Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

Институт информационных технологий и радиоэлектроники

Кафедра информатики и защиты информации

Основание: решение кафедры ИЗИ
от «28» 12 2016 года.

Зав. кафедрой ИЗИ _____ М.Ю. Монахов

Фонд оценочных средств
для текущего контроля и промежуточной аттестации
при изучении учебной дисциплины
«Методы и средства защиты объектов информатизации»

Направление подготовки: 10.04.01 «информационная безопасность»

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Владимир, 2016

1. Паспорт фонда оценочных средств

Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации при изучении учебной дисциплины «Методы и средства защиты объектов информатизации» разработан в соответствие с рабочей программой, входящей в ОПОП направления подготовки 10.04.01 «информационная безопасность».

№ п/п	Контролируемые разделы (темы) дисциплины	Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Общая классификация технических средств обеспечения информационной безопасности	2	ПК-10, ПК-14, ПК-15, ПК-16	Контрольные вопросы и задания
2	Внедрение ТС проектирование, , монтаж ТС, пуско-наладочные работы).	2	ПК-10, ПК-14, ПК-15, ПК-16	Контрольные вопросы и задания
3	Технические средства предотвращения утечки информации по техническим каналам.	2	ПК-10, ПК-14, ПК-15, ПК-16	Контрольные вопросы и задания
4	Технические средства недопущения НСД.	2	ПК-10, ПК-14, ПК-15, ПК-16	Контрольные вопросы и задания
5	Технические средства СКУД.	2	ПК-10, ПК-14, ПК-15, ПК-16	Контрольные вопросы и задания
6	Технические средства СВН.	2	ПК-10, ПК-14, ПК-15, ПК-16	Контрольные вопросы и задания
7	Основы организации службы защиты информации на объекте, ее основные и вспомогательные функции.	2	ПК-10, ПК-14, ПК-15, ПК-16	Контрольные вопросы и задания
8	Защита информации в электронных банковских и платежных системах.	2	ПК-10, ПК-14, ПК-15, ПК-16	Контрольные вопросы и задания
9	Аттестация объектов информатизации и выделенных помещений. Проведение специальных проверок и специальных обследований.	2	ПК-10, ПК-14, ПК-15, ПК-16	Контрольные вопросы и задания

Комплект оценочных средств по дисциплине «Методы и средства защиты объектов информатизации» предназначен для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям образовательной программы, в том числе рабочей программы дисциплины «Методы и средства защиты объектов информатизации», для оценивания результатов обучения: знаний, умений, навыков и уровня приобретенных компетенций.

Комплект оценочных средств по дисциплине «Методы и средства защиты объектов информатизации» включает:

2 семестр

1. Оценочные средства для проведения текущего контроля успеваемости:

- комплект вопросов рейтинг-контроля, позволяющих оценивать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, распознавание объектов изучения в рамках определенного раздела дисциплины;

- комплект вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ, позволяющих оценивать знание фактического материала и умение использовать теоретические знания при решении практических задач.

- комплект вопросов для контроля самостоятельной работы обучающихся при выполнении заданий по СРС, позволяющих оценивать знание фактического материала и умение использовать теоретические знания при решении практических задач.

2. Оценочные средства для проведения промежуточной аттестации в форме контрольных вопросов для проведения экзамена, позволяющие провести процедуру измерения уровня знаний и умений обучающихся.

2. Перечень компетенций, формируемых в процессе изучения дисциплины «Методы и средства защиты объектов информатизации» при освоении образовательной программы по направлению подготовки 10.04.01 «информационная безопасность»

Перечень компетенций содержится в разделе 3 Рабочей программы дисциплины «Компетенции обучающегося, формируемые в результате освоения дисциплины»:

ПК-10 - способностью проводить аттестацию объектов информатизации по требованиям безопасности информации;		
Знать	Уметь	Владеть
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации	- пользоваться научно- технической и справочной литературой для решения прикладных задач; осуществлять поиск информации в Интернет и выполнять аналитического исследования по определенной теме - квалифицированно применять имеющийся математический аппарат; использовать математические методы и модели для решения прикладных задач; применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности - организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов - анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации	- навыками работы с нормативными правовыми актами; методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методами анализа и формализации информационных процессов объекта и связей между ними; профессиональной терминологией; навыками безопасного использования технических средств в профессиональной деятельности - методами технической защиты информации -методами формирования требований по защите информации -методами расчета и инструментального контроля показателей технической защиты информации

ПК-14 – способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;		
Знать	Уметь	Владеть
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации - принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом,	- пользоваться научно-технической и справочной литературой для решения прикладных задач; осуществлять поиск информации в Интернет и выполнять аналитического исследования по определенной теме - организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных	- навыками работы с нормативными правовыми актами; методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методами анализа и формализации информационных процессов объекта и связей между ними; профессиональной терминологией; навыками безопасного использования технических средств в профессиональной деятельности - методами технической защиты информации

охранного телевидения - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации	документов - анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации - формировать комплекс мер по информационной безопасности с учетом его технической обоснованности и реализуемости	- методами формирования требований по защите информации -методами расчета и инструментального контроля показателей технической защиты информации

ПК 15 – способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;		
Знать	Уметь	Владеть
- принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации	- квалифицированно применять имеющийся математический аппарат; использовать математические методы и модели для решения прикладных задач; применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности - анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации - формировать комплекс мер по информационной безопасности с учетом его технической обоснованности и реализуемости	- навыками работы с нормативными правовыми актами; методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методами анализа и формализации информационных процессов объекта и связей между ними; профессиональной терминологией; навыками безопасного использования технических средств в профессиональной деятельности - методами и средствами выявления угроз безопасности автоматизированным системам - методами технической защиты информации -методами расчета и инструментального контроля показателей технической защиты информации - методами использования сетевых ресурсов с целью организации интерактивного взаимодействия

ПК-16 – способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.		
Знать	Уметь	Владеть
- принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам,	- пользоваться научно-технической и справочной литературой для решения прикладных задач; осуществлять поиск информации в Интернет и выполнять аналитического исследования по определенной теме - анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации - формировать комплекс мер по	- навыками работы с нормативными правовыми актами; методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методами анализа и формализации информационных процессов объекта и связей между ними; профессиональной терминологией; навыками безопасного использования технических средств в профессиональной деятельности - методами и средствами выявления угроз безопасности автоматизированным системам

методы и средства контроля эффективности технической защиты информации	информационной безопасности с учетом его технической обоснованности и реализуемости	- методами формирования требований по защите информации - методами использования сетевых ресурсов с целью организации интерактивного взаимодействия

Оценка по дисциплине выставляется с учетом среднего балла освоения компетенций, формируемых дисциплиной, при условии сформированности каждой компетенции не ниже порогового уровня.

3. Показатели, критерии и шкала оценивания компетенций текущего контроля знаний по учебной дисциплине «Методы и средства защиты объектов информатизации»

Текущий контроль знаний, согласно «Положению о рейтинговой системе комплексной оценки знаний студентов в ВлГУ» (далее Положение) в рамках изучения дисциплины «Методы и средства защиты объектов информатизации» предполагает письменный рейтинг-контроль, выполнение и защиту лабораторных, а также выполнение самостоятельных работ. В случае использования при изучении дисциплины дистанционных образовательных технологий проводится компьютерное тестирование.

Регламент проведения письменного рейтинг-контроля

№	Вид работы	Продолжительность
1	Предел длительности рейтинг-контроля	35-40 мин.
2	Внесение исправлений	до 5 мин.
	Итого	до 45 мин.

Критерии оценки письменного рейтинг-контроля

Результаты каждого письменного рейтинга оцениваются в баллах. Максимальная сумма, набираемая студентом на каждом письменном рейтинге, составляет 10 баллов.

Критерии оценки для письменного рейтинга:

- 9-10 баллов выставляется обучающемуся, если соблюдаются критерии: полное раскрытие темы, вопроса, указание точных названий и определений, правильная формулировка понятий и категорий, приведение формул и (в необходимых случаях) их вывода, приведение статистики, самостоятельность ответа, использование дополнительной литературы;

- 7-8 баллов выставляется обучающемуся, если соблюдаются критерии: недостаточно полное раскрытие темы, несущественные ошибки в определении понятий и категорий, формулах, выводе формул, статистических данных, кардинально не меняющих суть изложения, наличие грамматических и стилистических ошибок, использование устаревшей учебной литературы;

- 5-6 баллов выставляется обучающемуся, если соблюдаются критерии: отражение лишь общего направления изложения лекционного материала и материала современных учебников, наличие достаточно количества несущественных или одной-двух существенных ошибок в определении понятий и категорий, формулах, их выводе, статистических данных, наличие грамматических и стилистических ошибок, использование устаревшей учебной литературы, неспособность осветить проблематику дисциплины;

- 1-4 балла выставляется обучающемуся, если соблюдаются критерии: нераскрытые темы; большое количество существенных ошибок, наличие грамматических и стилистических ошибок, отсутствие необходимых умений и навыков.

Оценочные средства для текущего контроля знаний по учебной дисциплине «Методы и средства защиты объектов информатизации» (письменный рейтинг-контроль)

2 семестр:

Перечень вопросов для текущего контроля (письменный рейтинг №1):

- Дайте классификацию акустоэлектрических преобразователей.
- Принцип действия электромагнитных, электродинамических и магнитострикционных акустоэлектрических преобразователей.
- Принцип действия емкостных акустоэлектрических преобразователей.
- Принцип действия пьезоэлектрических акустоэлектрических преобразователей.
- Классификация каналов утечки информации.
- Физическая сущность и основные свойства оптического канала утечки информации.
- Физическая сущность акустического канала утечки информации.
- Физическая сущность радиоэлектронного канала утечки информации.
- Физическая сущность акустооптического канала утечки информации.
- Физическая сущность акусто-вибрационного канала утечки информации.
- Классификация методов защиты от утечки по техническим каналам.
- Технические мероприятия по защите информации с помощью пассивных технических средств.
- Технические мероприятия по защите информации с помощью активных технических средств.
- Электростатическое экранирование технических средств.
- Магнитостатическое экранирование технических средств.
- Электромагнитное экранирование технических средств.
- Заземление технических средств.
- Развязывание информационных сигналов .
- Фильтрация информационных сигналов.
- Пространственное зашумление.
- Линейное зашумление.
- Пассивные методы защиты акустической (речевой) информации.
- Активные методы защиты акустической (речевой) информации.
- Защита телефонных линий методами синфазной маскирующей низкочастотной (НЧ) помехи и высокочастотной маскирующей помехи.
- Защита телефонных линий методами ультразвуковой маскирующей помехи и повышения напряжения.
- Защита телефонных линий методами "обнуления" и низкочастотной маскирующей помехи.
- Защита телефонных линий компенсационным методом и методом "выжигания".
- Какие бывают категории (группы объектов), какие объекты к какой категории относятся?
- Основные требования по технической укрепленности периметров охраняемых территорий.

Перечень вопросов для текущего контроля (письменный рейтинг №2):

- Какие существуют категории объектов и какие объекты относятся к группе Б1?
- Какие существуют категории объектов и какие объекты относятся к группе А1?
- Какие существуют категории объектов и какие объекты относятся к группе А2?

- Что является рубежом охраны? Сколько есть рубежей охраны, что они защищают и какие извещатели используются в рубежах охраны?
- Что защищает 1 рубеж охраны? Какие извещатели используются в 1 рубеже охраны, какие строительные конструкции и каким образом они защищают, как устанавливаются?
- Что защищает 2 рубеж охраны? Какие извещатели используются во 2 рубеже охраны, что и каким образом они защищают, как устанавливаются?
- Что защищает 3 рубеж охраны? Какие извещатели используются в 3 рубеже охраны, что и каким образом они защищают, как устанавливаются?
- Классификация охранных извещателей.
- Какие бывают извещатели для защиты окон на разбитие? Каким образом они защищают окна, как устанавливаются, приведите примеры.
- Какие бывают извещатели для защиты окон и дверей на открытие? Каким образом они устанавливаются, приведите примеры.
- Классификация приемно-контрольных приборов.
- Классификация СПИ. Приведите примеры разных типов СПИ.
- Задачи технической эксплуатации ТСО.
- Составные части технической эксплуатации ТСО.
- Назначение параметра «время на вход» для шлейфа сигнализации.

Перечень вопросов для текущего контроля (письменный рейтинг №3):

- Классификация идентификаторов по физическому принципу действия.
- Идентификация на основе проксимити карт.
- Идентификация с использованием штрихкодов.
- Идентификация с использованием карт Виганда.
- Идентификация с использованием магнитных карт.
- Идентификация с использованием смарт-карт.
- Идентификация с использованием электронных таблеток Touch Memory.
- Квазидинамические и статические биометрические признаки.
- Связанные точки доступа СКУД.
- Основные технические характеристики СКУД.
- Исполнительные устройства СКУД.
- Преграждающие устройства СКУД.
- Основные технические характеристики видеокамер.
- Классификация видеокамер.
- Основные технические характеристики объективов видеокамер.
- Общая структурная схема видеокамеры, назначение составных частей.
- Какова цель задачи обнаружения в системах охранного телевидения?
- Какова цель задачи различения в системах охранного телевидения?
- Какова цель задачи идентификации в системах охранного телевидения?
- Каково назначение диафрагмы. Какие существуют способы управления диафрагмой?
- Дайте определение и поясните физический смысл понятия разрешающей способности видеокамеры.
- Что такое гамма-коррекция видеокамеры?
- Дайте определение и поясните физический смысл понятия чувствительности видеокамеры.
- Основные технические характеристики объективов видеокамер.
- Дайте определение и поясните физический смысл понятия фокусного расстояния и апертуры объектива.
- Понятие геометрической (сферической) и хроматической аберрации объектива.
- Классификация объективов по способу управления диафрагмой объектива.
- Классификация объективов по фокусному расстоянию и углу обзора.

- Какие существуют объективы по способу крепления к камере?
- Общие стандарты беспроводных сетей (Bluetooth, WiFi, сотовой связи).
- Стандарты беспроводных сетей WiFi.
- Стандарты сетей сотовой связи.
- Способы осуществления атак на сети Bluetooth.
- Механизмы защиты сетей Bluetooth.
- Способы осуществления атак на сети WiFi.
- Механизмы защиты сетей WiFi.
- Способы осуществления атак на сети сотовой связи.
- Механизмы защиты сетей сотовой связи.
- Основные требования по защите банкоматов и платежных терминалов.
- Способы осуществления атак и взломов банкоматов и платежных терминалов.
- Нормативное обеспечение аттестации объектов информатизации и выделенных помещений;
- Порядок проведения аттестации объектов информатизации и выделенных помещений;
- Документация, составляемая по итогам проведения аттестации объектов информатизации и выделенных помещений;
- Проведение специальных проверок объектов информатизации и выделенных помещений;
- Проведение специальных обследований объектов информатизации и выделенных помещений;
- Проведение категорирования объектов информатизации и выделенных помещений;
- Проведение категорирования информационных систем.

Регламент проведения лабораторных работ

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Методы и средства защиты объектов информатизации» предполагается выполнение лабораторных работ, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

Критерии оценки выполнения лабораторных работ

Результаты выполнения каждой лабораторной работы оцениваются в баллах. Максимальная сумма, набираемая студентом за выполнение каждой лабораторной работы, составляет 2 балла.

Критерии оценки для выполнения лабораторной работы:

- 1,5-2 балла выставляется обучающемуся, если соблюдаются критерии: представлен полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения и надлежащим образом оформленный (в печатном или электронном виде - в соответствие с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся верно и полно ответил на все контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно и в определенный преподавателем срок;

- 0,9-1,4 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствие с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся преимущественно верно и полно ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно, возможно, с нарушением

определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки;

- 0,5-0,8 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание не всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствие с требованием преподавателя), в основном выполнено задание на лабораторную работу, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с отражением лишь общего направления изложения материала, с наличием достаточно количества несущественных или одной-двух существенных ошибок, лабораторная работа выполнена самостоятельно, с нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература;

- 0,1-0,4 балла выставляется обучающемуся, если соблюдаются критерии: письменный отчет по лабораторной работе (в печатном или электронном виде - в соответствие с требованием преподавателя) не представлен или представлен неполный, отчет содержит описание не всех этапов выполнения работы, имеет погрешности в оформлении, задание на лабораторную работу выполнено не полностью, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с большим количеством существенных ошибок, продемонстрировал неспособность осветить проблематику лабораторной работы, лабораторная работа выполнена несамостоятельно, с существенным нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература, обучающийся при выполнении работы продемонстрировал отсутствие необходимых умений и практических навыков.

При оценке за лабораторную работу менее 0,1 балла, данная работа считается невыполненной и не зачитывается. При невыполнении лабораторной работы хотя бы по одной из изучаемых тем, обучающийся не получает положительную оценку при промежуточном контроле по дисциплине (экзамен).

Оценочные средства для текущего контроля знаний по учебной дисциплине «Методы и средства защиты объектов информатизации» (лабораторные работы)

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ (2 семестр):

Лабораторная работа №1 Организация и проведение обследования объектов на предмет состояния инженерно-технического укрепления

-Что такое инженерно-техническое укрепление?

-Что подразумевается под обследованием объектов на предмет состояния инженерно-технического укрепления?

-Как организуется обследование объектов на предмет состояния инженерно-технического укрепления?

-Как проводится обследование объектов на предмет состояния инженерно-технического укрепления?

Лабораторная работа №2 Проектирование охранно-тревожной сигнализации объектов на основе оборудования интегрированной системы безопасности (ИСБ) «Орион» НВП «Болид»

-Что такое интегрированная система безопасности?

-Какое оборудование имеется у интегрированной системы безопасности (ИСБ) «Орион» НВП «Болид»?
-Что такое охранно-тревожная сигнализация объектов?
-Каким образом проектируется охранно-тревожная сигнализация объектов?
Лабораторная работа №3 Программирование аппаратуры безопасности (ИСБ) «Орион» НВП «Болид»
-Что такое ИСБ?
-Что такое аппаратура безопасности (ИСБ)?
-Приведите примеры аппаратуры безопасности (ИСБ)?
-Каким образом производится программирование аппаратуры безопасности (ИСБ)?
Лабораторная работа №4 Изучение программного обеспечения АРМ ИСБ «Орион-Pro»
-Чем занимается АРМ ИСБ «Орион-Pro»?
-Что такое программное обеспечение?
-Приведите классификацию программного обеспечения.
-Какое программное обеспечение имеется у АРМ ИСБ «Орион-Pro»?
Лабораторная работа №5. Проектирование охранно-тревожной сигнализации объектов на основе радиоканального оборудования ВОРС «Стрелец»
-Чем занимается ВОРС «Стрелец»?
-Что такое радиоканальное оборудование?
-Какое радиоканальное оборудование имеется у ВОРС «Стрелец»?
-Что такое охранно-тревожная сигнализация объектов?
-Каким образом проектируется охранно-тревожная сигнализация объектов?
Лабораторная работа №6. Программирование оборудования ВОРС «Стрелец» утилитой «WirelEx»
-Что такое утилита?
-Чем занимается ВОРС «Стрелец»?
-Какое оборудование имеется у ВОРС «Стрелец»?
-Каким образом программируется оборудование?

Регламент проведения самостоятельной работы

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Методы и средства защиты объектов информатизации» предполагается выполнение заданий СРС, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

Критерии оценки выполнения самостоятельной работы

Результаты выполнения самостоятельной работы оцениваются в баллах. Максимальная сумма, набираемая студентом за выполнение работы по каждой теме, составляет 1 балл.

Критерии оценки для выполнения работы:

- 0,9-1 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся верно и полно ответил на все контрольные вопросы преподавателя по теме; полностью, самостоятельно и в определенный преподавателем срок выполнено задание;

- 0,7- 0,8 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся преимущественно верно и полно ответил на контрольные вопросы преподавателя по теме; задание выполнено самостоятельно, возможно, с нарушением определенного преподавателем срока;

- 0,5-0,6 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся ответил на контрольные вопросы преподавателя по теме с отражением лишь общего направления изложения материала; задание выполнено самостоятельно, возможно, с нарушением определенного преподавателем срока, содержит незначительные ошибки;

- 0,1-0,4 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся ответил на контрольные вопросы преподавателя по теме с большим количеством существенных ошибок, продемонстрировал неспособность осветить проблематику темы; задание выполнено не полностью, не самостоятельно, с существенным нарушением определенного преподавателем срока, при выполнении задания продемонстрировал отсутствие необходимых умений и практических навыков.

Оценочные средства для текущего контроля знаний по учебной дисциплине «Методы и средства защиты объектов информатизации» (самостоятельная работа)

2 семестр:

№ пп	Раздел (тема) дисциплины	Виды СРС	Формы контроля СРС	Баллы по СРС
1	Общая классификация технических средств обеспечения информационной безопасности	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
2	Внедрение ТС проектирование, , монтаж ТС, пуско-наладочные работы).	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
3	Технические средства предотвращения утечки информации по техническим каналам.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
4	Технические средства недопущения НСД.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
5	Технические средства СКУД.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
6	Технические средства СВН.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
7	Основы организации службы защиты информации на объекте, ее основные и вспомогательные функции.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
8	Защита информации в электронных банковских и платежных системах.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
9	Аттестация объектов информатизации и выделенных помещений. Проведение специальных проверок и специальных обследований.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
			Итого за семестр:	9

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении СРС (2 семестр):

- Общая классификация технических средств обеспечения информационной безопасности, защиты информации, охраны и безопасности.
- Внедрение ТС (предпроектное обследование, проектирование, составление сметной документации, монтаж ТС, пуско-наладочные работы).
- Эксплуатационно-техническое обслуживание ТС (плановое и внеплановое обслуживание, периодичность и объем обслуживания, контроль ЭТО, ведение э/технической документации). Ремонты ТС (гарантии, обменный фонд и др.).
- Плановые замены ТС (сроки эксплуатации и сертификации).

- Обучение и профподготовка кадров.
- Ложные срабатывания ТС. Обследование объектов и технический надзор.
- Акустоэлектрические преобразования.
- Утечка информации по каналам связи. Понятия ОТСС и ВТСС.
- Пассивные ТС защиты (маскировка, экранирование, заземление, фильтрация и др.). Активные ТС защиты (линейное и пространственное зашумление, средства подавления диктофонов, защиты линий связи).
- Оборудование нелегального съема информации (телефонные закладки и их классификация, микрофоны, средства видеонаблюдения, комплексы радиоконтроля).
- Оборудование поиска закладных устройств (индикаторы поля, радиосканеры, интерсепторы, анализаторы спектра и частотомеры, комплексы радиоконтроля, нелинейные локаторы, оборудование защиты проводных линий, средства поиска диктофонов и видеокамер, радиолоаторы и пеленгаторы и т.д.).
- Требования по обеспечению инженерно-технического укрепления объектов.
- Классификация типов защиты ИТУ объектов по классам защиты.
- Классификация извещателей, СП и оповещателей.
- СПИ (принцип действия, ТТД, способ применения и эксплуатации).
- Понятия ИСБ.
- Тактика охраны объектов (основные понятия).
- Технические средства недопущения Н.С.Д. на объекты и в помещения.
- Виды считывателей и идентификаторов.
- Биометрическая идентификация. Типы исполнительных устройств. Типы заграждающих устройств.
- Технические средства СВН.
- Мультиплексоры, коммутаторы, видеорегистраторы, назначение и основные ТТД. Способы передачи видеосигнала.
- Основы организации службы защиты информации на объекте, ее основные и вспомогательные функции.
- Организация постов и маршрутов. Дисклокация нарядов, обеспечение средствами связи, специальными средствами, средствами активной обороны, вооружением.
- Контроль за несением службы. Технические средства контроля за несением службы.
- Обеспечение контрольно-пропускного и объектового режимов. Правила и порядок проведения досмотра.
- Защита информации в беспроводных сетях WiFi. Физические принципы функционирования. Стандарты. Способы осуществления атак.
- Методы защиты WiFi сетей. Защита информации в мобильных устройствах сотовой связи. Физические принципы функционирования. Стандарты.
- Защита информации в электронных банковских и платежных системах.
- Защита банкоматов и платежных терминалов. Способы осуществления атак и взломов. Методы защиты.
- Аттестация объектов информатизации и выделенных помещений. Проведение специальных проверок и специальных обследований.
- Специальные исследования акустических и виброакустических каналов. Специальные исследования ПЭМИН.
- Технический контроль эффективности мер по организации защиты информации от утечек по техническим каналам. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИН.
- Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.

- Методы контроля побочных электромагнитных излучений генераторов технических средств.
- Контроль технических средств и систем на соответствие установленным нормам на параметры в речевом диапазоне частот

Общее распределение баллов текущего контроля по видам учебных работ для студентов (в соответствие с Положением)

2 семестр

№	Пункт	Максимальное число баллов
1	Письменный рейтинг-контроль 1	10
2	Письменный рейтинг-контроль 2	10
3	Письменный рейтинг-контроль 3	10
4	Посещение занятий студентом	5
5	Дополнительные баллы (бонусы)	4
6	Лабораторные работы	12
7	Выполнение семестрового плана самостоятельной работы	9
8	Экзамен	40
	Всего	100

4. Показатели, критерии и шкала оценивания компетенций промежуточной аттестации знаний по учебной дисциплине «Методы и средства защиты объектов информатизации»

Регламент проведения промежуточного контроля (экзамена)

Промежуточная аттестация по итогам освоения дисциплины (экзамен) проводится в экзаменационную сессию. Экзамен проводится по билетам, содержащим три вопроса. Студент пишет ответы на вопросы экзаменационного билета на листах белой бумаги формата А4, на каждом из которых должны быть указаны: фамилия, имя отчество студента; шифр студенческой группы; дата проведения экзамена; номер экзаменационного билета. Листы должны быть подписаны и студентом и экзаменатором после получения студентом экзаменационного билета. Экзаменационные билеты должны быть оформлены в соответствие с утвержденным регламентом.

После подготовки студент устно отвечает на вопросы билета и уточняющие вопросы экзаменатора. Экзаменатор вправе задать студенту дополнительные вопросы и задания по материалам дисциплины для выявления степени усвоения студентом компетенций.

Максимальное количество баллов, которое студент может получить на экзамене, в соответствие с Положением составляет 40 баллов.

Критерии оценивания компетенций на экзамене

Оценка в баллах	**Оценка за ответ на экзамене**	**Критерии оценивания компетенций**
30 - 40	«Отлично»	Студент глубоко и прочно усвоил программный материал,

		исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, использует при ответе материалы из основной и дополнительной литературы по дисциплине, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач, подтверждает полное освоение компетенций, предусмотренных рабочей программой дисциплины.
20 - 29	«Хорошо»	Студент показывает твердое знание материала, грамотно и по существу излагает его, не допускает существенных неточностей при ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, допуская некоторые неточности; демонстрирует хороший уровень освоения материала, информационной и коммуникативной культуры и в целом подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины.
10 - 19	«Удовлетворительно»	Студент показывает знания только основного материала, но не усвоил его деталей; допускает неточности, недостаточно правильные формулировки, которые в целом не препятствуют усвоению последующего программного материала; допускает нарушения логической последовательности в изложении программного материала; испытывает затруднения при выполнении практических работ; подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины, на минимально допустимом уровне.
0 - 10	«Неудовлетворительно»	Студент не знает значительной части программного материала, имеет менее 50% правильно выполненных заданий от общего объема работы, допускает существенные ошибки при изложении материала, неуверенно, с большими затруднениями выполняет практические работы, не подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины.

Оценочные средства для промежуточной аттестации по учебной дисциплине «Методы и средства защиты объектов информатизации» (экзамен)

Перечень вопросов для промежуточного контроля (экзамена)

2 семестр:

1. Дайте классификацию акустоэлектрических преобразователей.
2. Принцип действия электромагнитных, электродинамических и магнитострикционных акустоэлектрических преобразователей.
3. Принцип действия емкостных акустоэлектрических преобразователей.
4. Принцип действия пьезоэлектрических акустоэлектрических преобразователей.
5. Классификация каналов утечки информации.
6. Физическая сущность и основные свойства оптического канала утечки информации.
7. Физическая сущность акустического канала утечки информации.
8. Физическая сущность радиоэлектронного канала утечки информации.
9. Физическая сущность акустооптического канала утечки информации.
10. Физическая сущность акусто-вибрационного канала утечки информации.

11. Классификация методов защиты от утечки по техническим каналам.
12. Технические мероприятия по защите информации с помощью пассивных технических средств.
13. Технические мероприятия по защите информации с помощью активных технических средств.
14. Электростатическое экранирование технических средств.
15. Магнитостатическое экранирование технических средств.
16. Электромагнитное экранирование технических средств.
17. Заземление технических средств.
18. Развязывание информационных сигналов.
19. Фильтрация информационных сигналов.
20. Пространственное зашумление.
21. Линейное зашумление.
22. Пассивные методы защиты акустической (речевой) информации.
23. Активные методы защиты акустической (речевой) информации.
24. Защита телефонных линий методами синфазной маскирующей низкочастотной (НЧ) помехи и высокочастотной маскирующей помехи.
25. Защита телефонных линий методами ультразвуковой маскирующей помехи и повышения напряжения.
26. Защита телефонных линий методами "обнуления" и низкочастотной маскирующей помехи.
27. Защита телефонных линий компенсационным методом и методом "выжигания".
28. Какие бывают категории (группы объектов), какие объекты к какой категории относятся?
29. Основные требования по технической укрепленности периметров охраняемых территорий.
30. Какие существуют категории объектов и какие объекты относятся к группе Б1?
31. Какие существуют категории объектов и какие объекты относятся к группе А1?
32. Какие существуют категории объектов и какие объекты относятся к группе А2?
33. Что является рубежом охраны? Сколько есть рубежей охраны, что они защищают и какие извещатели используются в рубежах охраны?
34. Что защищает 1 рубеж охраны? Какие извещатели используются в 1 рубеже охраны, какие строительные конструкции и каким образом они защищают, как устанавливаются?
35. Что защищает 2 рубеж охраны? Какие извещатели используются во 2 рубеже охраны, что и каким образом они защищают, как устанавливаются?
36. Что защищает 3 рубеж охраны? Какие извещатели используются в 3 рубеже охраны, что и каким образом они защищают, как устанавливаются?
37. Классификация охранных извещателей.
38. Какие бывают извещатели для защиты окон на разбитие? Каким образом они защищают окна, как устанавливаются, приведите примеры.
39. Какие бывают извещатели для защиты окон и дверей на открытие? Каким образом они устанавливаются, приведите примеры.
40. Классификация приемно-контрольных приборов.
41. Классификация СПИ. Приведите примеры разных типов СПИ.
42. Задачи технической эксплуатации ТСО.
43. Составные части технической эксплуатации ТСО.
44. Назначение параметра «время на вход» для шлейфа сигнализации.
45. Что такое «тихая тревога»?
46. Что такое тревога «по принуждению»?
47. Что такое самовосстанавливающиеся шлейфы сигнализации?
48. Какие шлейфы сигнализации называются самовосстанавливающимися?
49. Каковы основные причины ложных срабатываний ТСО?

50. Какие существуют виды обследования объектов?
51. Что проверяется при обследовании состояния ТСО объекта?
52. Классификация идентификаторов по физическому принципу действия.
53. Идентификация на основе проксимити карт.
54. Идентификация с использованием штрихкодов.
55. Идентификация с использованием карт Виганда.
56. Идентификация с использованием магнитных карт.
57. Идентификация с использованием смарт-карт.
58. Идентификация с использованием электронных таблеток Touch Memory.
59. Квазидинамические и статические биометрические признаки.
60. Связанные точки доступа СКУД.
61. Основные технические характеристики СКУД.
62. Исполнительные устройства СКУД.
63. Преграждающие устройства СКУД.
64. Основные технические характеристики видеокамер.
65. Классификация видеокамер.
66. Основные технические характеристики объективов видеокамер.
67. Общая структурная схема видеокамеры, назначение составных частей.
68. Какова цель задачи обнаружения в системах охранного телевидения?
69. Какова цель задачи различения в системах охранного телевидения?
70. Какова цель задачи идентификации в системах охранного телевидения?
71. Каково назначение диафрагмы. Какие существуют способы управления диафрагмой?
72. Дайте определение и поясните физический смысл понятия разрешающей способности видеокамеры.
73. Что такое гамма-коррекция видеокамеры?
74. Дайте определение и поясните физический смысл понятия чувствительности видеокамеры.
75. Основные технические характеристики объективов видеокамер.
76. Дайте определение и поясните физический смысл понятия фокусного расстояния и апертуры объектива.
77. Понятие геометрической (сферической) и хроматической аберрации объектива.
78. Классификация объективов по способу управления диафрагмой объектива.
79. Классификация объективов по фокусному расстоянию и углу обзора.
80. Какие существуют объективы по способу крепления к камере?
81. Общие стандарты беспроводных сетей (Bluetooth, WiFi, сотовой связи).
82. Стандарты беспроводных сетей WiFi.
83. Стандарты сетей сотовой связи.
84. Способы осуществления атак на сети Bluetooth.
85. Механизмы защиты сетей Bluetooth.
86. Способы осуществления атак на сети WiFi.
87. Механизмы защиты сетей WiFi.
88. Способы осуществления атак на сети сотовой связи.
89. Механизмы защиты сетей сотовой связи.
90. Основные требования по защите банкоматов и платежных терминалов.
91. Способы осуществления атак и взломов банкоматов и платежных терминалов.
92. Нормативное обеспечение аттестации объектов информатизации и выделенных помещений;
93. Порядок проведения аттестации объектов информатизации и выделенных помещений;
94. Документация составляемая по итогам проведения аттестации объектов информатизации и выделенных помещений;
95. Проведение специальных проверок объектов информатизации и выделенных помещений;

96. Проведение специальных обследований объектов информатизации и выделенных помещений;
97. Проведение категорирования объектов информатизации и выделенных помещений;
98. Проведение категорирования информационных систем.