ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Проектирование защищенных телекоммуникационных систем

Код модуля	Модуль
1156882(1)	Проектирование защищенных телекоммуникационных систем

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
2	Синадский Николай Игоревич	кандидат технических наук, Доцент	Доцент	УНЦ "Информационная безопасность"

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Проектирование защищенных телекоммуникационных систем

1.	**Объем дисциплины в зачетных единицах**	4	
2.	**Виды аудиторных занятий**	Лекции Лабораторные занятия	
3.	**Промежуточная аттестация**	Экзамен	
4.	**Текущая аттестация**	Контрольная работа	1
		Реферат	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Проектирование защищенных телекоммуникационных систем

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	**Планируемые результаты обучения (индикаторы)**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**
ОПК-9 -Способен использовать программные, программно-аппаратные и технические средства защиты информации при решении задач профессиональной деятельности	З-1 - Идентифицировать профессиональную и криптографическую терминологию в области безопасности информации З-2 - Объяснять основные информационные технологии, используемые в автоматизированных системах З-3 - Объяснять основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах З-4 - Различать принципы работы элементов и функциональных узлов электронной аппаратуры,	Лабораторные занятия Лекции Экзамен

	типовые схемотехнические решения основных узлов и блоков электронной аппаратуры П-1 - Разрабатывать техническую документацию в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем П-2 - Разрабатывать программное обеспечение, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации П-3 - Оптимизировать работу электронных схем с учетом требований по защите информации У-1 - Оценивать сложность алгоритмов и вычислений У-2 - Проводить комплексное тестирование аппаратных и программных средств	
ПК-4 -Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем (Информационная безопасность телекоммуникационных систем)	З-1 - Характеризовать основные информационные технологии, используемые в автоматизированных системах З-2 - Характеризовать средства и способы обеспечения безопасности информации, принципы построения систем защиты информации П-1 - Иметь опыт практической разработки программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации У-1 - Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с	Лабораторные занятия Лекции Экзамен

	целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах	
ПК-5 -Способен разработать и смоделировать программно-технические средства защиты информации от несанкционированного доступа (Информационная безопасность телекоммуникационных систем)	З-1 - Различать стандарты ЕСКД, ЕСТД и ЕСПД З-10 - Характеризовать средства проектирования электронных схем З-2 - Характеризовать современные информационные технологии (операционные системы, базы данных, вычислительные сети) З-3 - Характеризовать способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах З-4 - Различать основные классы и виды уязвимостей программного обеспечения З-5 - Объяснять методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее З-6 - Характеризовать (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее З-7 - Характеризовать методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий З-8 - Характеризовать средства контроля защищенности информации от несанкционированного доступа З-9 - Характеризовать методики контроля защищенности	Лабораторные занятия Лекции Экзамен

	информации от несанкционированного доступа П-1 - Иметь опыт практической разработки технического (эскизного) проекта программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий на нее П-2 - Иметь опыт практического испытания программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий на нее П-3 - Иметь опыт практической разработки рабочей и эксплуатационной документации на техническое средство защиты У-1 - Составлять техническое задание на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее У-2 - Составлять проектно-сметную документацию на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее У-3 - Составлять программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее	

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	10,5	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрено		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– не предусмотрено		
Промежуточная аттестация по практическим/семинарским занятиям–нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0.5		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
реферат	10,15	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -1		
Промежуточная аттестация по лабораторным занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено**		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		
Текущая аттестация на онлайн-занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено		
Промежуточная аттестация по онлайн-занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено**		

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	Сроки − семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)		
№ п/п	**Содержание уровня выполнения критерия оценивания результатов**	**Шкала оценивания**

	обучения (выполненное оценочное задание)	Традиционная характеристика уровня		Качественная характеристика уровня
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Лабораторные занятия

Примерный перечень тем

1. Анализ сертифицированного СЗИ на предмет его функциональных возможностей. Построение модели типа «черный ящик» для исследуемой системы с последующей детализацией по технологии IDEF0.

2. Оценка общих критериев и определение класса защищенности автоматизированной системы.

3. Анализ СЗИ с использованием ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3 Требования доверия к безопасности Условные обозначения» на предмет оценочных уровней доверия.

LMS-платформа − не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Контрольная работа

Примерный перечень тем

1. Защищенность телекоммуникационных систем

Примерные задания

Что такое цель безопасности (security objective)?

о Совокупность функциональных возможностей всего аппаратного, программного и программно-аппаратного обеспечения ОО, которые необходимо использовать для корректной реализации ФТБ.

Требование безопасности (security requirement), то есть требование, изложенное на стандартизованном языке и направленное на достижение безопасности для объекта оценивания.

о Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и/или предположениям.

о Совокупность правил, описывающих конкретный режим безопасности, реализуемый ФБО, и выраженных в виде совокупности ФТБ.

2 Что такое Проблема безопасности (security problem)?

о Изложение, которое в формализованном виде определяет характер и масштабы безопасности, которую должен обеспечивать объект оценки (ОО).

о Изложение угроз продукту ИТ, отличному от ОО, для которого имеются свои функциональные требования, организационно скоординированные с ОО, и который, как предполагается, реализует свои функциональные требования корректно.

о Описание субъектов, пользователей (включая внешние продукты ИТ), объектов, информации, сеансов и/или ресурсов, которые используются при определении ФТБ, и значения которых используются при осуществлении ФТБ.

о Описание угроз, которым должно быть обеспечено противостояние со стороны объекта оценки; политики безопасности организации, осуществляемых ОО, и - предположений, которые определены для ОО и его среды функционирования.

3 Что такое Функциональные возможности безопасности ОО (TOE security functionality)?

о Функциональные возможности всех аппаратных и программных средств объекта оценки (ОО) по обеспечению безопасности ОО.

о Все политики функций безопасности (ПФБ), реализуемые функциями безопасности объекта (ФБО), чьи механизмы осуществляют правила, определенные в функциональных требованиях безопасности (ФТБ).

о Различные политики функций безопасности (ПФБ), определяемые ФТБ. Каждая такая ПФБ
специфицирует свою область действия, определяющую субъекты, объекты, ресурсы или
информацию и операции, по отношению к которым она применяется.
о Совокупность функциональных возможностей всего аппаратного, программного и программно-аппаратного обеспечения объекта оценки (ОО), которые необходимо использовать для корректной реализации ФТБ.
4 Что такое Уровень гарантированности?
о Полная функциональная спецификация функций безопасности объекта.
о Мера доверия, которая может быть оказана архитектуре и реализации информационной
системы;
о Описание архитектуры безопасности.
о Представление реализации функций безопасности объекта.
5 Что такое Механизмы безопасности, согласно Оранжевой книге?
о Произвольное управление доступом; безопасность повторного использования объектов;
метки безопасности; принудительное управление доступом.
о Аутентификационные данные и секреты;
о Политики функций безопасности управления доступом и информационными потоками.
о Атрибуты пользователей, ресурсов, субъектов, объектов, сеансов, данных состояния функций
безопасности объекта и операций в пределах области действия.
LMS-платформа − не предусмотрена

5.2.2. Реферат

Примерный перечень тем
1. Защищенность телекоммуникационных систем
2. Проектирование систем управления доступом к информации
3. Организация проектирования инженерно-технических и программно-аппаратных средств охраны объектов информатизации
Примерные задания
Целью подготовки реферата по дискуссионным вопросам является привитие студентам навыков самостоятельной работы над законодательными и литературными источниками, чтобы на основе их анализа и обобщения студенты могли делать собственные выводы теоретического и практического характера, обосновывая их соответствующим образом
LMS-платформа − не предусмотрена

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Экзамен

Список примерных вопросов

1. 1. Принципы информационной защиты. 2. Категории защищаемых информационных ценностей. Цели информационной защиты. 3. Модель абсолютной защиты С.П.Расторгуева и формы ее реализации при проектировании информационной защиты. 4. Стратегия пассивной защиты объектов информатизации. Рубеж сопротивления информационному вторжению и его характеристика. 5. Стратегия информационного сокрытия. 6. Стратегия ликвидации опасности. 7. Стратегия маневра. 8. Модели защиты каналов связи. 9. Проектирование комплексной информационной защиты от несанкционированного доступа. Элементы защиты и их краткая характеристика. 10. Требования к рубежу контроля за информационным вторжением. 11. Формы и методы реагирования на несанкционированный доступ. 12. Признаки и следы несанкционированного доступа к защищаемой информации в компьютерных системах. 13. Качественные и количественные подходы к оценке эффективности информационной защиты. Временные, вероятностные и затратные критерии оценки. 14. Оценка вероятности обнаружения нарушителя на рубежах контроля сложной конфигурации. 15. Классификация информационных нарушителей. «Внутренние» и «внешние» нарушители. Характеристика нарушителей с позиций их осведомленности и оснащенности. 16. Физические модели человека-нарушителя. Биомеханические и геометрические характеристики. 17. Физические модели человека-нарушителя. Физико-химические и социальные признаки. 18. Варианты несанкционированного доступа нарушителей к хранимой компьютерной информации. 19. Требования к проектированию периметровых ограждений объектов информатизации, ограждающих конструкций зданий и помещений, предназначенных для хранения и обработки конфиденциальной информации. 20. Требования к проектированию защищенных оконных проемов. Виды и характеристики оконных решеток, рольставень, защитных стекол и пленок. 21. Требования к оборудованию проходов на объекты информатизации. Двери в защищенном исполнении. Исполнительные устройства управления доступом. Шлагбаумы, турникеты и шлюзы. 22. Виды и характеристика механических и электромеханических запорных устройств. Способы защиты замковых устройств от взлома. 23. Сигнализационные датчики генераторного и параметрического типов. Характеристики чувствительных элементов сигнализационных датчиков. 24. Средства обнаружения человека-нарушителя по тепловому излучению его тела. Принцип действия инфракрасных датчиков пассивного типа. 25. Построение оптической системы и тракта обработки тревожной информации в пассивных инфракрасных датчиках. 26. Вывод количественных соотношений для построения тракта обработки сигнала в радиотехнических датчиках. 27. Радиотехнические и ультразвуковые датчики доплеровского типа. Принцип действия, построение чувствительных элементов, требования к установке на объектах информатизации. 28. Принцип действия датчиков емкостного типа. Варианты контроля чувствительных элементов внутри охраняемого помещения. 29. Сигнализационные датчики контроля остекленных поверхностей. 30. Проектирование рубежа защиты от непосредственного физического доступа к автоматизированным рабочим местам на базе персональных компьютеров. 31. Использование сигнализационных датчиков для контроля доступа к рабочему месту пользователя. Контроль за рабочим местом с использованием Web-камер. 32. Радиотехнические средства охраны периметра объекта информатизации. 33. Приемно-контрольные приборы охранной сигнализации. Классификация и основные характеристики ПКП. 34. Принципы контроля проводных шлейфов охранной и пожарной сигнализации. 35. Проводные и радиоканальные системы передачи тревожной

информации. 36. Тактические требования, предъявляемые к системам охранного телевидения. Назначение элементов системы TV-охраны. 37. Подходы к оценке эффективности средств телевизионного наблюдения. 38. Классификация систем управления физическим и логическим доступом на объекты информатизации. Термины и определения. Специальные режимы доступа. 39. Способы представления и хранения аутентифицирующей информации. Удаленная аутентификация с нулевой передачей знаний. 40. Биометрическая аутентификация по статическим признакам. Принципы распознавания человека по дактилоскопическому узору пальцев и форме руки. 41. Биометрическая аутентификация по статическим признакам. Принципы распознавания человека по радужной оболочке и сетчатке глаза. Распознавание по признакам внешности и тепловой «карте» лица. 42. Биометрическая аутентификация по динамическим признакам. Принципы распознавания говорящего по голосу, рукописному и клавиатурному почерку. 43. Физические носители ключевой информации контактного считывания: формы реализации, характеристики, достоинства и недостатки. 44. Общее устройство и характеристики смарт-карт. 45. Бесконтактные носители аутентифицирующей информации: принципы построения и характеристики. 46. Понятия о физических принципах и стойкости запечатления компьютерной информации на внешних машинных носителях. Программные способы гарантированного уничтожения компьютерной информации на магнитных носителях. 47. Аппаратные средства мгновенного размагничивания магнитных носителей. Уничтожение машинных носителей. 48. Существующие программно-аппаратные способы реставрации удаленной компьютерной информации на магнитных носителях. 49. Регламентация порядка обращения с машинными носителями конфиденциальной информации.

LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	**Контрольно-оценочные мероприятия**
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ОПК-9	У-2	Контрольная работа Лабораторные занятия Лекции Реферат Экзамен