МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

Институт естественных наук и математики

УТВЕРЖДАЮ
Проректор по учебной работе

_____ С.Т. Князев

«___» _____ 2018 г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ (ГИА)

Перечень сведений о программе ГИА	**Учетные данные**
Образовательная программа Компьютерная безопасность	**Код ОП** 10.05.01/01.02
Направление подготовки Компьютерная безопасность	**Код направления и уровня подготовки** 10.05.01
Уровень подготовки специалитет	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: 1 декабря 2016 г., № 1512

Екатеринбург, 2018

Программа государственной итоговой аттестации составлена авторами:

№	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Баранский Виталий Анатольевич	Доктор физ.-мат. наук, профессор	профессор	Кафедра алгебры и фундаментальной информатики	

Руководитель образовательной программы (далее - ОП) В.А. Баранский

Рекомендовано учебно-методическим советом Института Естественных Наук и Математики

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15.12.2016 г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

ОБЩАЯ ХАРАКТЕРИСТИКА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

1.1. Цель государственной итоговой аттестации

Целью государственной итоговой аттестации является установление уровня подготовленности обучающегося, осваивающего образовательную программу бакалавриата выполнению профессиональных задач и соответствия его подготовки требованиям федерального государственного образовательного стандарта высшего образования (требованиям образовательного стандарта, разрабатываемого и утверждаемого университетом самостоятельно) и ОП по направлению подготовки высшего образования, разработанной на основе образовательного стандарта. В рамках государственной итоговой аттестации проверяется уровень сформированности следующих результатов освоения образовательной программе, заявленных в ОХОП:

Код результата обучения	Результаты обучения	Компетенции, формируемые в рамках достижения результатов обучения
РО-01	Способность эффективно общаться в межкультурной среде в устной и письменной форме с применением информационно-коммуникационных технологий, демонстрировать профессиональную, социальную ответственность на основе правовых и этических норм, работать в команде и организовывать работу коллективов, развивать свои духовные и физические качества.	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, способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности; ОК-8, способность к самоорганизации и самообразованию; ОК-9, способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности; ОПК-3, способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и

		обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации; ОПК-6, способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций; ПК-1, способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности; ПК-13, способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности; ДПК-1, способность разрабатывать планы и программы проведения научных исследований и технических разработок, подготавливать отдельные задания для исполнителей и контролировать их выполнение.
РО-02	Способность применять основополагающие принципы и современные достижения физико-математических наук, математического описания и построения компьютерных систем, а также современные информационные технологии в разработке технологических решений с использованием программного кода.	ПК-4, способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем; 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-8, способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов; ПСК-2.5, способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

РО-03	Способность осуществлять проектирование систем защиты информации с учётом актуальных информационных угроз и с использованием современных достижений науки и техники.	ОК-2, способность использовать основы экономических знаний в различных сферах деятельности; ОПК-4, способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами; ОПК-7, способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения; 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; 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, способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем; ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов.
РО-04	Способность обеспечивать защищенность и функциональность компьютерных систем, производить их администрирование и профилактику работоспособности.	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; 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-10, способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-12, способностью проводить инструментальный мониторинг защищенности компьютерных систем; ПК-17, способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение; 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, способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций; ПСК-2.4, способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации; ПСК-2.5, способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации; ДПК-1, способность разрабатывать планы и программы проведения научных исследований и технических разработок, подготавливать отдельные задания для исполнителей и контролировать их выполнение;

		ДПК-5, способность восстанавливать работоспособность систем защиты при сбоях и нарушении функционирования; ДПК-6, способность обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи.
РО-05	Способность демонстрировать понимание нормативно-методической документации в сфере информационной безопасности, охраны труда и профилактики травматизма для дальнейшего применения в области организации и контроля в рамках организационно-управленческой деятельности.	ОК-4, способность использовать основы правовых знаний в различных сферах деятельности; 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; 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-16, способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем; ПКД-4, способность организовывать работы по совершенствованию, модернизации и унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России.
РО-06	Способность осуществлять планирование работ по защите информации в компьютерных системах.	ОК-2, способность использовать основы экономических знаний в различных сферах деятельности; ОК-4, способность использовать основы правовых знаний в различных сферах деятельности; 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; 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; 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-13, способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности; ПК-14, способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа; ПК-15, способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы; ПСК-2.2, способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ДПК-1, способность разрабатывать планы и программы проведения научных исследований и технических разработок, подготавливать отдельные задания для исполнителей и контролировать их выполнение; ДПК-2, способность к разработке требований и критериев информационной безопасности, согласованных со стратегией развития предприятия.
РО-07	Способность проводить аудит и аттестацию объектов, обеспечивающих информационную безопасность, на соответствие требованиям государственных и/или корпоративных документов, а также устанавливать режим информационной безопасности на предприятии и контролировать его соблюдение.	ОК-4, способность использовать основы правовых знаний в различных сферах деятельности; ОПК-5, способностью использовать нормативные правовые акты в своей профессиональной деятельности; 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-9, способность участвовать в проведении аттестации объектов с учетом требований к уровню защищенности компьютерной системы; ПК-11, способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации; ДПК-3, способность проводить аудит информационной безопасности и составлять итоговые документы аудита, содержащие выводы и рекомендации.
РО-08	Способность к разработке, анализу и обоснованию адекватности математических моделей процессов, возникающих при функционировании программно-аппаратных средств защиты информации, а также к разработке математических моделей для оценки безопасности компьютерных систем.	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-7, способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения; 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; 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-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы; ПСК-2.1, способностью разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов; ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации; ПСК-2.5, способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

1.2. Структура государственной итоговой аттестации

- государственный междисциплинарный экзамен;

- защита выпускной квалификационной работы в форме дипломной работы.

1.2.1.Форма проведения государственного экзамена:

устная.

1.3. Трудоемкость государственной итоговой аттестации:

Общая трудоемкость государственной итоговой аттестации составляет 9 з.е.

1.4. Время проведения государственной итоговой аттестации

- государственный экзамен – 11 семестр;

- выпускная квалификационная работа – 11 семестр.

1.5.Требования к процедуре государственной итоговой аттестации.

Требования к порядку планирования, организации и проведения ГИА, к структуре и форме документов по организации ГИА сформулированы в утвержденной в УрФУ документированной процедуре «Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры» (СМК-ПВД-6.1-01-65-2015), введенной в действие приказом ректора от 01.12.2015 №899/03.

1.6. Требования к оцениванию результатов освоения ОП в рамках государственной итоговой аттестации

Объективная оценка уровня соответствия результатов обучения требованиям к освоению ОП обеспечивается системой разработанных критериев (показателей) оценки освоения знаний, сформированности умений и опыта выполнения профессиональных задач.

Критерии оценки утверждены на заседании учебно-методического совета института, реализующего ОП, от «11» апреля 2016 г., протокол № 4.

ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

2.1. Тематика государственного экзамена

Часть 1

1. Теорема о существовании и единственности НОД двух многочленов.
2. Теорема о размерности пространства решений однородной системы линейных уравнений.
3. Теорема о размерности суммы двух подпространств.
4. Теорема о ранге матрицы.
5. Формула Эйлера для плоских графов, непланарность K5 и K3,3.
6. Теорема Хивуда о пяти красках.
7. Теорема о связи собственных значений линейного преобразования с корнями его характеристического многочлена.
8. Теорема о связи размерностей ядра и образа линейного отображения.
9. Теорема об ортогонализации линейно независимой последовательности элементов евклидова пространства.
10. Нормальные делители и факторгруппы, первая теорема о гомоморфизмах для групп.
11. Непрерывные функции. Теорема Больцано–Коши о промежуточных значениях для функций, непрерывных на отрезке. Теоремы Вейерштрасса о функциях, непрерывных на отрезке.
12. Теоремы Ролля и Лагранжа для дифференцируемых функций. Формула Тейлора с остаточным членом в форме Лагранжа.
13. Определенный интеграл Римана по отрезку. Теорема существования определенного интеграла от непрерывной функции. Свойства интеграла с переменным верхним пределом: непрерывность и дифференцируемость. Формула Ньютона–Лейбница.
14. Степенные ряды на числовой прямой и в комплексной плоскости. Круг и радиус сходимости степенного ряда; вычисление радиуса сходимости степенного ряда. Бесконечная дифференцируемость суммы степенного ряда.
15. Дифференцируемость сложной функции от нескольких переменных; производная по направлению; градиент.
16. Теорема об общем решении линейного однородного дифференциального уравнения с постоянными коэффициентами (с доказательством для случая простых корней).

17. Схема независимых испытаний. Формула Бернулли. Теорема Пуассона.
18. Математическое ожидание случайной величины и его свойства.
19. Закон больших чисел (неравенство Чебышева, теоремы Чебышева, Маркова и Бернулли).
20. Представление булевых функций формулами алгебры высказываний и многочленами Жегалкина.
21. Замкнутые классы булевых функций, критерий полноты для булевых функций.
22. Задача о минимальном остове и алгоритм Борувки-Краскала.
23. Алгоритм Дейкстры нахождения кратчайших расстояний от выделенной вершины до остальных вершин графа.
24. Линейные коды, порождающая матрица, граница Синглтона, граница Плоткина.
25. Контрольная матрица, код Хэмминга, характеризация минимального расстояния в терминах контрольной матрицы, граница Гильберта-Варшамова.
26. Циклические коды. Коды, исправляющие пакеты ошибок, граница Рейджера, алгоритм исправления пакетов ошибок.
27. Основные параметры кодов, исправляющих ошибки: длина, скорость, минимальное расстояние. Связь между минимальным расстоянием и корректирующими возможностями кода. Граница Хэмминга.
28. Шифры замены и перестановки (общие определения и конкретные примеры). Абсолютно стойкий шифр Вернама.
29. Классическая схема криптографической защиты информации. Ее достоинства и недостатки. Примеры симметричных криптоалгоритмов. Стандарты Российской Федерации. Основные режимы шифрования длинных сообщений.
30. Схема криптографической защиты информации с открытым ключом. Ее достоинства и недостатки. Примеры асимметричных криптоалгоритмов. Понятие хэш-функции. Стандарт Российской Федерации. Криптосистема RSA.

Часть 2

1. Понятие ущерба компьютерной информации. Понятие угрозы безопасности информации. Классификационные схемы и каталоги угроз. Идентификация и описание угроз. Общая схема оценивания угроз. Оценка рисков, методы и шкалы оценки. Человеческий фактор в угрозах безопасности и модель нарушителя информационной безопасности.
2. Понятие политики и моделей безопасности информации в компьютерных системах. Субъектно-объектная модель Щербакова. Аксиомы защищенности компьютерных систем. Политики безопасности компьютерных систем. Монитор безопасности. Гарантии выполнения политики безопасности. Изолированная программная среда.
3. Модели мандатного доступа. Решетка уровней безопасности. Модель Белла-ЛаПадулы. Безопасная функция перехода МакЛина. Модель LowWraterMark.
4. Архитектура файловых систем ext*fs. Размещение элементов файловой системы на дисковом пространстве. Блоки и экстенты. Назначение и структура суперблока, описателей групп блоков, карт битовых полей, индексных дескрипторов, журнала транзакций. Структура регулярного файла, каталога, символической ссылки.
5. Учетные записи пользователей в ОС Linux. Изменение, редактирование, удаление и временное блокирование учетных записей. Конфигурационные файлы group, passwd, shadow, login.defs. Смена паролей. Процедура регистрации и ее безопасность. Смена пользователей. Предоставление эффективных прав доступа. Механизм SUDO. Списки контроля доступа. Распространенные атаки на права администратора системы.
6. Аудит событий безопасности в ОС (на примере ОС Linux и Windows). Понятие адекватной политики аудита. Сбор информации об опасных файловых объектах. Наблюдение за процессами и пользователями. Отслеживание взаимосвязей между субъектами, процессами и объектами. Аудит событий: источники, потребители и уровни значимости сообщений. Анализ событий аудита. Защита системы протоколирования событий.
7. Разграничение доступа в ОС Windows. Объекты и субъекты доступа. Права и методы доступа. Дескриптор защиты. Дискреционный список контроля доступа. Системный список контроля доступа. Структура маркера доступа. Методы идентификации и аутентификации пользователей, применяемые в ОС Windows. Процесс проверки подлинности при входе в систему. Хранение парольной информации. Алгоритмы локальной и сетевой аутентификации.

8. Механизмы криптозащиты, встроенные в ОС Windows. Криптографическая защита пользовательских данных средствами шифрующей файловой системы EFS. Структура зашифрованного файла. Понятие агента восстановления. Технология BitLocker.
9. Организация и свойства файловой системы NTFS. Структура MFT. Стандартные атрибуты файлов и каталогов в NTFS. Основные операции над объектами файловой системы. Резидентные и нерезидентные атрибуты. Потоки. Структура каталогов.
10. Анализ и восстановление данных на логических разделах. Последовательность логического удаления файлов в файловых системах ext*fs и NTFS. Виды повреждений файловых систем. Возможности дисковых редакторов по восстановлению информации. Копирование информации с поврежденных машинных носителей.
11. Функции, выполняемые средствами защиты информации (СЗИ). Механизмы доверенной загрузки ОС, реализованные в СЗИ. Контроль целостности системного программного обеспечения и аппаратных средств. Программно-аппаратная идентификация и аутентификация пользователей. Формирование и поддержка изолированной программной среды. Требования к специализированным средствам защиты информации от несанкционированного доступа. Основные возможности СЗИ от НСД «Аккорд-АПМДЗ», «Secret Net».
12. Возможности СЗИ по криптографическому преобразованию информации. Способы формирования ключевой информации. Структура файл-образа виртуального зашифрованного диска. Способы формирования электронной подписи. Требования к СКЗИ. Основные возможности СКЗИ «КриптоПро CSP».
13. Понятие и виды электронной подписи. Схема использования электронной подписи. Требования к средствам электронной подписи. Понятие инфраструктуры открытых ключей. Электронные сертификаты. Понятие удостоверяющих центров.
14. Определение и классификация компьютерных атак. Уязвимости компьютерных систем. Общедоступные базы данных уязвимостей. Наиболее актуальные компьютерные сетевые атаки, механизмы их осуществления, способы защиты. Понятие распределенных атак на отказ в обслуживании. Классификация уязвимостей Web-приложений, способы их выявления.
15. Назначение и классификация систем обнаружения атак. Технологии обнаружения компьютерных атак. Правила обнаружения атак на примере СОА Snort. Системы обнаружения аномалий на примере Cisco IDS Sensor. Требования к СОВ.
16. Понятие о межсетевом экранировании. Компоненты межсетевого экрана. Политика сетевой безопасности. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов. Требования к межсетевым экранам. Списки доступа и их настройка (на примере оборудования Cisco).
17. Сущность технологий VPN, цели и задачи их использования. Компоненты VPN. Туннелирование в VPN. Протоколы и средства создания VPN на канальном, сетевом, транспортном и прикладном уровнях.
18. Аудит безопасности компьютерных систем. Цели, стандарты, подходы. Классификация средств анализа защищенности компьютерных систем, их возможности и недостатки. Методика проведения инструментальных проверок безопасности компьютерных систем.
19. Понятие о вредоносных программах. Классификация вредоносных программ по основным свойствам и признакам. Деструктивные функции вредоносных программ. Механизмы вирусного заражения. Способы выявления деструктивной активности программ. Понятие о сигнатуре вредоносного программного кода. Принцип антивирусного сканирования. Антивирусные сканеры, мониторы и эвристические анализаторы.
20. Инженерно-техническая защита объектов от неправомерного физического доступа. Виды охраняемых объектов. Требования к элементам инженерной защиты объекта информатизации. Средства и методы контроля за проникновением человека-нарушителя на территорию объекта. Требования к техническим средствам охраны.
21. Защита информации от утечки по техническим каналам. Понятие утечки и перехвата информации с использованием технических каналов. Каналы утечки и их виды. Общая характеристика визуально-оптического, электромагнитного, акустического и материально-вещественного каналов. Виды защиты от технической утечки: определение факта и пространственной зоны утечки, энергетическое скрытие сигналов.
22. Требования к режимным помещениям и рабочим местам, предназначенным для размещения АС. Категорирование АС. Объем, содержание и порядок проведения специальной лабораторной проверки компонентов и узлов СВТ. Назначение, объем и содержание специальных исследований

АС. Оформление предписания на эксплуатацию и формуляра АС. Порядок приобретения, использования и обновления общесистемного и прикладного программного обеспечения АС.

23. Государственная тайна как особый вид защищаемой информации, и ее характерные признаки. Степени секретности сведений, составляющих государственную тайну, гриф секретности и реквизиты их носителей. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Правовой режим защиты государственной тайны. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Система контроля за состоянием защиты государственной тайны. Ответственность за нарушения правового режима защиты государственной тайны.
24. Понятие персональных данных. Специальные категории персональных данных. Понятия оператора персональных данных и информационной системы персональных данных. Государственный орган по защите прав субъектов персональных данных и его компетенция. Предусмотренные законом меры по защите персональных данных. Классификация ИСПДн.
25. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Характеристика объективной стороны преступлений, предусмотренных гл. 28 УК РФ. Формы несанкционированного копирования, удаления, модификации и блокирования защищаемой законом компьютерной информации, нейтрализации средств ее защиты. Ответственность за совершение преступлений, предусмотренных ст. 272 – 274 УК РФ.
26. ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Категорирование объектов критической информационной инфраструктуры Российской Федерации. Назначение, функции и принципы создания ГосСОПКА. Концепция ГосСОПКА.
27. Интеллектуальные права и право собственности. Автор и правообладатель результатов интеллектуальной деятельности. Виды лицензионных договоров. Защита личных неимущественных и исключительных прав. Авторское и смежные права и их объекты. Охрана авторских прав на программы для ЭВМ и смежных прав на базы данных и технические средства их защиты. Ответственность за нарушение авторских и смежных прав.
28. Лицензирование и техническое регулирование деятельности в сфере защиты информации; организационная структура и общая характеристика систем лицензирования. Цели и принципы сертификации. Органы добровольной и обязательной сертификации; их аккредитация. Системы сертификации в сфере защиты информации; особенности разработки, производства и эксплуатации средств защиты информации.
29. Требования и меры защиты информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Классификация ГИС. Порядок определения класса защищенности информационной системы.
30. Выявление и реагирование на инциденты информационной безопасности. Понятие компьютерных инцидентов. Нормативные требования в области управления инцидентами информационной безопасности. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности.

2.2. Тематика выпускных квалификационных работ

Примерная тематика выпускных квалификационных (дипломных) работ

1. Интеллектуальная система конкурентного обучения для анализа сетевой активности пользователя.
2. Аутентификация человека по движению.
3. Обзор попыток атак на WPA2.
4. Интеллектуальная система внедрения и обнаружения цифровых визуальных водяных знаков на основе конкурентного обучения нейронных сетей.
5. Интеллектуальный аватар анализа активности пользователя.
6. Интеллектуальная система выявления фактов шпионажа устройств в рамках системы "умный дом».
7. Криптографическая стойкость генераторов псевдослучайных чисел на основе апериодических последовательностей.
8. Создание вычислительного кластера на базе операционной системы Linux для решения переборных задач в сфере информационной безопасности.

9. Поиск закономерностей в зашифрованных текстах на основе известных закономерностей в открытых текстах.

10. Об одном подходе к интеграции виртуальных машин .NET и Java.

11. Разработка обучающего программного комплекса «исследование актуальных Web уязвимостей».

12. Защита персональных данных в системе контроля состояния здоровья спортсменов спортивными организациями.

Содержание выпускной квалификационной работы обучающегося должно удовлетворять установленным требованиям ФГОС по специальности Компьютерная безопасность.

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

3.1. Рекомендуемая литература

3.1.1. Основная литература

1. Андрончик А.Н. и др. Защита информации в компьютерных сетях. Практический курс: учебное пособие / А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский, А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков, М.Ю. Щербаков; Под ред. Н.И. Синадского. – Екатеринбург: ГОУ ВПО УГТУ - УПИ, 2007. – 246 с.

2. Асанов М.О., Баранский В.А., Расин В.В. Дискретная математика: графы, матроиды, алгоритмы (второе издание, исправленное и дополненное). – СПБ: Изд – во «Лань», 2010.

3. Бакланов В.В. Администрирование и безопасность операционных систем Linux : учебное пособие [для вузов] / В. В. Бакланов ; науч. ред. Н. А. Гайдамакин. — Екатеринбург : [УГТУ-УПИ], 2006 . — 92 с. : ил. — (Информационная безопасность) . — Библиогр.: с. 85. 15 экз.

4. Бакланов В.В. Введение в информационную безопасность. Направления информационной защиты : курс лекций : учеб. пособие для вузов / В. В. Бакланов .— Екатеринбург : Изд-во Уральского университета, 2007 .— 232 с. — (Приоритетный национальный проект "Образование") (Математика. Компьютерные науки) .— Библиогр.: с. 229-232 .— ISBN 5-7996-0259-5.

5. Баранский В.А., Кабанов В.В. Общая алгебра и ее приложения. – Екатеринбург: Изд-во УрГУ, 2008.- 244 С.

6. Бузов Г.А., Защита от утечки информации по техническим каналам : учеб. пособие для подгот. экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев .— М. : Горячая линия - Телеком, 2005. — 416 с.

7. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах / Н. А. Гайдамакин. — Екатеринбург : Издательство Уральского университета, 2003 .— 328 с. : ил. ; 21 см .— Алф.-предм. указ.: с. 306-316. — Библиогр.: с. 317-322 (80 назв.). — ISBN 5-86037-024-5 : 40.00.

8. А.И.Кострикин. Введение в алгебру. М.: МЦНМО, 2009 (Кострикин А.И., Введение в алгебру: Учеб. пособие для вузов / А. И. Кострикин .— М. : Наука, 1977 .— 495 с.)

9. Расторгуев С.П. Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телекоммуникац. систем" / С. П. Расторгуев .— Москва : Академия, 2007 .— 188 с. ; 22 см .— (Высшее профессиональное образование, Информационная безопасность) .— Слов. терминов: с. 182-185. — Библиогр.: с. 180-181 (39 назв.). — Допущено в качестве учебного пособия. — ISBN 978-5-7695-3098-2.

10. Синадский Н.И. Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие / Н. И. Синадский ; науч. ред. В. В. Бакланов .— Екатеринбург : [ГОУ ВПО УГТУ-УПИ], 2007. — 136 с. 90 экз.

11. Сидельников, В.М. Теория кодирования [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : Физматлит, 2008. — 320 с. <URL: http://www.biblioclub.ru/book/68384/>.

10. Синицын С.В. Операционные системы : учебник для вузов / С. В. Синицын, А. В. Батаев, Н. Ю. Налютин .— 3-е изд., стер. — Москва : Издательский центр "Академия", 2013 .— 296 с. 9 экз.

12. Торокин, А.А. Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. безопасности / А. А. Торокин .— Москва : Гелиос АРВ, 2005 .— 960 с.

13. Фергюсон Н. Практическая криптография / Нильс Фергюсон, Брюс Шнайер ; [пер. с англ. Н. Н. Селиной под ред. А. В. Журавлева] .— Москва ; Санкт-Петербург ; Киев : Диалектика, 2005 .— 424 с.

; 24 см .— Предм. указ.: с. 418-421. — Пер. изд.: Practical Cryptography / N. Ferguson, B. Schneier. - 2003. — Библиогр.: с. 410-417.
14. Фихтенгольц Г.М. Основы математического анализа: учеб. для студентов вузов, обучающихся по специальностям в обл. естественных наук и математики, техники и технологий, образования и педагогики. Ч. 1 / Фихтенгольц Г. М. - Изд. 9-е, стер. – СПб. И др.: Лань, 2008. – 448 с.
15. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие для студентов вузов, обучающихся по направлению 23100 (654600) "Информатика и вычисл. техника" / П. Б. Хорев .— М. : Academia, 2005 .— 256 с. 29 экз.
16. Ширяев А. Н. Вероятность. В 2-х кн. Кн.1. — 3-е изд., перераб. и доп. — М.: МЦНМО, 2004. - 520 с ISBN 5-94057-036-4
17. Шолохович Ф.А.. Лекции по дифференциальным уравнениям (университетский курс). - Екатеринбург: УрГУ, 2005. 232 с.

3.1.2. Дополнительная литература

1. Барсуков, В. С. Современные технологии безопасности: интегральный подход / В.С. Барсуков, В.В. Водолазкий .— М. : Нолидж, 2000 .— 496 с.
2. Введение в криптографию: Учебник / В.В. Ященко, Н.П. Варновский, Ю.В. Нестеренко и др. ; Под общ. ред. В.В. Ященко .— СПб.; М.; Харьков; Минск : МЦНМО : Питер, 2001 .— 288 с. : ил.; 24 см .— (Новые математические дисциплины) .— Библиогр. в конце гл. — Прил.: Отрывок из ст. К. Шеннона "Теория связи в секретных системах": с. 251-287. — без грифа .— ISBN 5-318-00443-1 : 80.00.
3. Галатенко, В. А. Стандарты информационной безопасности. Курс лекций : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. технологий / В. А. Галатенко ; под ред. В. Б. Бетелина .— 2-е изд. — Москва : Интернет-Университет Информационных Технологий, 2009 .— 264 с.
4. Копылов, Виктор Александрович. Информационное право: учебник / В. А. Копылов ; М-во образования РФ, Моск. гос. юрид. акад. — Изд. 2-е, перераб. и доп. — М. : Юристъ, 2005 .— 511 с.
5. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки: учебник. РГГУ, 2002. — 400 с.
5. Олифер В. Г. Сетевые операционные системы : учеб. для вузов / В. Г. Олифер, Н. А. Олифер .— 2-е изд. — Москва [и др.] : Питер, 2008 .— 669 с.
6. Петраков, А.В. Основы практической защиты информации : Учеб. пособие для вузов по спец. 20. 18. 00 "Защищенные системы связи" / А.В. Петраков .— 2-е изд. — М. : Радио и связь, 2000 .— 368 с.
7. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студентов вузов, обучающихся по специальностям 090102, 090105 / В. В. Платонов .— Москва : Академия, 2006 .— 240 с.
8. Проскурин В. Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах : Учеб. пособие для студентов вузов, обучающихся по спец. "Защищенные телекоммуникационные системы", "Орг. и технология защиты информации", "Комплексное обеспечение информ. безопасности автоматизир. систем" / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. — М. : Радио и связь, 2000 .— 168 с.
9. Робачевский А.М. Операционная система UNIX : Учеб. пособие для студентов вузов / А.М. Робачевский. — Дюссельдорф; Киев; М.; СПб. : БХВ-Петербург, 2002. — 514 с.
10. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — 2008. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11071>.

3.2. Методические разработки

1. Бакланов, В. В. Основы информационной безопасности / Бакланов В.В. — 2007. — Курс "Основы информационной безопасности" предназначен для студентов специальности "Компьютерная безопасность". — в корпоративной сети УрФУ. — <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11063>.
2. Гайдамакин Н.А. Теоретические основы компьютерной безопасности / Гайдамакин Н.А. — <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11073>. — 2008 .— Курс "Теоретические основы компьютерной безопасности" предназначен для студентов специальности "Компьютерная

безопасность".
3. Гайдамакин Н.А. Учебно-методический комплекс дисциплины "Основы создания и эксплуатации защищенных компьютерных систем" [Электронный ресурс] / Н. А. Гайдамакин ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (8,17 Мб) .— Екатеринбург : [б. и.], 2007 .— 1 электрон. опт. диск (CD-ROM) .— Загл. с этикетки
4. Исследование технических каналов утечки информации и методов борьбы с ними : метод. указания к лаб. работам по дисциплине "Техн. средства и методы защиты информации" для студентов специальности 075600 - Информ. безопасность телекоммуникац. систем / Урал. гос. техн. ун-т - УПИ ; [сост. А. С. Лучинин ; науч. ред. А. П. Мальцев] .— Екатеринбург : УГТУ-УПИ, 2004 .— 39 с.
5. Сборник нормативных правовых актов по компьютерной и информационной безопасности. Т. 1. Законодательные акты РФ, указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ / Урал. гос. техн. ун-т - УПИ, Регион. учеб.-науч. центр по проблемам информ. безопасности ; [авт.-сост. Н. А. Гайдамакин] .— Екатеринбург : Гриф, 2006 .— 658 с. ; 29 см .— Библиогр. в тексте, библиогр. в примеч. — ISBN 5-98058-021-2.
6. Сборник нормативных правовых актов по компьютерной и информационной безопасности. Т. 2. Ведомственные нормативные правовые акты и руководящие документы / Урал. гос. техн. ун-т - УПИ, Регион. учеб.-науч. центр по проблемам информ. безопасности ; [авт.-сост. Н. А. Гайдамакин] .— Екатеринбург : Гриф, 2006. — 740 с.
7. Синадский Н.И. Безопасность операционных систем. УМК, 2007. Метаданные ресурса №7029.
8. Синадский Н.И. Учебно-методический комплекс дисциплины "Защита информации в компьютерных сетях" [Электронный ресурс] / Н. И. Синадский ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (13,3 Мб) .— Екатеринбург : [б. и.], 2008 .— 1 электрон. опт. диск (CD-ROM) .— Загл. с этикетки диска .— <URL:http://elar.urfu.ru/handle/10995/1654>.
9. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — 2008. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11071>.

3.3. Программное обеспечение

MS Office, Операционные системы семейства MS Windows

3.4. Базы данных, информационно-справочные и поисковые системы

1. http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
2. http://www.edu.ru/ - Федеральный портал. Российское образование.
3. http://study.urfu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.urfu.ru - официальный сайт ИРИТ-РтФ

3.5. Электронные образовательные ресурсы

1. Портал информационно-образовательных ресурсов УрФУ http://study.urfu.ru/info/default.aspx
2. Официальный сайт ИРИТ-РтФ http://rtf.urfu.ru
3. Официальный сайт кафедры ТОР УрФУ http://tor.rtf.urfu.ru

4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Персональные компьютеры. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.