УТВЕРЖДАЮ
Проректор по учебной работе
_____ В.Е. Федоров
«02» 09 2019 г.

ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

Специальность
10.05.01 Компьютерная безопасность

Специализация
Анализ безопасности компьютерных систем

Присваиваемая квалификация (академическая степень)
специалист по защите информации

Форма обучения
очная

Челябинск, 2019

Программа государственного экзамена принята:

Ученым советом математического факультета
Протокол заседания № 13 от «29» 08 2019 г.

Председатель Ученого совета
математического факультета _____Е.А. Сбродова

Секретарь Ученого совета
математического факультет _____С.А. Никитина

Программа государственного экзамена одобрена и рекомендована кафедрой компьютерной безопасности и прикладной алгебры
Протокол заседания № 11 от «15» 07 2019 г.

Заведующий кафедрой компьютерной
безопасности и прикладной алгебры _____А.Н. Ручай

Программа государственного экзамена составлена **в соответствии с требованиями** ФГОС ВО по специальности 10.05.01 Компьютерная безопасность (уровень специалитета), утвержден приказом Министерства образования и науки Российской Федерации № 1512 от 01.12.2016 г.

Программа государственного экзамена соответствует утвержденному учебному плану по специальности 10.05.01 Компьютерная безопасность.

Разработчик программы:

Заведующий кафедрой компьютерной
безопасности и прикладной алгебры _____А.Н. Ручай

Содержание

1. Вводная часть

Государственный экзамен (ГЭ) по специальности 10.05.01 Компьютерная безопасность представляет собой комплексный итоговый экзамен по основным разделам математики, компьютерных наук и информационной безопасности, а также той части образовательной программы, относящейся к присвоению выпускнику квалификации «Специалист по защите информации».

1.1. Цели и задачи государственного экзамена

Целью государственного экзамена является определение соответствия результатов освоения обучающимися основной профессиональной образовательной программы высшего образования – программы специалитета – требованиям действующего федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по специальности 10.05.01 Компьютерная безопасность.

Задачей государственного экзамена является оценка уровня сформированности общепрофессиональных (ОПК), профессиональных (ПК) и профессионально-специализированных (ПСК) компетенций, соответствующими видам деятельности, на которые ориентирована программа по специальности 10.05.01 Компьютерная безопасность, специализации Анализ безопасности компьютерных систем. Уровень сформированности ОПК, ПК и ПСК компетенций оценивается на заседаниях ГЭК (оценочный лист).

1.2. Форма проведения и трудоемкость государственного экзамена

В соответствии с основной профессиональной образовательной программой по специальности 10.05.01 Компьютерная безопасность подготовка к сдаче и сдача государственного экзамена составляет 3 з.е.

Государственный экзамен проводится государственной экзаменационной комиссией (ГЭК).

Государственный экзамен проводится в отдельной аудитории, которая должна быть оснащена средствами вычислительной техники, обеспечивающими рабочие места для решения экзаменационных задач с использованием профессиональных продуктов. Необходимое число рабочих мест должно быть установлено, исходя из количества задач, содержащихся в пакете экзаменационных заданий, который предполагается задействовать на ГЭ.

Перечень оборудования и профессиональных программных средств, используемых на ГЭ регламентируется ГЭК.

Компьютеры в аудитории для проведения государственного экзамена должны быть подключены исключительно к локальной сети структурного подразделения вуза.

В процессе подготовки к ответам на вопросы и решения задачи экзаменуемый имеет возможность пользоваться учебной и справочной литературой. Указанная литература должна располагаться в аудитории на специально отведенном месте, исключающем ведение записей и позволяющим читать необходимые тексты.

Государственный экзамен проводится в устной форме.

2. Перечень компетенций, подлежащих оценки в ходе государственного экзамена

Основной профессиональной образовательной программой ЧелГУ по специальности 10.05.01 Компьютерная безопасность, а также ФГОС ВО данной специальности предусмотрен следующий перечень компетенций, подлежащих оценки в ходе государственного экзамена:

Коды компетенций (по ФГОС ВО)	Содержание компетенций согласно ФГОС ВО
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
ОКП-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
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-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
ПСК-1.1	способность проводить анализ защищенности и находить уязвимости компьютерной системы
ПСК-1.2	способность оценивать корректность и эффективность программных реализаций алгоритмов защиты информации
ПСК-1.3	способность использовать современные критерии и стандарты для анализа безопасности компьютерных систем
ПСК-1.4	способность разрабатывать, отлаживать и тестировать программный код с использованием языков и систем программирования низкого уровня
ПСК-1.5	способность учитывать в профессиональной деятельности современные тенденции развития алгоритмов кодирования и сжатия различных видов информации

3. Критерии оценки государственного экзамена

3.1. Структура контрольно-оценочных материалов ГЭ

В состав контрольно-оценочных материалов, предназначенных для контроля и оценивания уровней освоения контролируемых на ГЭ компетенций, входят: теоретические вопросы ГЭ, практические задачи ГЭ, индивидуальные экзаменационные задания.

Теоретические вопросы ГЭ:

Вопросы обеспечивают контроль компонентов «Знать». Содержание вопросов определяется содержанием учебных дисциплин, обеспечивающих в ходе их изучения формирование у обучающихся определенных компонентов, контролируемых в процессе ГЭ компетенций. В целом содержание государственного экзамена определяется содержанием нескольких дисциплин и (или) модулей образовательной программы, результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников.

Практические задачи ГЭ:

Задачи должны обеспечивать контроль деятельностной составляющей компетенций («уметь») и носить, как правило, комплексный, междисциплинарный характер. Содержание задачи должно включать некоторую проблему, решение которой завершается определенным результатом, связанным с будущей профессиональной деятельностью и раскрывающим достигнутый уровень освоения заданных компетенций. В процессе подготовки решения задачи экзаменуемый производит анализ состояния проектной (исследуемой) проблемы, выбор и обоснование пути решения, реализацию проектного решения, в том числе с использованием информационных технологий (ИТ), оценивание результатов и практической ценности решения, формулирование выводов. На экзамене предлагаются задачи по следующим разделам: «Математический анализ», «Геометрия», «Дифференциальные уравнения», «Алгебра и теория конечных полей», «Теория вероятностей и математическая статистика», «Теория информации и кодирования», «Математическая логика», «Дискретная математика».

Индивидуальные экзаменационные практические задания ГЭ:

Индивидуальные экзаменационные задания (далее задания), выдаваемые экзаменуемым на ГЭ, являются, как правило, средствами контроля открытого типа, предполагающими подготовку ответов (решений) на содержащиеся вопросы и задачи. Индивидуальные задания ГЭ выполняют функцию контроля, обеспечивая формирование и представление результатов контроля (ответы на вопросы, решение задачи). Конкретное индивидуальное экзаменационное задание формируется из элементов Перечня вопросов ГЭ и Перечня задач ГЭ. Индивидуальное задание ГЭ включает 1 (одну) практическую задачу из следующих разделов: «Операционные системы и системное программирование», «Базы данных», «Вычислительные сети», «Программно-аппаратные средства обеспечения информационной безопасности», «Структуры данных и алгоритмы», «Языки программирования», «Технология программирования».

Практические задачи и индивидуальные экзаменационные практические задания каждый год актуализируются и предоставляются студенту во время государственного экзамена.

3.2. Критерии оценки государственного экзамена

Шкала оценивания достигнутых выпускником уровней освоения каждого из объектов контроля, представленных и раскрытых соответствующими индикаторами, должна быть составлена из следующих значений критерия соответствия:

– полностью соответствует;
– соответствует;
– соответствует частично;
– не соответствует.

Эти качественные значения степени соответствия каждого из объектов контроля требованиям ФГОС ВО и ОПОП эквивалентны следующим оценкам по четырехбалльной шкале:

– полностью соответствует – «отлично» (5);
– соответствует – «хорошо» (4);
– соответствует частично – «удовлетворительно» (3);
– не соответствует – «неудовлетворительно» (2).

В указанной шкале каждый из членов ГЭК производит оценивание уровня освоения каждого из компонентов контролируемых компетенций. В результате формируется множество частных оценок, фиксируемых в персональных оценочных листах экспертов.

Итоговая оценка ГЭ определяется как среднее арифметическое частных оценок, поставленных членами ГЭК, и округляется до целого значения. Частная оценка определяется по четырехбалльной шкале.

Оценка «5» («отлично») выставляется студентам, успешно сдавшим экзамен и показавшим глубокое знание теоретической части курса, умение проиллюстрировать изложение практическими примерами, полно и подробно ответившим на вопросы билета и вопросы членов экзаменационной комиссии.

Оценка «4» («хорошо») выставляется студентам, сдавшим экзамен с незначительными замечаниями, показавшим глубокое знание теоретических вопросов, умение проиллюстрировать изложение практическими примерами, полностью ответившим на вопросы билета и вопросы членов экзаменационной комиссии, но допустившим при ответах незначительные ошибки, указывающие на наличие не систематичности в знаниях.

Оценка «3» («удовлетворительно») выставляется студентам, сдавшим экзамен со значительными замечаниями, показавшим знание основных положений теории при наличии существенных пробелов в деталях, испытывающим затруднения при практическом применении теории, допустившим существенные ошибки при ответе на вопросы билетов и вопросы членов экзаменационной комиссии.

Оценка «2» («неудовлетворительно») выставляется, если студент показал существенные пробелы в знаниях основных положений теории, не умеет применять теоретические знания на практике, не ответил на вопросы билета или членов экзаменационной комиссии.

4. Методические рекомендации обучающимся по подготовке к государственному экзамену

Подготовка к государственному экзамену осуществляется в строгом соответствии с целевой установкой и в тесной взаимосвязи с потребностями области применения. Основу теоретической подготовки студентов составляет освоение лекционного и практического материала по базовым дисциплинам: «Теоретико-числовые методы в криптографии», «Теория информации и кодирования», «Структура данных и алгоритмы», «Технология программирования», «Криптографические методы защиты информации», «Защита информации», «Операционные системы и системное программирование», «Базы данных», «Вычислительные сети», «Программно-аппаратные средства обеспечения информационной безопасности», дополненной изучением соответствующих разделов рекомендуемой учебной литературы.

Проведенные практические и лабораторные занятия в компьютерных классах и специализированных лабораториях по защите информации позволяют закрепить знания, полученные студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельности будущего специалиста.

Защита объектов информатизации требует углубленного знания предметной области. В связи с этим необходимо использовать знания, приобретенные при изучении соответствующих специальных дисциплин, таких, как «Дискретная математика», «Конечные поля», «Математическая логика», «Дифференциальные уравнения», «Математический анализ», «Геометрия», «Теория вероятностей и математическая статистика», «Теория кодирования», «Теория информации и случайные процессы».

Для проверки уровня освоения учебного материала студенты имеют возможность воспользоваться контрольными вопросами по каждому разделу данной программы.

5. Особенности организации процедуры государственной итоговой аттестации лиц, имеющих ограниченные возможности здоровья

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

5.2. При проведении ГЭ обеспечивается соблюдение общих требований:

- проведение государственной итоговой аттестации для инвалидов в одной аудитории, совместно с обучающимися, не имеющими ограниченных возможностей здоровья (далее - ОВЗ), если это не создает трудностей для обучающихся при прохождении ГЭ;
- 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 членами ГЭК);
- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении государственной итоговой аттестации с учетом их индивидуальных особенностей;
- обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже, наличие специальных кресел и других приспособлений).

5.3. Все локальные нормативные акты ФГБОУ ВО «ЧелГУ» по вопросам проведения государственного экзамена доводятся до сведения обучающихся инвалидов в доступной для них форме.

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

– продолжительность сдачи государственного экзамена, проводимого в письменной форме – не более чем на 90 минут.

5.5. В зависимости от индивидуальных особенностей обучающихся с ОВЗ в ФГБОУ ВО «ЧелГУ» обеспечивается 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 обеспечение для слепых, либо зачитываются ассистентом;

письменные задания выполняются обучающимися на бумаге рельефно-точечным шрифтом Брайля, или выполняются на компьютере со специализированным программным обеспечение для слепых, либо надиктовываются ассистентом;

при необходимости обучающимся предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечение 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 предоставляются увеличивающие 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 коллективного пользования;

по их желанию государственные испытания проводятся в письменной форме;

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

письменные задания выполняются обучающимися на компьютере со специализированным программным обеспечением или надиктовываются ассистентом;

по их желанию государственные аттестационные испытания проводятся в устной форме.

5.6. Обучающийся инвалид, не позднее, чем за 3 месяца до начала проведения ГИА, в частности ГЭ, подает письменное заявление о необходимости создания для него специальных условий при проведении государственных аттестационных испытаний с указанием особенностей его психофизического развития, индивидуальных возможностей и состояния здоровья. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в ФГБОУ ВО «ЧелГУ»).

В заявлении обучающийся указывает на необходимость (отсутствие необходимости) присутствия ассистента на государственном аттестационном испытании, необходимость (отсутствие необходимости) увеличения продолжительности сдачи государственного аттестационного испытания по отношению к установленной продолжительности (для каждого аттестационного испытания).

Приложение
Теоретические вопросы ГЭ

Раздел 1. Дискретная математика
1. Комбинаторика.
   1) Правила суммы и произведения.
   2) Формула включения и исключения, примеры применения.
   3) Сочетания, перестановки, размещения, числа Стирлинга первого и второго рода, комбинаторный смысл этих чисел.
2. Графы.
   1) Определения графа, орграфа. Виды графов(полные, двудольные, регулярные, связные, плоские, планарные) и их основные свойства.
   2) Деревья, свойства деревьев, перечисление деревьев.
3. Конечные автоматы.
   1) Определение детерминированного конечного автомата (ДКА), недетерминированного конечного автомата (НКА), недетерминированного конечного автомата с ε-переходами (ε-НКА). Способы их задания. Расширение функций перехода по цепочке. Языки ДКА, НКА, ε-НКА.
4. Грамматики.
   1) Лемма о накачке для регулярных языков.
   2) Определение контекстно-свободных грамматик, примеры.
   3) Язык, задаваемый грамматикой.

Раздел 2. Теоретико-числовые методы в криптографии
1. Вероятностные тесты определения простоты числа (на основе теоремы Ферма, Соловея – Штрассена, Рабина – Миллера).
2. Тестирование чисел на простоту (Конягина-Померанса, Миллера).
3. Теорема Эйлера и малая теорема Ферма (с доказательством).
4. Алгоритмы факторизации целых чисел (Ленстры, p-1 - метод Полларда, ρ-метод Полларда, Шермана-Лемана, Диксона).

Раздел 3. Теория информации и кодирования
1. Энтропия и информация.
   1) Виды информации: собственная информация, условная информация, взаимная информация.
   2) Энтропия вероятностной схемы и ее свойства.
   3) Условная энтропия и ее свойства.
   4) Взаимная информация и ее свойства.
   5) Дискретный источник без памяти.

2. Коды источника.
   1) Скорость кодирования, скорость создания информации.
   2) Теоремы Шеннона об источниках.
   3) Префиксные коды, неравенство Крафта.
   4) Коды Шеннона – Фено, оптимальные коды Хаффмана.
3. Математическая модель канала связи.
   1) Дискретный канал без памяти.
   2) Код канала, скорость передачи кода по каналу.
   3) Средняя вероятность ошибки декодирования.
   4) Информационная ёмкость канала, пропускная способность канала связи, формулировка теоремы Шеннона о кодировании в канале.
4. Линейные коды.
   1) Порождающая матрица линейного кода, проверочная матрица.
   2) Минимальное кодовое расстояние, теорема Хемминга (с доказательством).
   3) Синдромное декодирование.
   4) Коды Хэмминга, декодирование кодов Хемминга.
5. Циклические коды.
   1. Порождающий многочлен циклического кода, проверочный многочлен.
   2. Порождающая и проверочная матрицы циклического кода.
   3. Синдром циклического кода, теорема о синдроме циклического кода (с доказательством).

Раздел 4. Структуры данных и алгоритмы

1. Алгоритмы на графах.
   1) Обход графа в глубину (алгоритм, сложность, применение).
   2) Алгоритмы нахождения компонент связности (поиск в ширину).
2. Алгоритмы на графах.
   1) Алгоритм нахождения кратчайших расстояний от выделенной вершины до всех остальных вершин графа (алгоритм Дейкстры).
   2) Поиск в ширину и кратчайшие пути в графе (теорема Флойда).
3. Алгоритмы внутренней сортировки.
   1) Сортировки сравнениями (сортировка вставками, пирамидальная сортировка, быстрая сортировка). Оценки сложности.
4. Алгоритмы поиска в деревьях.
   1) Деревья двоичного поиска, сбалансированные по высоте (красно-черные деревья).
   2) Оценка максимальной высоты сбалансированного дерева с n узлами.
   3) Алгоритм вставки элемента в дереве двоичного поиска, сбалансированного по высоте.

Раздел 5. Технология программирования

1. Жизненный цикл программ.
   1) Оптимизация программ. Алгоритмическая, машинно-зависимая, машинно-независимая оптимизация. Виды оптимизации, выполняемые компиляторами. Влияние оптимизации на переносимость.
   2) Способы написания переносимых программ.
   3) Тестирование программ. Функциональное и структурное тестирование.
2. Методологии программирования.
   1) Структурное программирование.
   2) Модульное программирование.
   3) Объектно-ориентированное программирование (ООП). Концепции ООП: инкапсуляция, наследование, полиморфизм, абстрагирование. Абстрактные типы данных. Классы, объекты и методы.

Раздел 6. Криптографические методы защиты информации

1. Математическая модель шифра.
   1) Классификация шифров: шифр замены и шифр перестановки. Примеры.
   2) Методы криптоанализа классических шифров.
   3) Современные стандарты шифрования: примеры, параметры, стойкость, скорость. Сравнительный анализ.
2. Симметрические системы шифрования.
   1. Определение блочного шифра. Режимы блочного шифрования. Сферы применения.
   2. Сеть Фейстеля, SP-сеть.
   3. Составные элементы алгоритмов шифрования AES, DES, ГОСТ 28147-89, ГОСТ 34.12-2015. Сравнительный анализ.
3. Поточные системы шифрования.
   1) Определение поточных шифров. Принципы построения. Требования к параметрам. Примеры. Сравнительный анализ.
   2) Линейные рекуррентные последовательности (регистры сдвига с обратной связью). Требования к параметрам.
4. Асимметричные системы шифрования.
   1. Асимметричная криптография. Модель и задачи асимметричной криптографии. Сферы применения.
   2. Алгоритм шифрования RSA. Атаки, не требующие факторизации, на алгоритм RSA. Выбор безопасных параметров алгоритма.
   3. Алгоритм шифрования Эль-Гамаля. Стойкость алгоритма Эль-Гамаля.
5. Электронная цифровая подпись.
   1) Математическая модель ЭЦП. Задачи ЭЦП. Сравнение ЭЦП и

собственноручной подписи. Атаки на ЭЦП. Сферы применения.
2) Общая ЭЦП, параметры, достоинства.
3) Слепая ЭЦП, совместная подпись.
4) Инфраструктура открытых ключей. Удостоверяющий центр. Сертификат: определение, цепочки, иерархия, управление.
5) Стандарты ЭЦП DSA, ГОСТ 34.10-94, ГОСТ 34.10-2012: параметры, стойкость, скорость. Сравнительный анализ.

6. Хеш-функции.
1) Общее понятие хеш-функции. Понятие однашаговой ХФ. Области применения ХФ. Основное требование к ХФ.
2) Ключевая ХФ, области использования. Безключевая ХФ, области использования.
3) Криптоанализ хеш-функции: коллизии 1 и 2 рода, атаки нахождения коллизий.
4) Стандарты хеш-функции SHA-1, SHA-3, ГОСТ 34.11-94, ГОСТ 34.11-2012: параметры, стойкость, скорость. Сравнительный анализ.

7. Протоколы передачи ключей.
1) Классификация ключей. Особенности управления симметрическими и асимметрическими ключами.
2) Основные принципы построения протоколов передачи ключей. Примеры.
3) Схема предварительного распределения ключевой информации. Пример.

8. Протоколы открытого распределения ключей.
1) Определение, примеры, сравнительный анализ.
2) Протокол Диффи-Хеллмана. Основные атаки на протокол. Выбор безопасных параметров протокола.
3) Атака «человек посередине» на протокол Диффи-Хеллмана. Возможные способы устранения этой атаки.

9. Протоколы аутентификации.
1) Основные подходы к построению протокола аутентификации. Примеры.
2) Основные задачи и цели протокола аутентификации Kerberos. Протокол Kerberos.
3) Основные атаки на протоколы аутентификации. Примеры.

10. Криптографические протоколы.
1) Схема разделения секрета. Пример.
2) Протокол доказательства с нулевым разглашением. Пример.
3) Протокол совместной генерации случайного значения. Пример.

Раздел 7. Защита информации

1. Информационная безопасность.

1) Понятие информационной безопасности и её место в системе национальной безопасности.
2) Виды и источники угроз информационной безопасности.
3) Система нормативно-правовых актов, регламентирующих обеспечение информационной безопасности.

2. Основные понятия защиты информации.
   1) Объекты, субъекты, методы доступа.
   2) Несанкционированный доступ (НСД).
   3) Уровни конфиденциальности объектов и уровни доступа субъектов.
   4) Категорирование автоматизированных систем (АС) и средств вычислительной техники (СВТ).
   5) Каналы утечки, побочные электромагнитные излучения и наводки (ПЭМИН).
   6) Специальные исследования (СИ) технических средств и специальная лабораторная проверка (СЛП).
3. Противоправная деятельность в информационной сфере.
   1) Уголовно-процессуальная характеристика компьютерных преступлений.
   2) Основные задачи организационной системы обеспечения ИБ.
   3) Понятие политики обеспечения ИБ. Структура, задачи службы информационной безопасности.
4. Модели разграничения доступа.
   1) Избирательное (дискреционное) разграничение доступа.
   2) Изолированная (замкнутая) программная среда.
   3) Полномочное (мандатное) разграничение доступа.
   4) Полномочное разграничение доступа с контролем информационных потоков.
   5) Ролевое разграничение доступа.

Раздел 8. Операционные системы и системное программирование

1. Операционная система.
   1) Понятие ОС. Компоненты ОС. Архитектура ОС. Ядро ОС.
   2) Основные функции ОС.
   3) Программно-аппаратные средства поддержки режима мультипрограммирования. Механизмы реализации многозадачности.
2. Процессор.
   1) Принципы работы процессора. Команды процессора, счетчик команд, слово состояния процессора.
   2) Режимы работы процессора (на примере процессоров архитектуры IA-32). Реальный и защищённый режимы работы. Привилегированный и

непривилегированный режимы работы.
3) Прерывания (программные, аппаратные и исключения) и их обработка.

3. Виртуальная память.
   1. Концепция виртуальной памяти, назначение.
   2. Аппаратные средства поддержки виртуальной памяти (на примере процессоров архитектуры IA-32). Механизм страничной трансляции. Таблицы и каталоги страниц.
4. Файловая система.
   1) Понятие ФС, назначение. Реализация ФС.
   2) Методы хранения информации о дисковых блоках, принадлежащих файлу в FAT, Ext2, NTFS, ReFS.
   3) Средства обеспечения надежности и высокой производительности ФС.
5. Процессы и потоки.
   1) Понятие процесса и потока. Представление процессов и потоков (на примере ОС Windows NT и Linux), основные структуры данных.
   2) Концепция состояний процессов. Диаграмма состояний процесса.
   3) Контекст процесса и потока.
6. Синхронизация процессов.
   1) Понятие синхронизации потоков и процессов.
   2) Условия корректной синхронизации (взаимного исключения, прогресса, ограниченного ожидания).
   3) Критические секции. Состояние гонки. Взаимное исключение.
   4) Примитивы синхронизации: семафоры, события, мьютексы, спин-блокировки.
   5) Примитивы межпроцессного взаимодействия: сообщения, каналы.
7. Программное окружение ОС.
   1) Компиляторы, линковщики.
   2) Статические и динамические библиотеки.
   3) Форматы объектных и исполняемых файлов.
   4) Загрузчик исполняемых файлов. Динамическая линковка.
   5) Интерфейс библиотечных вызовов. Системные вызовы.

Раздел 9. Базы данных

1.Базы данных.
   1) Понятие банка данных, классификация банков данных.
   2) Иерархическая, сетевая и реляционная модели данных; модели управления данными; преимущества и недостатки централизованной и распределенной модели управления данными.
   3) Понятие целостности и непротиворечивости базы данных, методы и средства обеспечения целостности и непротиворечивости.

2.Реляционная модель данных.
1) Суть, достоинства и недостатки.
2) Понятие о нормализации, виды нормальных форм, какие недостатки они устраняют.

3.Операторы и запросы SQL.
1) Общий вид оператора SQL (SELECT, INSERT, UPDATE, DELETE).
2) Вложенные подзапросы, объединения. Примеры.
3) Порядок выполнения оператора SELECT.

4.Реляционные базы данных.
1) Реляционная алгебра Кода.
2) Понятие схемы, логическое представление базы данных.
3) Таблицы и представления БД. Теоретико-множественные и специальные реляционные операции.

Раздел 10. Вычислительные сети

1.Технология Ethernet.
1) Принцип случайного множественного доступа к среде передачи — CSMA/CD. Обнаружение и устранение коллизий.
2) Ограничение на максимальный размер широковещательной сети Ethernet. Домен коллизий.
3) Fast Ethernet.
4) Полудуплексный и полнодуплексный режимы работы сети Ethernet. Условия для организации полного дуплекса, преимущества использования.

2.Концентраторы и коммутаторы.
1) Понятие концентратора, коммутатора. Принципы их работы.
2) Управляемые коммутаторы Ethernet.
3) Spanning Tree.
4) VLAN, IEEE 802.1Q.

3.Стек протоколов TCP/IP.
1) Межсетевой уровень: назначение, понятие IP-адреса, адреса сети, маски подсети, зарезервированные адреса.
2) Маршрутизация в IP-сетях: виды маршрутизации, таблица маршрутизации.
3) Транспортный уровень: назначение, протоколы, логические порты, диапазоны логических портов, сокеты.
4) Трансляция сетевых адресов: технологии NAT, PAT.
5) Прикладной уровень: функция, протоколы.
6) Физический уровень: MAC, LLC, протокол ARP.

4.Вычислительные сети.

1) Понятие вычислительной сети.
2) Топологии сетей.
3) Физическая организация сетей: Ethernet, Token Ring, FDDI.
4) Семиуровневая модель ISO/OSI.
5) Характеристики сетей: надежность, отказоустойчивость, масштабируемость, расширяемость, быстродействие. Примеры.

Раздел 11. Программно-аппаратные средства обеспечения информационной безопасности

1. Сетевая безопасность.
   1) Достоинства и недостатки основных технологий межсетевых экранов.
   2) Сравнительный анализ сетевых и хостовых систем обнаружения вторжений.
2. Виртуальные частные сети (VPN).
   1. Технологии построения VPN. Назначение. Режимы функционирования. Примеры использования.
   2. IPSec. Общая схема, назначение, характеристики, защитные функции. Туннельный и транспортный режимы работы.
   3. VPN в домене Windows. MSCHAP(v2) (общая схема, назначение, характеристики). NAP (основные компоненты, причины развертывания).
3. Вредоносное программное обеспечение.
   1) Понятие вредоносного программного обеспечения, классификация.
   2) Основные виды (вирусы, черви, руткиты, эксплоиты, трояны, бэкдоры). Механизмы работы.
   3) Модели распространения, методы внедрения.
   4) Методы обнаружения и защиты.
4. Уязвимости программного обеспечения.
   1) Понятие уязвимости. Классификация уязвимостей.
   2) Основные уязвимости кодирования: переполнение буфера, ошибки форматной строки, целочисленное переполнение, ошибки обращения по индексу.
   3) Шеллкоды. Эксплоиты. Методы создания, особенности функционирования.
   4) Защитные механизмы (защита на уровне компилятора, ASLR, DEP).
   5) Методы обхода защитных механизмов.
5. Защита программного кода.
   1) Статическое исследование кода и методы защиты от него.
   2) Динамическое исследование кода и методы защиты от него.
   3) Защита от несанкционированного копирования и использования.

6. Стандартные средства защиты ОС Windows.
   1) Внутренние механизмы разграничения доступа (маркеры доступа и дескрипторы защиты), структура и назначение, участие маркеров доступа и дескрипторов защиты в процедуре получения субъектов доступа к объектам ОС.
   2) Права ФС NTFS, назначение прав, управление правами, наследование прав, определение действующих прав, проверка прав при обращении к объекту ФС.
   3) Шифрованная файловая система EFS, архитектура, используемые алгоритмы шифрования и генерации ключей, способы хранения ключевой информации, разница в действии атрибута шифрования для файла и каталога, агенты восстановления EFS, организация совместного доступа к зашифрованному файлу.
   4) Механизмы аудита и протоколирования в ОС Windows, классы регистрируемых событий, управление аудитом (включение, отключение аудита определенных событий), аудит доступа к объектам ФС и реестра, журналы аудита, правила обращения с журналами аудита.
   5) Учетные записи пользователей и групп, хранение информации об учетных записях на жестком диске, классическая атака по сбросу и подбору пароля пользователя, способы защиты. Парольная политика.
   6) Доменные службы AD. Определение домена, леса. Схема AD. Объекты AD, атрибуты объектов. Контроллеры домена. Групповая политика.
7. Стандартные средства защиты ОС Linux.
   1) Внутренние механизмы разграничения доступа: атрибуты субъектов и объектов ОС, права (биты) доступа, SUID-, SGID-биты (подмена пользователя/группы пользователя).
   2) Учетные записи пользователей и групп, файлы учетных записей пользователей и групп, файлы теневых паролей. Классическая атака по сбросу и модификации пароля пользователя, противодействие атаке.