - М.: Право и закон, 1996. – 182 с.
23. Волкова, Н.А. Элементы математики и статистики [Электронный ресурс]: учебное пособие / Н.А. Волкова, Н.Ю. Кропачева, Е.Г. Михайлова. — Электрон. дан. — Санкт-Петербург: Лань, 2018. — 128 с. — Режим доступа: https://e.lanbook.com/book/99207. — Загл. с экрана.
24. Гаврилов, М.В. Информатика и информационные технологии [Электронный ресурс]: учеб. для бакалавров : электрон. копия. - М.: Юрайт, 2013. - on-line.
25. Информационная безопасность и защита информации [Текст]: [учеб. пособие для вузов]. - Старый Оскол: ТНТ, 2015. - 383 с.
26. Ищейнов, В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие для вузов. - Москва: Форум, Инфра-М, 2014. - 255 с.
27. Казарин, О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О.В. Казарин, А.С. Забабурин. — М.: Издательство Юрайт, 2017. — 312 с. — (Серия : Специалист). — ISBN 978-5-9916-9043-0.
28. Корт, С.С. Теоретические основы защиты информации [Текст]: [учеб. пособие по группе специальностей в обл. информ. безопасности]. - М.: Гелиос АРВ, 2004. - 233 с.
29. Кузин, А.В. Базы данных: учеб. пособие для вузов. - М..: Академия, 2010. - 320 с.
30. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст]: [учеб. пособие для вузов по специальности 075400 - М.: Горячая линия - Телеком, 2004. - 280 с.
31. Меняев, М.Ф. Информационный менеджмент [Электронный ресурс]: учебник / М.Ф. Меняев. — Электрон. дан. — Москва: , 2017. — 301 с. — Режим доступа: https://e.lanbook.com/book/106285. — Загл. с экрана.
32. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. пособие для вузов. - СПб.: Питер, 2012. - 944 с
33. Основы информационной безопасности [Текст]: [учеб. пособие для вузов]. - Старый Оскол.: ТНТ, 2017. - 381 с.
34. Основы программирования [Электронный ресурс]: метод. указания. - Самара, 2015. - on-line.
35. Пшеничников, В.В. Языки и методы программирования. Курс лекций [Электронный ресурс]: электрон. учеб. пособие. - Самара, 2011. - on-line.
36. Робачевский, А.М. Операционная система UNIX [Текст]: [учеб. пособие для вузов]. - СПб.: БХВ-Петербург, 2,007. - 635 с
37. Родичев, Ю.А. Компьютерные сети: архитектура, технологии, защита [Текст]: учеб. пособие для вузов: [по специальностям 090103 "Орг. и технология защиты информ." и. - Самара.: Универс-групп, 2006. - 466 с
38. Родичев, Ю.А. Ч. 1; Компьютерные сети. Нормативно-правовые аспекты информационной безопасности [Текст]: учеб. пособие для вузов. - Самара: Изд-во "Универс групп", 2007. Ч. 1. - 343 с.

39. Рощупкин, В.Г. Методология и организация информационно-аналитической деятельности [Электронный ресурс]: [учеб. пособие]. - Самара: Изд-во "Самар. ун-т", 2015. - on-line.
40. Скиба, В.Ю. Руководство по защите от внутренних угроз информационной безопасности [Текст]. - СПб., М., Нижний Новгород.: Питер, Питер Пресс, 2008. - 318 с.
41. Торокин, А.А. Инженерно-техническая защита информации [Текст]: [учеб. пособие для вузов по специальностям в обл. информ. безопасности]. - М.: Гелиос АРВ, 2005. - 959 с.
42. Харрис, Д.М. Цифровая схемотехника и архитектура компьютера [Электронный ресурс] : [пер. с англ.]. - New York.: Elsevier. inc: Изд-во Morgan Kaufman, 2,013. - on-line.
43. Шатских, С.Я. Методы теории информации в криптологии: доп. главы теории вероятностей и мат. статистики для специальности "Компьютерная безопасность": [учеб. посо. - Самара: Универс групп, 2006. - 57 с.

6. ТРЕБОВАНИЯ К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ И ПОРЯДКУ ЕЕ ВЫПОЛНЕНИЯ

6.1 Требования к структуре, объему и содержанию выпускной квалификационной работы

Структурными элементами текста ВКР в соответствии со стандартом Самарского университета «Общие требования к учебным текстовым документам» являются:

– титульный лист ВКР (оформляется на бланке университета и служит обложкой ВКР);

– задание (оформляется на типовом бланке);

– содержание (включает введение, наименование всех разделов и подразделов (если имеются), заключение, список использованных источников, приложения (при наличии) с указанием номеров страниц, с которых начинаются эти структурные элементы ВКР);

– введение (содержит актуальность, цель, задачи, предмет и объект исследования, содержание проблемы, личный вклад автора в её решение, методология и избранные методы исследования, научная новизна, практическая значимость, область применения результатов);

– основная часть (определяется кафедрой, выдавшей задание в соответствии с ФГОС ВО;

– заключение (отражает выводы и результаты работы, полученный социально-экономический эффект, что осталось нерешённым, как нужно решать в дальнейшем при использовании результатов работы);

– список использованных источников (включает все использованные источники: книги, статьи из журналов и сборников, авторские свидетельства, государственные стандарты и прочие сведения, которые оформляются в соответствии с требованиями ГОСТ);

– приложения (оформляются при наличии материалов, которые не являются самой работой, но способствуют её обоснованности).

Структура и объем ВКР определяется научным руководителем в целях раскрытия темы. Качество и сроки выполнения этапов ВКР контролирует руководитель ВКР из числа работников университета. После завершения подготовки обучающимся ВКР руководитель ВКР представляет в университет на кафедру письменный отзыв о работе обучающегося в период подготовки ВКР.

6.2 Требования к оформлению выпускной квалификационной работы

Оформление ВКР осуществляется в соответствии со стандартом Самарского университета «Общие требования к учебным текстовым документам».

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, НЕОБХОДИМОГО ДЛЯ ПРОВЕДЕНИЯ ГИА

7.1. Описание материально-технической базы

Материально-техническая база, необходимая для подготовки к ГИА и проведения ГИА, обеспечена специальными помещениями – учебными аудиториями для проведения групповых и индивидуальных консультаций, проведения ГИА, а также помещениями для самостоятельной работы и помещениями для хранения и профилактического обслуживания учебного оборудования.

Контактная работа с руководителем ВКР и консультантом (консультантами) (при наличии) проходит в аудитории, оснащенной презентационной техникой (проектор, экран, компьютер/ноутбук), учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя.

Для самостоятельной работы обучающегося предоставляется компьютерный класс, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

При проведении ГИА используется презентационная техника (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентационные материалы).

Организовано асинхронное взаимодействие обучающегося и руководителя ВКР (консультантов при их наличии) с использованием электронной информационной образовательной среды университета через систему личных кабинетов обучающихся и преподавателей. Обучающийся размещает в личном кабинете ВКР, отзыв руководителя ВКР, рецензию на ВКР. Руководитель ВКР проверяет и верифицирует размещенные ВКР, отзыв и рецензию. После этого ВКР, отзыв и рецензия сохраняются в электронном портфолио обучающегося и в электронной библиотечной системе университета.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде организации (http://lib.ssau.ru/els). Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивает возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории университета, так и вне ее.

7.2 Перечень лицензионного программного обеспечения

Таблица 5. Перечень лицензионного программного обеспечения

№ п/п	Наименование	Тип и реквизиты ресурса
1.	Microsoft Windows Professional 7	Microsoft Open License №45936857 от 25.09.2009, Microsoft Open License №45980114 от 07.10.2009, Microsoft Open License №47598352 от 28.10.2010, Microsoft Open License №49037081 от 15.09.2011, Microsoft Open License №60511497 от 15.06.2012
2	Microsoft Office Professional 2007	Microsoft Open License №42482325 от 19.07.2007, Microsoft Open License №42738852 от 19.09.2007, Microsoft Open License

		№42755106 от 21.09.2007, Microsoft Open License №44370551 от 06.08.2008, Microsoft Open License №44571906 от 24.09.2008, Microsoft Open License №44804572 от 15.11.2008, Microsoft Open License №44938732 от 17.12.2008, Microsoft Open License №45936857 от 25.09.2009

7.3 Перечень свободно распространяемого программного обеспечения

1 Apache Open Office orgv.3
2 LibreOffice.
3 СПО Kali Linux.
4 Система виртуализации Virtual Box

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

8.1. Основная литература

1. Выпускная квалификационная работа [Текст]: метод. указания по направлению "Информ. безопасность". – Самара: Изд-во "Самар. ун-т", 2014. – 31 с.
2. Гречников, Ф.В. Основы научных исследований [Электронный ресурс]: [учеб. пособие по программам высш. проф. образования укрупн. группы специальностей и направлений 15. - Самара: Изд-во СГАУ, 2,015. - on-line
3. Оформление результатов научной работы [Электронный ресурс]. - 2,011. - on-line.
4. Экспериментальные методы исследований [Электронный ресурс]. - 2,011. - on-line.
5. Галатенко, В.А. Стандарты информационной безопасности [Текст]: курс лекций: учеб. пособие: [для вузов по специальностям в обл. информ. технологий]. – М.: ИНТУИТ. ру, 2006. – 263 с.
6. Защита информации [Текст]: учеб. пособие: [для вузов]. – М: РИОР: ИНФРА-М, 2017. – 392 с.
7. Моисеев, А.И. Информационная безопасность распределенных информационных систем [Электронный ресурс]: [учеб. по специальности "Информ. безопасность автоматизир. сис. – Самара: [Изд-во СГАУ], 2013. – on-line.
8. Родичев, Ю.А. Компьютерные сети: Нормативно-правовые аспекты информационной безопасности [Текст]: Учеб. пособие для вузов, Ч.1. – Самара: Универс-групп, 2007. Ч.1. – 344 с.
9. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности [Текст]: [учеб. пособие по направлению подгот. 10.00.00 "Информ. безопасность"]. – СПб.; М.; Екатеринбург: Питер, 2017. – 254 с.
10. Степанов, Е.А. Информационная безопасность и защита информации [Текст]: Учеб. пособие для вузов. – М.: Инфра-М, 2001. – 302с.
11. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей [Текст]: учеб. пособие. – М.: Форум: Инфра-М, 2017. – 415 с.

8.2. Дополнительная литература.

1. Введение в защиту информации [Текст]: [учеб. пособие для вузов по специальностям, не входящим в группу специальностей 075000 "Изучающий федер. компон. – М.: ФОРУМ, ИНФРА-М, 2004. – 127 с
2. Ищейнов, В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации [Текст]: учебное пособие для вузов. – Москва: Форум, Инфра-М, 2014. – 255 с.
3. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст]: [учеб. пособие для вузов по специальности 075400 "Ко. – М.: Горячая линия – Телеком, 2004. – 280 с.
4. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах [Текст]: учебное пособие для вузов. – Москва.: ИД Форум, Инфра-М, 2010. – 591 с.
5. Методология научных исследований [Электронный ресурс]: [метод. указания к курс. работе]. - Самара: Изд-во СГАУ, 2,014. - on-line.
6. Подготовка выпускных квалификационных работ [Электронный ресурс]: [метод. указания по прогр. высш. образования]. - Самара: Изд-во Самар. ун-та, 2,016. - on-line.
7. Шкляр, М.Ф. Основы научных исследований : учебное пособие / М.Ф. Шкляр. - 6-е изд. - Москва : Издательско-торговая корпорация «Дашков и К°», 2017. - 208 с. - [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=450782.
8. Самарский, А.А. Математическое моделирование / А.А. Самарский, А.П. Михайлов. - Москва : Физматлит, 2005. - 160 с. - ISBN 978-5-9221-0120-2; [Электронный ресурс]. – Режим доступа: //biblioclub.ru/index.php?page=book&id=68976.

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для подготовки к государственной итоговой аттестации

Таблица 6. Ресурсы информационно-телекоммуникационной сети «Интернет», необходимые для подготовки к ГИА

№ п/п	Наименование ресурса	Адрес	Тип доступа
1.	Сайт ФСТЭК	http://www.fstec.ru	Открытый ресурс
2	Сайт ФСБ	http://www.fsb.ru	Открытый ресурс
3.	Каталог на сервере университета с учебными материалами по курсу	\\jupiter4\Teach-Info\Yury A. Rodichev	Открытый ресурс
4.	Электронный фонд правовой и нормативно-технической документации	http://docs.cntd.ru/	Открытый ресурс
5	Сайт федерального агентства по техническому регулированию и метрологии (Росстандарт)	https://www.gost.ru/portal/gost/	Открытый ресурс
6.	Открытая электронная библиотека «Киберленинка»	http://cyberleninka.ru	Открытый ресурс
7.	Словари и энциклопедии онлайн	http://dic.academic.ru/	Открытый ресурс

8.4 Перечень информационных справочных систем и современных профессиональных баз данных, необходимых для подготовки к ГИА

Таблица 7. Информационные справочные системы, необходимые для подготовки к ГИА

№ п/п	Наименование ресурса	**Тип и реквизиты ресурса**
1.	СПС КонсультантПлюс	Договор № ЭК- 18/16 от 29.12.2016 Договор ЭК-69/17 от 13.12.2017
2.	Система интегрированного поиска EBSCO Discovery Service EBSCO Publishing	Договор № 799 от 06.06.2016 Договор № 800 от 08.06.2017

Таблица 8. Современные профессиональные базы данных, необходимые для подготовки к ГИА

№ п/п	Наименование ресурса	**Тип и реквизиты ресурса**
1.	Электронная библиотека диссертаций РГБ	Договор № 095/04/0324 от 11.10.2016 Договор № 095/04/0143 от 18.10.2017
2.	Научная электронная библиотека eLibrary.ru	Договор № SU-16-10/2017-1 от 24.10.2017

9. КРИТЕРИИ ОЦЕНКИ РЕЗУЛЬТАТОВ СДАЧИ ГОСУДАРСТВЕННОГО ЭКЗАМЕНА И ЗАЩИТЫ ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

Критерии оценки результатов сдачи государственного экзамена и защиты ВКР приведены в фонде оценочных средств для проведения ГИА (Приложение 2 к настоящей программе).

10. ПОРЯДОК ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ ДЛЯ ВЫПУСКНИКОВ ИЗ ЧИСЛА ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Для обучающихся из числа инвалидов ГИА проводится с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья (далее – индивидуальные особенности).

При проведении ГИА обеспечивается соблюдение следующих общих требований:

- проведение ГИА для инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при прохождении ГИА;
- 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 ГЭК);
- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении ГИА 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).

Все локальные нормативные акты Университета по вопросам проведения ГИА доводятся до сведения обучающихся инвалидов в доступной для них форме.

По письменному заявлению обучающегося инвалида продолжительность сдачи обучающимся инвалидом государственного аттестационного испытания может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность выступления обучающегося при защите ВКР – не более чем на 15 минут.

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья структурное подразделение обеспечивает выполнение следующих требований при проведении государственного аттестационного испытания:

а) для слепых:

- задания и иные материалы для сдачи государственного аттестационного испытания оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом;
- письменные задания выполняются обучающимися на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых, либо надиктовываются ассистенту;
- при необходимости обучающимся предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

б) для слабовидящих:

- задания и иные материалы для сдачи государственного аттестационного испытания (оформляются увеличенным шрифтом);
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования;
- по их желанию государственные аттестационные испытания проводятся в письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются обучающимися на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по их желанию государственные аттестационные испытания проводятся в устной форме.

Обучающийся из числа инвалидов не позднее чем за 3 месяца до начала проведения ГИА подает письменное заявление о необходимости создания для него специальных условий при проведении государственных аттестационных испытаний с указанием его индивидуальных особенностей в Центр инклюзивного образования Университета. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в Университете).

В заявлении обучающийся из числа инвалидов 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).

Приложение 1

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ
к программе государственной итоговой аттестации

Направление подготовки (специальность)	10.05.01 Компьютерная безопасность (уровень специалитета)
Профиль (направленность) образовательной программы	Информационно-аналитическая и техническая экспертиза компьютерных систем
Форма обучения, год набора	Очная, набор 2018

на 20__20__ уч. г.

В программу государственной итоговой аттестации вносятся следующие изменения:

1. _____
_____
2. _____
_____

Изменения в программе государственной итоговой аттестации рассмотрены и одобрены на заседании кафедры безопасности информационных систем

Протокол № ___ от «_ __ _»____ _____ 20__ г.

Заведующий
кафедрой безопасности информационных систем _____ М.Н. Осипов

Руководитель основной профессиональной образовательной программы высшего образования Информационно-аналитическая и техническая экспертиза компьютерных систем по специальности 10.05.01 Компьютерная безопасность

_____ М.Н. Осипов

Приложение 2

федеральное государственное автономное образовательное учреждение высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева»
(Самарский университет)

САМАРСКИЙ УНИВЕРСИТЕТ
SAMARA UNIVERSITY

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Код плана	100501.65-2020-О-ПП-5г06м-02
Направление подготовки (специальность)	10.05.01 Компьютерная безопасность
Профиль (направленность) образовательной программы	Информационно-аналитическая и техническая экспертиза компьютерных систем
Квалификация (степень)	Специалист по защите информации
Блок, в рамках которого проводится государственная итоговая аттестация	Б3
Институт (факультет)	Факультет математики
Кафедра	Безопасности информационных систем
Форма обучения	Очная, набор 2020
Курс, семестр	6 курс, 11 семестр
Форма (формы) государственной итоговой аттестации	Государственный экзамен Защита выпускной квалификационной работы,

Самара, 2020

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ, КОТОРЫМИ ДОЛЖНЫ ОВЛАДЕТЬ ОБУЧАЮЩИЕСЯ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Таблица 1. Компетенции, которыми должны овладеть обучающиеся в результате освоения образовательной программы, соотнесенные с формами ГИА

Код компетенции	**Содержание компетенции**	**Формы ГИА**
ОК-1	Способность использовать основы философских знаний для формирования мировоззренческой позиции	Государственный экзамен Защита ВКР
ОК-2	Способность использовать основы экономических знаний в различных сферах деятельности	Государственный экзамен Защита ВКР
ОК-3	Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма	Государственный экзамен Защита ВКР
ОК-4	Способность использовать основы правовых знаний в различных сферах деятельности	Государственный экзамен Защита ВКР
ОК-5	Способность 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 Защита ВКР
ОК-6	Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Государственный экзамен Защита ВКР
ОК-7	Способность 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 Защита ВКР
ОК-8	Способность к самоорганизации и самообразованию	Государственный экзамен Защита ВКР
ОК-9	Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	Государственный экзамен Защита ВКР
ОПК-1	Способность анализировать физические явления и процессы при решении профессиональных задач	Государственный экзамен Защита ВКР
ОПК-2	Способность 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 Защита ВКР

Код компетенции	Содержание компетенции	Формы ГИА
ОПК-3	Способность 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 Защита ВКР
ОПК-4	Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Государственный экзамен Защита ВКР
ОПК-5	Способность использовать нормативные правовые акты в своей профессиональной деятельности	Государственный экзамен Защита ВКР
ОПК-6	Способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций	Государственный экзамен Защита ВКР
ОПК-7	Способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Государственный экзамен Защита ВКР
ОПК-8	Способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Государственный экзамен Защита ВКР
ОПК-9	Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Государственный экзамен Защита ВКР
ОПК-10	Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Государственный экзамен Защита ВКР
ПК-1	Способность 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 Защита ВКР
ПК-2	Способность 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) Защита ВКР
ПК-3	Способность проводить анализ безопасности компьютерных систем на соответствие отече-	Государственный экзамен Защита ВКР

Код компетенции	Содержание компетенции	Формы ГИА
	ственным и зарубежным стандартам в области компьютерной безопасности	
ПК-4	Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Государственный экзамен Защита ВКР
ПК-5	Способность 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 Защита ВКР
ПК-6	Способность участвовать в разработке проектной и технической документации	Государственный экзамен Защита ВКР
ПК-7	Способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем	Государственный экзамен Защита ВКР
ПК-8	Способность участвовать в разработке подсистемы информационной безопасности компьютерной системы	Государственный экзамен Защита ВКР
ПК-9	Способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	Государственный экзамен Защита ВКР
ПК-10	Способность 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 Защита ВКР
ПК-11	Способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	Государственный экзамен Защита ВКР
ПК-12	Способность проводить инструментальный мониторинг защищенности компьютерных систем	Государственный экзамен Защита ВКР
ПК-13	Способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности	Государственный экзамен Защита ВКР
ПК-14	Способность организовать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Государственный экзамен Защита ВКР
ПК-15	Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной	Государственный экзамен Защита ВКР

Код компетенции	Содержание компетенции	Формы ГИА
	системы	
ПК-16	Способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующих работу по обеспечению информационной безопасности компьютерных систем	Государственный экзамен Защита ВКР
ПК-17	Способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	Государственный экзамен Защита ВКР
ПК-18	Способность 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 Защита ВКР
ПК-19	Способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Государственный экзамен Защита ВКР
ПК-20	Способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	Государственный экзамен Защита ВКР
ПСК-7.1	Способность использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов	Государственный экзамен Защита ВКР
ПСК-7.2	Способность проводить экспертизу вычислительной техники и носителей компьютерной информации	Государственный экзамен Защита ВКР
ПСК-7.3	Способность руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий	Государственный экзамен Защита ВКР
ПСК-7.4	Способность подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем	Государственный экзамен Защита ВКР
ПСК-7.5	Способность разрабатывать программное обеспечение, предназначенное для выявления следов компьютерных преступлений и инцидентов	Государственный экзамен Защита ВКР

2. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ, А ТАКЖЕ ШКАЛ ОЦЕНИВАНИЯ

2.1 Показатели и критерии оценивания сформированности компетенций при проведении государственного экзамена

Показателями оценивания сформированности компетенций при проведении государственного экзамена являются выполненные задания экзаменационного билета на государственном экзамене (таблица 2). Оценка ведется по 5-балльной шкале.

Таблица 2. Показатели оценивания сформированности компетенций при проведении государственного экзамена

Показатели оценки	**Коды компетенций**	**Удельный вес показателя**	**Отлично**	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
Ответ на 1 вопрос билета	ОК-1, ОПК-1, ОПК-2, ОПК-4, ОПК-7, ОПК-10, ПК-4, ПК-7, ПК-8, ПК-15, ПК-17, ПК-18, ПСК-7.5	0,5	5	4	3	2
Ответ на 2 вопрос билета	ОК-1, ОК-2, ОК-3, ОК-4, ОК-5, ОК-6, ОК-7, ОК-8, ОК-9, ОПК-1, ОПК-3, ОПК-4, ОПК-5, ОПК-6, ОПК-7, ОПК-8, ОПК-9, ОПК-10, ПК-1, ПК-2, ПК-3, ПК-5, ПК-6, ПК-7, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16, ПК-17, ПК-18, ПК-19, ПК-20, ПСК-7.1, ПСК-7.2, ПСК-7.3, ПСК-7.4, ПСК-7.5	0,5	5	4	3	2

Оценка результата государственного экзамена выполняется с использованием формулы:

$$P = \sum_{i=1}^{n} П_i * k_i$$

где $П_i$ – оценка каждого показателя государственного экзамена на основе критериев и шкалы интерпретации результатов оценивания компетенций (таблица), в баллах;
k_i – удельный вес каждого критерия;
P – округляется до целого в большую сторону.

Результаты сдачи государственного экзамена определяются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»

Шкала интерпретации результатов оценивания компетенций и критерии оценки результатов сдачи государственного экзамена приведена в таблице 3.

Таблица 3. Шкала интерпретации результатов оценивания компетенций на государственном экзамене

Итоговый результат (*P*)	**Критерии оценки результатов сдачи государственного экзамена**	**Оценка результатов государственного экзамена**
2	Уровень владения компетенциями для решения профессиональных задач недостаточен	Неудовлетворительно
3	Уровень владения компетенциями для решения профессиональных задач удовлетворителен	Удовлетворительно
4	Уровень владения компетенциями для решения профессиональных задач преимущественно высокий	Хорошо
5	Уровень владения компетенциями для решения профессиональных задач высокий	Отлично

2.2 Показатели и критерии оценивания сформированности компетенций при проведении защиты выпускной квалификационной работы

Оценивание ВКР осуществляется в два этапа:

1. Предварительное оценивание ВКР – осуществляется руководителем ВКР обучающегося (отзыв руководителя ВКР) и рецензентом (рецензия на ВКР).
2. Оценка результатов защиты ВКР членами ГЭК – итоговая оценка выставляется на основании результатов экспертной оценки членов ГЭК (Таблица 4).

Таблица 4. Показатели оценивания сформированности компетенций при проведении защиты выпускной квалификационной работы

Показатели оценки защиты ВКР	**Коды компетенций**	**Удельный вес показателя**	**Отлично**	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
1. Обоснованность проблемы, постановка цели, выделение основных задач, объекта и предмета исследования	ОК-1, ОК-2, ОК-4 ОПК-1	0,05	5	4	3	2
2. Уровень теоретической, научно-исследовательской и практической проработки проблемы	ОК-1, ОК-2, ОК-3, ОК-4, ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-6, ОПК-7, ОПК-8, ОПК-9, ОПК-10, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16, ПК-17, ПК-18, ПК-19, ПК-20, ПСК-7.1, ПСК-7.2, ПСК-7.3, ПСК-7.4, ПСК-7.5	0,2	5	4	3	2

3. Качество анализа проблемы, наличие и качество вносимых предложений по совершенствованию деятельности исследуемой организации, оценка эффективности рекомендаций	ОК-1, ОК-2, ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-6, ОПК-7, ОПК-8, ОПК-9, ОПК-10, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16, ПК-17, ПК-18, ПК-19, ПК-20, ПСК-7.1, ПСК-7.2, ПСК-7.3, ПСК-7.4, ПСК-7.5	0,3	5	4	3	2
4. Степень самостоятельности исследования	ОК-8, ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-6, ОПК-7, ОПК-8, ОПК-9, ОПК-10, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16, ПК-17, ПК-18, ПК-19, ПК-20, ПСК-7.1, ПСК-7.2, ПСК-7.3, ПСК-7.4, ПСК-7.5	0,2	5	4	3	2
5. Навыки публичной дискуссии, защиты собственных научных идей, предложений и рекомендаций	ОК-1, ОК-2, ОК-3, ОК-4, ОК-7	0,1	5	4	3	2
6. Общий уровень культуры общения с аудиторией	ОК-1, ОК-2, ОК-3, ОК-4, ОК-5, ОК-6, ОК-7, ОК-9	0,05	5	4	3	2
7. Полнота и точность ответов на вопросы	ОК-2, ОК-3, ОК-4, ОК-5, ОК-6, ОК-7	0,1	5	4	3	2

Каждый критерий оценивается по 5-балльной шкале. Оценка результата ВКР выполняется с использованием формулы:

$$P = \sum_{i=1}^{n} \Pi_i * k_i,$$

где $П_i$ – оценка каждого критерия ВКР, в баллах;

k_i – удельный вес каждого критерия;

P – округляется до целого в большую сторону.

Результаты защиты ВКР определяются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Шкала интерпретации результатов оценивания компетенций и критерии оценки результатов защиты ВКР приведена в таблице 5.

Таблица 5. Шкала интерпретации результатов оценивания компетенций на защите ВКР

Итоговый результат (*P*)	**Критерии оценки результатов защиты ВКР**	**Оценка результатов защиты ВКР и ГИА**
2	Уровень владения компетенциями для решения профессиональных задач недостаточен: значительная часть результатов выполнения ВКР, ответы на вопросы членов ГЭК содержат ошибки, характер которых указывает на недостаточный уровень владения выпускником знаниями, умениями, навыками и (или) опытом, необходимыми для решения профессиональных задач.	Неудовлетворительно
3	Уровень владения компетенциями для решения профессиональных задач удовлетворителен: некоторые результаты выполнения ВКР, ответы на вопросы членов ГЭК содержат ошибки, характер которых указывает на посредственный уровень владения выпускником необходимыми знаниями, умениями, навыками и (или) опытом, но при этом позволяет сделать вывод о готовности выпускника решать типовые профессиональные задачи в стандартных ситуациях.	Удовлетворительно
4	Уровень владения компетенциями для решения профессиональных задач преимущественно высокий: некоторые результаты выполнения ВКР, ответы на вопросы членов ГЭК содержат незначительные ошибки и технические погрешности, характер которых указывает на преимущественно высокий уровень владения выпускником необходимыми знаниями, умениями, навыками и (или) опытом и позволяет сделать вывод о готовности выпускника решать типовые и ситуативные профессиональные задачи.	Хорошо
5	Уровень владения компетенциями для решения профессиональных задач высокий: результаты выполнения ВКР, ответы на вопросы членов ГЭК не содержат ошибок и технических погрешностей, указывают на высокий уровень владения выпускником необходимыми знаниями, умениями, навыками и (или) опытом и позволяют сделать вывод о готовности выпускника решать профессиональные задачи повышенного уровня сложности, а также способности разрабатывать новые решения.	Отлично

3. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕДЛЯ ОЦЕНКИ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

3.1 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы, на государственном экзамене

Таблица 6. Содержание заданий экзаменационного билета на государственном экзамене

Номер задания в билете	**Список вопросов**	**Коды компетенций**
1	1. Непрерывность действительных функций одной действительной переменной. Классификация точек разрыва. Свойства функций непрерывных на отрезке. Доказательство теоремы о промежуточном значении непрерывной функции. 2. Дифференцируемость функций одной и нескольких действительных переменных. Дифференциал функции. Достаточные условия дифференцируемости (без доказательства). Основные теоремы дифференциального исчисления функций одной переменной: теорема Ферма (с доказательством), теоремы Роля, Лагранжа, Коши (без доказательства). 3. Вывод формулы Тейлора для функций одной действительной переменной. Экстремумы функций одной переменной. Достаточное условие существования экстремума (с доказательством). 4. Абсолютно и условно сходящиеся числовые ряды: признаки сравнения и Даламбера (с доказательством), признаки Коши и Лейбница (без доказательства.) 5. Степенные ряды: теорема Абеля (без доказательства). Область и радиус сходимости степенного ряда. Ряды Тейлора и Маклорена. Достаточное условие разложимости функции в ряд Тейлора (с доказательством). 6. Первообразная и неопределенный интеграл. Определенный интеграл и его свойства. Существование первообразной для непрерывной функции (без доказательства). Интеграл с переменным верхним пределом, формула Ньютона-Лейбница (с доказательством). 7. Ряды Фурье. Признак Дини поточечной сходимости рядов Фурье (с доказательством). 8. Матрицы и операции над ними. Определители матриц и их свойства. Ранг матрицы. Критерий обратимости матриц (с доказательством). Способы вычисления обратной матрицы. 9. Системы линейных уравнений. Критерий Кронекера–Капелли (с доказательством). Теорема о структуре общего решения системы линейных уравнений (без доказательства). 10. Кольцо вычетов. Сравнения и их основные свойства. Малая теорема Ферма (с доказательством). 11. Кольцо многочленов. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. 12. Группы и их основные свойства. Примеры: циклические группы, конечные абелевые группы. Смежные классы по подгруппе. Теорема Лагранжа (с доказательством). 13. Векторные пространства их базисы и размерность. Координаты векторов в базисе и их изменение при переходе к другому базису. 14. Линейные преобразования векторного пространства и их матрицы. Характеристический многочлен линейного преобразования.	ОК-1 ОПК-1 ОПК-2 ОПК-4 ОПК-7 ОПК-10 ПК-4 ПК-7 ПК-8 ПК-15 ПК-17 ПК-18 ПСК-7.5

Номер задания в билете	Список вопросов	Коды компетенций
	Собственные значения и собственные векторы. 15. Квадратичные формы, их матрицы и ранг. Эквивалентность квадратичных форм, приведение к каноническому виду (с доказательством). Положительно определенные квадратичные формы, критерий Сильвестра (без доказательства). 16. Конечные поля. Характеристика поля. Построение конечного поля с заданным числом элементов. 17. Вероятностное пространство. Аксиоматика А.Н. Колмогорова. Свойства вероятностной меры. Классическое определение вероятности. 18. Условные вероятности. Независимость событий. Формула полной вероятности и формула Байеса. 19. Случайные величины. Функции распределения случайных величин и их свойства. Плотности распределения. Типовые распределения: биномиальное, пуассоновское, равномерное, гауссовское (нормальное). Многомерные функции распределения. Многомерное нормальное Распределение. Независимые случайные величины. 20. Определение математического ожидания случайной величины, как интеграла Лебега по вероятностной мере. Формулы вычисления математических ожидания для дискретных и абсолютно непрерывных случайных величин. Дисперсия случайной величины и ее свойства. Коэффициент ковариации случайных величин. Вычисление математических ожиданий и дисперсий случайных величин имеющих типовые распределения. 21. Неравенство П.Л. Чебышева (с доказательством). Закон больших чисел в форме Чебышева (с доказательством). 22. Определение характеристических функций случайных величин. Вычисление характеристических функций случайных величин имеющих типовые распределения. Свойства характеристических функций (без доказательства). Метод характеристических функций в доказательстве предельных теорем. Центральная предельная теорема для независимых одинаково распределенных случайных величин с ограниченной дисперсией (с доказательством). Следствие: теорема Муавра-Лапласа. 23. Дифференцируемость функции комплексного переменного. Вывод условий Коши-Римана. 24. Интеграл от функции комплексного переменного. Теорема Коши об интеграле от аналитической функции по замкнутому контуру (с доказательством). Интегральная формула Коши (с доказательством). 25. Основные типы дифференциальных уравнений первого порядка и методы их решения. Теорема существования и единственности решения дифференциального уравнения первого порядка (без доказательства). 26. Линейные дифференциальные уравнения n-го порядка, структура общего решения (без доказательства). Решение линейных дифференциальных уравнений n-го порядка с постоянными коэффициентами. 27. Алгебра множеств и отношений. Представление алгебр множеств и отношений матричными алгебрами.	

Номер задания в билете	Список вопросов	Коды компетенций
	28. Функциональные отношения. Отношения эквивалентности и порядка на конечных множествах, свойства их матриц. 29. Универсальные алгебры с конечным носителем. Представление операций многомерными двоичными массивами. 30. Булевы функции. Представление булевых функций формулами алгебры. 31. Исчисления высказываний и предикатов, их полнота и непротиворечивость. 32. Мера количества информации. Энтропия и ее свойства.	
2	1. Теорема Шеннона о пропускной способности канала связи. 2. Линейные блоковые коды. Корректирующие свойства кодов. Код Хемминга. 3. Определение циклического кода. Сверточный код. Алгоритм Витерби. 4. Виды атак в IP сетях. Причины уязвимости IP сетей. 5. Модель информационной безопасности систем. Типовые виды угроз безопасности. 6. Классификация способов и средств защиты информации в сетях. 7. Защита от вирусов. 8. Стандартные методы защиты сетей, МСЭ. Защита доверительной сети, VPN. 9. Требования к системе безопасности сетей. Принципы построения системы обеспечения безопасности корпоративной сети. 10. Понятие базы данных и СУБД. Основные функции СУБД. Архитектура многопользовательских СУБД 11. Базы данных. Реляционная модель и нормализация. 12. Алгоритмы на графах. Алгоритм Крускала. Алгоритм Дейкстры. Оценка сложности. 13. Алгоритмы поиска в последовательно организованных файлах. Оценка трудоемкости. 14. Алгоритмы поиска в деревьях. 15. Основные понятия защиты информации. Построение защищенной автоматизированной системы. 16. Угрозы безопасности информации. Понятие политики безопасности. 17. Модели системы безопасности, примеры моделей. 18. Основные положения Руководящих документов ФСТЭК в области защиты информации. 19. Основное содержание ГОСТ в области защиты информации. 20. Криптография и криптоанализ. Конфиденциальность, целостность, имитостойкость. Теоретическая и практическая стойкость шифра. 21. Классификация криптографических систем. Шифры простой и сложной замены, перестановки, гаммирования. 22. Криптосистемы с секретным ключом. Поточные криптосистемы. Шифрование методом гаммирования. 23. Криптосистемы с секретным ключом. Блочные шифры. Сеть Фейстеля. Стандарт шифрования DES. Российский стандарт шифрования ГОСТ 28147-89. Основные режимы работы блочных шифров. 24. Криптосистемы с открытым ключом. Односторонние функции,	ОК-1 ОК-2 ОК-3 ОК-4 ОК-5 ОК-6 ОК-7 ОК-8 ОК-9 ОПК-1 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-7 ОПК-8 ОПК-9 ОПК-10 ПК-1 ПК-2 ПК-3 ПК-5 ПК-6 ПК-7 ПК-9 ПК-10 ПК-11 ПК-12 ПК-13 ПК-14 ПК-15 ПК-16 ПК-17 ПК-18 ПК-19 ПК-20 ПСК-7.1 ПСК-7.2 ПСК-7.3 ПСК-7.4 ПСК-7.5

Номер задания в билете	Список вопросов	Коды компетенций
	односторонние функции с секретом. Криптосистема RSA. Криптосистема Эль Гамаля. 25. Криптографические хэш-функции. Однонаправленные хэш-функции. Алгоритм безопасного хеширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции ГОСТ Р 34.11-94. 26. Электронная подпись. Схемы ЭП 27. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ. 28. Правовые основы защиты информации с использованием технических средств. 29. Организация и обеспечение режима секретности. 30. Лицензирование и сертификация в области защиты информации. 31. Проблемы компьютерной безопасности на современном этапе. 32. Экономическая эффективность объектов информационной безопасности. 33. Основные этапы и закономерности исторического развития России, история развития информационной безопасности. 34. Социальная значимость профессии в сфере информационной безопасности. Ее роль в жизни современного общества. 35. Основные методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности в области компьютерной безопасности. 36. Основные приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций	

3.2 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы на защите ВКР

3.2.1 Примерный перечень тем ВКР

1. Разработка электронной подписи, свободной от потайного канала.

2. Формирование ложной топологии сети с целью сокрытия информационных направлений.

3. Использование аннигиляторов булевых функций при криптоанализе поточных шифров.

4. Исследование методов защиты информации в мобильных системах.

5. Автоматизация процесса создания инфраструктуры обманных систем в корпоративной сети.

7. Способ обнаружения атак типа «инъекции» на WEB-приложения на основе анализа аномалий в его ответах.

8. Разработка криптографического протокола тайного электронного голосования.

9. Применение алгебраического метода для криптоанализа блочных шифров.

10. Генерация гаммы на основе хаотических отображений.

11. Корреляция и перепутывание фотонов с орбитальным угловым моментом в схемах квантовой коммуникации.

12. Эллиптические кривые специального вида.

13. Коды по алгебраическим кривым.

14. Применение параметрических семейств архимедовых копул при анализе сетевого трафика в ON/OFF модели.

15. Моделирование и анализ сетевого трафика с использованием MMPP методом 2-копул.

16. Быстрые корреляционные атаки.

17. Методы стеганографии для звуковых и видеоданных.

18. Сетевая стеганография для защиты открытых каналов связи.

19. Разработка среды автоматизированного тестирования WEB-сервисов на уязвимость.

20. Функциональное моделирование и алгоритм проактивной защиты в информационных системах.

21. Реализация и сравнительный анализ криптосистем RSA и Полига-Хеллмана.

22. Идентификация пользователя по его поведению в сети.

23. Разработка электронной подписи, свободной от скрытого канала, на основе алгоритма стохастической аутентификации.

24. Реализация защищенной социальной сети.

25. Разработка защищенной CRM системы.

26. Создание защищенного мобильного приложения с подключением к внешней базе данных криптоконтейнеров.

27. Криптографические методы защиты облачных вычислений.

28. Акустические сигналы и методы обработки. Дистанционные методы снятия акустических сигналов.

29. Построение сетевой IDS на платформе Linux с использованием NFQUEUE.

30. Проектирование и разработка Web-фильтра для обеспечения контроля доступа к сетевым ресурсам.

31. Анализ способа оптимизации дифференциального криптоанализа.

32. Исследование возможности дифференциального криптоанализа с использованием адаптивных технологий.

33. Исследование возможности линейного криптоанализа с использованием адаптивных технологий.

34. Способ оптимизации криптоанализа эвристическими алгоритмами.

3.2.2 Перечень примерных вопросов на защите ВКР

Таблица 7. Перечень примерных вопросов на защите ВКР

Код и наименование проверяемой компетенции	**Примерные вопросы**
Способность использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1)	1.Выделите основные проблемы информационной безопасности, в целом, и компьютерной безопасности, в частности, в эпоху всемирной глобализации? 2.К каким общим закономерностям относятся процессы, выявленные вами в ходе анализа предмета ВКР?
Способность использовать основы экономических знаний в различных сферах деятельности (ОК-2)	1. Каковы результаты расчета совокупной стоимости владения объектом, исследуемым в ВКР? 2. Производилась ли оценка рисков инфор-

	мационной безопасности объекта, исследуемого в ВКР?
Способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3)	1.Приведите примеры основных этапов развития информационной безопасности в России. 2. Каково место и роль России в современном мире?
Способность использовать основы правовых знаний в различных сферах деятельности (ОК-4)	1. Укажите нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа, которые были учтены при вводе в эксплуатацию объекта информатизации, предложенного в ВКР? 2. Какими электронными ресурсами, содержащих базы нормативных документов по информационной безопасности, Вы пользовались при выполнении ВКР?
Способность 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 (ОК-5)	1. Охарактеризуйте социальную значимость своей будущей профессии, ее роль в обществе? 2. Как в сфере информационной безопасности реализуется защита интересов личности, общества и государства?
Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6)	1. Легко ли вы установили контакт с научным руководителем в процессе преддипломной практики? 2. Какие методы управления используются при организации деятельности малых коллективов.
Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7)	1.Приведите примеры ведущих отечественных и зарубежных авторов и изданий, которые были использованы при проведении исследования. 2.Какие зарубежные научные издания были использованы при проведении исследования? 3. Какие из источников на иностранных языках изучены в ходе подготовки ВКР?
Способность к самоорганизации и самообразованию (ОК-8)	1.Какие методы и средства вы применили при испытании средств обеспечения информационной безопасности, не прибегая к помощи научного руководителя ВКР? 2. Какие источники литературы вы подобрали самостоятельно?
Способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9)	1. Какие физические упражнения вы использовали в процессе проведения исследования для обеспечения полноценной деятельности? 2. Какими методами и средствами физической культуры вы снимали нагрузку после работы на ЭВМ?
Способность анализировать физические явления и процессы при решении профессиональных задач	1.Какие законы классических и квантовых физических явлений и процессов были ис-

(ОПК-1)	пользованы при исследовании защищенности объекта, рассматриваемого в ВКР? 2. Обоснуйте выбранные технические средства обработки результатов эксперимента. 3.Обоснуйте выбор методов и средств решения задач, поставленных в вашей работе.
Способность 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 (ОПК-2)	1.Какие методы математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов были использованы при исследовании защищенности объекта, рассматриваемого в ВКР? 2. Какие методы теории вероятностей, математической статистики, теории информации, теоретико-числовых методов 3. Обоснуйте выбранные технические средства обработки результатов эксперимента.
Способность 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 (ОПК-3)	1. Выполните классификацию защищаемой информации по видам тайн 2. С информацией каких степеней классификации вы работали в процессе выполнения ВКР? 3. Произведите оценку угроз информационной безопасности для объекта информатизации, рассматриваемого в ВКР
Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4)	1. Какие физические и математические методы были использованы при выполнении экспериментальных исследований в ходе выполнения ВКР? 2. Какие технические и программные средства были использованы при выполнении экспериментальных исследований в ходе выполнения ВКР?
Способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5)	1. Какие нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа были использованы вами в ВКР? 2. Была ли разработана нормативно-правовая документация по вводу в эксплуатацию систем и средств обеспечения информационной безопасности, рассматриваемых в ВКР?
Способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-6)	1. Владеете ли вы приемами оказания первой помощи пострадавшим в ЧС и экстремальных ситуациях на объектах информатизации? 2. Какие первоочередные организационные меры необходимо применить в условиях чрезвычайных ситуаций на предприятии?
Способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	1. Насколько вы учли современные тенденции развития информатики и вычислительной техники, компьютерных технологий в ВКР при выборе программных средств общего и специального назначения?

(ОПК-7)	2. Какие новейшие программные средства были использованы при выполнении ВКР?
Способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8)	1. Какие языки и системы программирования, инструментальные средства были использованы для решения прикладных задач в ВКР? 2. Проходили ли тестирование и отладку программные средства, разработанные в ВКР?
Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9)	1. Были ли разработаны модели угроз и модели нарушителя безопасности компьютерных систем, исследуемых в ВКР? 2. Была ли разработана политика управления доступом и информационными потоками в компьютерных системах, исследуемых в ВКР? 3. Какими способами моделирования безопасности компьютерных систем вы овладели в ходе выполнения ВКР?
Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ОПК-10)	1. Какие алгоритмы и программы были применены вами в решении поставленных задач в ВКР? 2. Проведите оценку вычислительной сложности алгоритма, предложенного в ВКР?
Способность 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 (ПК-1)	1. Какие информационные ресурсы были использованы при подборе отечественных и зарубежных источников по проблемам компьютерной безопасности? 2. Какие нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации были использованы вами в ВКР?
Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований (ПК-2)	1. Какие теоретические и экспериментальные методы и средства научных исследований были использованы вами в ВКР? 2. Назовите основные этапы проведенного научного исследования в ВКР? 3. Был ли составлен отчет по результатам проведенного научного исследования в ВКР?
Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности (ПК-3)	1. Сформулируйте основные требования информационной безопасности при эксплуатации компьютерной системы и технических средств защиты информации, рассматриваемых в ВКР? 2. Был ли проведен анализа безопасности компьютерных систем, рассматриваемых в ВКР, на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности систем и средств обеспечения информационной безопасности?
Способность проводить анализ и участвовать в разработке математических моделей безопасности	1. Какие математические методы в решении прикладных задач были использованы вами

компьютерных систем (ПК-4)	в ВКР? 2. Была ли составлена математические модели безопасности компьютерной системы, рассматриваемой в ВКР?
Способность 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 (ПК-5)	1. В разработке каких программно-аппаратных средств защиты информации вы участвовали в ходе выполнения ВКР? 2. . В обслуживании (обновлении, настройки) какого программного обеспечения, антивирусных и криптографических средств защиты информации вы участвовали в ходе выполнения ВКР?
Способность участвовать в разработке проектной и технической документации (ПК-6)	1. Какие проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности, были разработаны в ВКР? 2. На основе каких нормативно-правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации законодательства Российской Федерации были разработаны проекты локальных правовых актов?
Способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем (ПК-7)	1. Был ли проведен анализ компьютерной системы с целью определения уровня защищенности и доверия? 2. Насколько эффективны предложенные в ВКР программно-аппаратные средства защиты информации компьютерных систем по сравнению с аналогами?
Способность участвовать в разработке подсистемы информационной безопасности компьютерной системы (ПК-8)	1. Какие методы анализа защищенности компьютерных систем и подсистем были использованы вами в ВКР? 2. Была ли разработана подсистемы информационной безопасности компьютерной системы в процессе выполнения ВКР?
Способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы (ПК-9)	1. Какие инструментальные средства проведения мониторинга защищенности компьютерных систем были использованы вами в ВКР? 2. Перечислите основные нормативно-правовые акты в области защиты информации, которые были применены при аттестации компьютерных систем в процессе выполнения ВКР?
Способность 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 (ПК-10)	1. Какие методы анализа защищенности компьютерных систем и сетей были применены в ВКР? 2. Оцените эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах исследуемого объекта
Способность участвовать в проведении экспери-	1. Какие инструментальные средства приме-

ментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации (ПК-11)	нялись в ходе проведения сертификационных испытаний средств защиты информации? 2. Подготовлен ли аналитический отчет по проведенным сертификационным испытаниям средств защиты информации?
Способность проводить инструментальный мониторинг защищенности компьютерных систем (ПК-12)	1. Какой уровень защищенности исследуемой компьютерной системы? 2. Подготовлен ли аналитический отчет по результатам проведенного анализа защищенности компьютерных систем? 3. Произведено ли сравнение эффективности защищенности исследуемых компьютерных систем?
Способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-13)	1. Проведите анализ эффективности управленческих решений в работе коллектива при выполнении ВКР? 2. Какие изменения вы бы внесли в работу коллектива при выполнении ВКР?
Способность организовать работы по выполнению режима защиты информации, в том числе ограниченного доступа (ПК-14)	1. Произведите классификацию угроз информационной безопасности для данного объекта информатизации 2. Была ли выполнена качественная оценка угроз информационной безопасности для данного объекта информатизации? 3. Какие организационно-правовые меры в области обеспечения информационной безопасности были вами предложены?
Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы (ПК-15)	1. Какие правовые нормативные акты и нормативные методические документы ФСБ России, ФСТЭК России по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности компьютерных систем были применены в ходе выполнения ВКР? 2. Какие предложения по совершенствованию системы управления информационной безопасностью компьютерной системы объекта были разработаны в ходе выполнения ВКР?
Способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующих работу по обеспечению информационной безопасности компьютерных систем (ПК-16)	1. Какие проекты локальных правовых актов, инструкций, организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, были разработаны в процессе выполнения ВКР? 2. Какие отечественные и зарубежные стандарты в области защиты информации были использованы при разработке проектов нормативных правовых актов и методических материалов?
Способность производить установку, наладку, тестирование и обслуживание современного общего	1. Была ли произведена установка, наладка, тестирование и обслуживание специального

и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение (ПК-17)	программного обеспечения исследуемого объекта, включая операционные системы, системы управления базами данных и сетевое программное обеспечение в процессе выполнения ВКР? 2. Какие сертифицированные средства и программные продукты используются в системах защиты информации?
Способность 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-18)	1. Была ли произведена установка, наладка, тестирование и обслуживание программно-аппаратных средств обеспечения информационной безопасности компьютерных систем исследуемого объекта? 2. Использовались ли в процессе выполнения ВКР сканеры безопасности при анализе защищенности компьютерных систем?
Способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации (ПК-19)	1. Какие нормативно-правовые акты, методические документы, национальные стандарты на соответствие требованиям безопасности информации и техническим условиям технических средств защиты информации были учтены при проверке исследуемого объекта? 2. Какие программы, методики были разработаны при проведении испытания защищенных технических средств обработки информации на соответствие требованиям безопасности информации и техническим условиям?
Способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций (ПК-20)	1. Какие методы анализа и инструментальные средства применялись при проведении мониторинга защищенности компьютерной системы? 2. Какие навыки восстановления работоспособности средств защиты информации вы приобрели в процессе выполнения ВКР?
Способность использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов (ПСК-7.1)	1. Назовите основные этапы и методы проведения расследования компьютерных преступлений, правонарушений и инцидентов? 2. Какие нормативно-правовые требования необходимо выполнять при сборе и обращении с доказательными данными? 3. Какие средства поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов были использованы в ходе выполнения ВКР??
Способность проводить экспертизу вычислительной техники и носителей компьютерной информации (ПСК-7.2)	1. Назовите основные типы экспертиз вычислительной техники и носителей компьютерной информации? 2. Какие инструментальные средства проведения экспертиз вычислительной техники и носителей компьютерной информации были

	использованы в ходе выполнения ВКР?
Способность руководствоваться в своей работе законодательной базой и требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий (ПСК-7.3)	1. Требованиями каких нормативно-правовых документов следует руководствоваться при проведении судебной компьютерно-технической экспертизы? 2. По каким критериям оценивается компетентность привлекаемого эксперта при проведении следственных и судебных действий?
Способность подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем (ПСК-7.4)	1. Какие методики использовалась при проведении работ по информационно-аналитической и технической экспертизе компьютерных систем? 2. Обоснуйте выводы, сделанные в экспертном заключении по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем, выполненной в ВКР?
Способность разрабатывать программное обеспечение, предназначенное для выявления следов компьютерных преступлений и инцидентов (ПСК-7.5)	1. Какие алгоритмы доступа, обработки и хранения данных, связанных со следами компьютерных преступлений и инцидентов были разработаны и программно реализованы в ВКР? 2. Какие специализированные утилиты операционных систем вы применяли при разработке программного обеспечения, предназначенного для выявления следов компьютерных преступлений и инцидентов 3. Владеете ли вы языком сценариев оболочки командной строки?

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4.1. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы на государственном экзамене

Специалист института за 3 рабочих дня до начала государственного экзамена передает секретарю ГЭК следующие документы:

– зачетные книжки обучающихся;

– приказ об утверждении составов ГЭК для проведения ГИА и апелляционных комиссий по результатам ГИА (копия);

– распоряжение директора института об утверждении расписания государственных аттестационных испытаний (копия);

– программу ГИА (копия);

– распоряжения директора института о допуске обучающихся к ГИА (копия);

– заявления от обучающийся из числа инвалидов о необходимости (отсутствие необходимости) присутствия ассистента на государственном аттестационном испытании, о необходимости (отсутствие необходимости) увеличения продолжительности сдачи государственного аттестационного испытания по отношению к установленной

продолжительности (для каждого государственного аттестационного испытания (копии, при наличии).

– экзаменационные ведомости по приему государственного аттестационного испытания.

На основании представленных документов секретарь ГЭК готовит:

– бланки протоколов ГЭК по приему государственного экзамена;

– бланки экзаменационных листов для подготовки ответа обучающимися на государственном экзамене;

– бланки оценочных листов для членов ГЭК.

Государственный экзамен по экзаменационным билетам, которые готовит руководитель ОПОП ВО (или заведующий кафедрой) в соответствии с программой государственного экзамена и утверждает директор института.

Билеты государственного экзамена обновляются 1 раз в год, хранятся на выпускающей кафедре**.**

Секретарь ГЭК непосредственно на государственном экзамене выдает обучающимся экзаменационные билеты и экзаменационные листы для подготовки ответа обучающимися при проведении государственного экзамена.

Для подготовки ответа обучающемуся выделяется не менее 45 минут.

На основании письменного заявления обучающегося инвалида продолжительность сдачи обучающимся инвалидом государственного экзамена должна быть увеличена по отношению к установленной продолжительности его сдачи:

В случае обнаружения у выпускника после получения им экзаменационного билета учебных пособий, методических материалов, учебной и иной литературы (за исключением разрешенных для использования на государственном экзамене), конспектов, независимо от типа носителя информации, а также любых технических средств и средств передачи информации, либо использования им подсказки, вне зависимости от того, были ли использованы указанные материалы и (или) средства в подготовке к ответу на государственном экзамене, комиссия изымает до окончания государственного экзамена указанные материалы и (или) средства с указанием соответствующих сведений в протоколе заседания ГЭК и принимает решение об оценке знаний такого выпускника «неудовлетворительно».

Государственный экзамен проводится в форме открытых заседаний ГЭК с участием не менее двух третей от числа лиц, входящих в состав ГЭК. Заседания ГЭК проводятся председателями ГЭК.

Заседание ГЭК по приему государственного экзамена проводится согласно утвержденному расписанию ГИА.

Решения ГЭК принимаются простым большинством голосов от числа лиц, входящих в состав ГЭК и участвующих в заседании. При равном числе голосов председатель ГЭК обладает правом решающего голоса.

Результаты государственного экзамена объявляются в день его проведения.

Оценка государственного экзамена проставляется в зачетную книжку обучающегося, в экзаменационную ведомость по приему государственного экзамена и в протокол заседания ГЭК по приему государственного экзамена.

По окончанию заседания ГЭК все документы передаются секретарем ГЭК специалисту института для организации хранения.

Обучающийся, не прошедший государственный экзамен по уважительной причине, допускается к защите ВКР.

Обучающиеся, не прошедшие государственный экзамен в связи с неявкой на государственное аттестационное испытание по неуважительной причине или в связи с получением оценки «неудовлетворительно», а также обучающиеся из числа инвалидов, не прошедшие государственное аттестационное испытание в установленный для них срок (в связи с неявкой на государственное аттестационное испытание или получением оценки «неудовлетворительно»), отчисляются из университета с выдачей справки об обучении как не

выполнившие обязанностей по добросовестному освоению образовательной программы и выполнению учебного плана по установленной форме.

4.2 Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы на защите ВКР

Защита ВКР является завершающим этапом ГИА. Не позднее чем за 2 календарных дня до защиты ВКР обучающийся представляет секретарю ГЭК ВКР, отзыв руководителя и рецензию.

Специалист института за 2 рабочих дня до защиты ВКР передает секретарю ГЭК следующие документы:

- зачетные книжки обучающихся;
- приказ об утверждении составов ГЭК для проведения ГИА и апелляционных комиссий по результатам ГИА (копия);
- распоряжение директора института об утверждении расписания государственных аттестационных испытаний (копия);
- приказ об утверждении тем и руководителей ВКР (копия);
- протоколы ГЭК по приему государственного экзамена;
- программу ГИА (копия);
- распоряжение директора института о допуске обучающихся к ГИА (копия);
- заявления от обучающийся из числа инвалидов о необходимости (отсутствие необходимости) присутствия ассистента на государственном аттестационном испытании, о необходимости (отсутствие необходимости) увеличения продолжительности сдачи государственного аттестационного испытания по отношению к установленной продолжительности (для каждого государственного аттестационного испытания (копии, при наличии);
- проект приложения к диплому, согласованный с выпускником, списки выпускников, претендующих на получение диплома с отличием;
- списки выпускников, распределенные по дням защиты ВКР в соответствии с расписанием ГИА;
- экзаменационные ведомости по приему государственного аттестационного испытания.

На основании представленных документов секретарь ГЭК готовит:

- бланки оценочных листов каждому члену ГЭК;
- протоколы заседания ГЭК по защите ВКР на каждый день защиты ВКР согласно расписанию ГИА.

Защита ВКР проводится в виде открытых заседаний ГЭК с участием не мене двух третей ее списочного состава.

Заседания ГЭК по защите ВКР проводится согласно утвержденному расписанию ГИА.

Процедура защиты ВКР включает в себя:

- открытие заседания ГЭК: председатель ГЭК в начале заседания излагает порядок защиты, принятия решения, оглашения результатов ГЭК; устанавливает обучающимся время для устного изложения основных результатов ВКР и ответов на вопросы членов ГЭК;
- доклад выпускника: доклад сопровождаться показом презентации, выполненной в редакторе PowerPoint с иллюстрациями, таблицами, рисунками, схемами и пояснениями и распечатанной в качестве раздаточного материала для каждого члена ГЭК на бумажном носителе;
- вопросы членов ГЭК записываются в протокол заседания ГЭК;
- заслушивание отзыва: после ответа обучающегося на все вопросы председатель ГЭК дает возможность руководителю ВКР выступить с отзывом. Выступление руководителя ВКР должно быть кратким и касаться аспектов отношения обучающегося к выполнению ВКР,

самостоятельности, результатов проверки текста ВКР на объем заимствований. При отсутствии руководителя ВКР его отзыв зачитывает председатель ГЭК;

−заслушивание рецензии: слово предоставляется рецензенту или председатель зачитывает его письменный отзыв.

−заключительное слово обучающегося: обучающемуся предоставляется возможность ответить на замечания, сделанные рецензентом.

Члены ГЭК на закрытом заседании оценивают результаты защиты ВКР каждым обучающимся и результаты освоения образовательной программы. Решения ГЭК принимаются на основе открытого голосования простым большинством голосов от числа лиц, входящих в состав ГЭК и участвующих в заседании. При равном числе голосов председатель ГЭК обладает правом решающего голоса.

Результаты защиты ВКР определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение государственного аттестационного испытания и ГИА.

Результаты защит ВКР оглашает председатель ГЭК после окончания закрытой части заседания ГЭК в день его проведения.

Оценка за защиту ВКР проставляется в зачетную книжку обучающегося, в экзаменационную ведомость по защите ВКР и в протокол заседания ГЭК по защите ВКР. Оценка за защиту ВКР, проставленная в зачетную книжку обучающегося, в экзаменационную ведомость по защите ВКР подтверждается подписями председателя и секретаря. Протокол заседания ГЭК по защите ВКР подписывают председатель и секретарь ГЭК.

По окончанию всех заседаний ГЭК по защите ВКР протоколы заседаний ГЭК сшиваются в книги. Книги передаются для хранения в архив университета, остальные документы передаются секретарем ГЭК специалисту института для организации хранения в деканате факультета.

Обучающиеся, не прошедшие защиту ВКР в связи с неявкой на данное государственное итоговое аттестационное испытание по неуважительной причине или в связи с получением оценки «неудовлетворительно», а также обучающиеся из числа инвалидов, не прошедшие данное государственное итоговое аттестационное испытание в установленный для них срок (в связи с неявкой на данное государственное итоговое аттестационное испытание или получением оценки «неудовлетворительно»), отчисляются из университета с выдачей справки об обучении как не выполнившие обязанностей по добросовестному освоению образовательной программы и выполнению учебного плана по установленной форме.

ФОС для проведения ГИА обсужден на заседании кафедры безопасности информационных систем.

Протокол № 08 от «13» января 2020 г.