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
«Защищенные информационные системы»

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 «Защищенные информационные системы» 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	Информационные технологии и информационные системы. Примеры информационных технологий и информационных систем	2	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
2	Проектирование и разработка защищенных информационных технологий	2	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
3	Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».	2	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
4	Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	2	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
5	Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты.	2	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
6	Классы в системе общих критериев. Классы защищенности в системе общих критериев. Понятие аудита политики безопасности.	2	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
7	Гарантии безопасности компьютерных систем в системе общих критериев. Понятие гарантии безопасности. Уровни гарантий.	2	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
8	Каналы утечки и их анализ в системе общих критериев. Виды каналов утечки информации.	2	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
9	Безопасное функционирование в системе общих критериев. Управление конфигурацией.	2	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
10	Основные угрозы безопасности информации в компьютерных системах.	3	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
11	Модель угроз. Анализ критичных технологий. Требования, предъявляемые к разработке модели угроз.	3	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
12	Государственная политика в области безопасности компьютерных систем. Система лицензирования и сертификации средств защиты.	3	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
13	Разработка политик безопасности для защищенных компьютерных систем. Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности.	3	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
14	Порядок аттестации защищенных компьютерных систем. Понятие аттестации защищенных компьютерных систем.	3	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
15	Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.	3	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
16	Порядок внедрения SLM-системы. Service	3	ПК-2, ПК-7, ПК-9	Контрольные

	Desk — цели, возможности, реализации. Microsoft Operations Framework (MOF).			вопросы и задания
17	Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС, техническое задание, эскизный проект, технический проект, рабочая документация	3	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания
18	Методы и методики оценки качества ЗИС. Требования к эксплуатационной документации ЗИС. Порядок приемки защищенных ЗИС	3	ПК-2, ПК-7, ПК-9	Контрольные вопросы и задания

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

Комплект оценочных средств по дисциплине «Защищенные информационные системы» 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: контрольные вопросы для проведения зачета, позволяющие провести процедуру измерения уровня знаний и умений обучающихся.

3 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: контрольные вопросы для проведения экзамена, позволяющие провести процедуру измерения уровня знаний и умений обучающихся.

2. Перечень компетенций, формируемых в процессе изучения дисциплины «Защищенные информационные системы» 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-2 – способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;		
Знать	Уметь	Владеть
- основные понятия теории защиты информации в объеме, необходимом для использования и анализа сервисов информационной безопасности, основные модели доступа к информации; - основные виды информационных атак и дестабилизирующих информационных воздействий; - типовые состав ЗИС, их методы функционирования и проектирования; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - методы концептуального проектирования технологий обеспечения информационной безопасности	- ставить и решать типовые задачи в области анализа безопасности информационных потоков в распределенной информационной системе; - подбирать и использовать адекватные методы и средства защиты информации; - оценивать эффективность методов защиты информационных процессов; - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; - организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности	- навыками применения теоретического аппарата защиты информации к текущим реальным ситуациям; - навыками обнаружения уязвимостей в распределенных информационных системах и программных комплексах; - навыками управления информационной безопасностью простых объектов

ПК-7 – способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;		
Знать	Уметь	Владеть
- основные понятия теории защиты информации в объеме, необходимом для использования и анализа сервисов информационной безопасности, основные модели доступа к информации; - основные виды информационных атак и дестабилизирующих информационных воздействий; - типовые состав ЗИС, их методы функционирования и проектирования; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - методы концептуального проектирования технологий обеспечения информационной безопасности	- ставить и решать типовые задачи в области анализа безопасности информационных потоков в распределенной информационной системе; - подбирать и использовать адекватные методы и средства защиты информации; - оценивать эффективность методов защиты информационных процессов; - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; - организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности	- навыками применения теоретического аппарата защиты информации к текущим реальным ситуациям; - навыками обнаружения уязвимостей в распределенных информационных системах и программных комплексах; - навыками управления информационной безопасностью простых объектов

ПК-9 – способностью проводить аудит информационной безопасности информационных систем и объектов информатизации.		
Знать	Уметь	Владеть
- основные понятия теории защиты информации в объеме, необходимом для использования и анализа сервисов информационной безопасности, основные модели доступа к информации; - основные виды информационных атак и дестабилизирующих информационных воздействий; - типовые состав ЗИС, их методы функционирования и проектирования; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - методы концептуального проектирования технологий обеспечения информационной безопасности	- ставить и решать типовые задачи в области анализа безопасности информационных потоков в распределенной информационной системе; - подбирать и использовать адекватные методы и средства защиты информации; - оценивать эффективность методов защиты информационных процессов; - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; - организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности	- навыками применения теоретического аппарата защиты информации к текущим реальным ситуациям; - навыками обнаружения уязвимостей в распределенных информационных системах и программных комплексах; - навыками управления информационной безопасностью простых объектов

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 «Защищенные информационные системы»

Текущий контроль знаний, согласно «Положению о рейтинговой системе комплексной оценки знаний студентов в ВлГУ» (далее Положение) в рамках изучения дисциплины «Защищенные информационные системы» 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 «Защищенные информационные системы» (письменный рейтинг-контроль)

2 семестр:

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

- Типы компьютерных систем, как элементов информационных технологий.
- Основные принципы успешного функционирования информационной (компьютерной) системы.
- Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений.
- Основные принципы и методы защиты информационных процессов в компьютерных системах.
- Понятие защищенной информационной технологии.
- Основные подходы, используемые при проектировании защищенных информационных технологий.
- Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении.
- Государственные стандарты на разработку и создание информационных систем в защищенном исполнении.
- CASE-технологии создания информационных систем.
- Стандарт ITIL.
- Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».
- Американский стандарт по защите информации «Оранжевая книга».
- Понятие гарантии защиты.
- Критерии оценки защищенности баз данных.
- Содержание классов защищенности.

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

- Требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения гарантированно защищенных информационных систем.
- Вопросы гарантий и эффективности в европейском стандарте ITSEC.
- Европейский стандарт по защите информации ITSEC.
- Понятие гарантии защиты в соответствии с европейским стандартом ITSEC.
- Критерии оценки защищенности в соответствии с европейским стандартом ITSEC. Содержание классов защищенности в соответствии с европейским стандартом ITSEC.

- Функциональные требования по защите информации, предъявляемые в каждом классе защищенности в соответствии с европейским стандартом ITSEC.
- Принципы и методы построения защищенных информационных систем.
- Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты.
- Функции поддержки политики безопасности. Гарантии безопасности.
- Требования по безопасности информационных технологий. Классы защищенности.
- Компоненты подсистем поддержки политики безопасности.
- Содержание типовой политики безопасности.
- Классы защищенности в системе общих критериев. Понятие аудита политики безопасности.
- Требования к подсистемам аудита.
- Подсистемы подтверждения подлинности отправки и получения сообщения.

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

- Подсистемы разграничения доступа.
- Подсистемы идентификации и аутентификации.
- Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы.
- Подсистемы защиты связи.
- Требования к подсистемам, предъявляемые в каждом классе защищенности.
- Гарантии безопасности компьютерных систем в системе общих критериев.
- Понятие гарантии безопасности. Уровни гарантий.
- Гарантии проектирования защищенных информационных систем.
- Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.
- Каналы утечки и их анализ в системе общих критериев.
- Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности.
- Методология анализа каналов утечки информации.
- Безопасное функционирование в системе общих критериев.
- Управление конфигурацией. Безопасная установка систем защиты информационных технологий.
- Безопасная модернизация информационных технологий.

3 семестр:

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

- Ценности, опасности, потери, риски, угрозы в компьютерных системах.
- Основные угрозы информации в компьютерных системах.
- Специфика возникновения угроз в открытых сетях.
- Особенности защиты информации на узлах компьютерной сети.
- Системные вопросы защиты программ и данных.
- Анализ рисков. Модель противника, возможности противника.
- Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.
- Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.
- Требования к защите автоматизированных систем от НСД.
- Модель угроз. Анализ критичных технологий.
- Требования, предъявляемые к разработке модели угроз.
- Структура модели угроз безопасности информации.
- Анализ критичных технологий обработки информации.

- Система лицензирования и сертификации средств защиты.

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

- Система лицензирования и сертификации средств защиты.
- Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.
- Нормативная база и ответственность за защиту информации в компьютерных системах.
- Основные руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа.
- Разработка политик безопасности для защищенных компьютерных систем.
- Требования, предъявляемые к разработке политик безопасности.
- Дискреционная и многоуровневая политика безопасности.
- Политика мандатного доступа.
- Политика защиты целостности информационных ресурсов.
- Понятие аттестации защищенных компьютерных систем.
- Руководящие документы ФСТЭК России по аттестации.
- Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
- Содержание этапов аттестационных испытаний.
- Контроль эффективности защитных мероприятий в системе аттестации.
- Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.

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

- Руководящие документы ФСТЭК России по аттестации.
- Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
- Содержание этапов аттестационных испытаний.
- Контроль эффективности защитных мероприятий в системе аттестации.
- Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.
- Современная структура ITIL.
- Преимущества внедрения ITSM.
- Бизнес-ориентированное управление ИТ на современном предприятии.
- Порядок внедрения SLM-системы.
- Service Desk — цели, возможности, реализации.
- Microsoft Operations Framework (MOF).
- Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС. Техническое задание, эскизный проект, технический проект, рабочая документация, ввод в действие.
- Сопровождение ЗИС.
- Методы и методики оценки качества ЗИС.
- Требования к эксплуатационной документации ЗИС.
- Порядок приемки защищенных ЗИС, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД.
- Особенности эксплуатации ЗИС на объекте защиты.

Регламент проведения лабораторных работ

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Защищенные информационные системы» предполагается выполнение лабораторных работ, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

Критерии оценки выполнения лабораторных работ (2 семестр)

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 (зачете).

Критерии оценки выполнения лабораторных работ (3 семестр)

Результаты выполнения каждой лабораторной работы оцениваются в баллах. Максимальная сумма, набираемая студентом за выполнение каждой лабораторной работы, составляет 5 баллов.

Критерии оценки для выполнения лабораторной работы:

- 4-5 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;

-3-3,9 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;

- 1-2,9 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;

- 0,5-0,9 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 0,5 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 (экзамене).

Оценочные средства для текущего контроля знаний по учебной дисциплине «Защищенные информационные системы» (лабораторные работы)

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

Лабораторная работа № 1. Сравнительный анализ различных стандартов в области защиты информационных технологий с точки зрения эффективности достижения цели построения защищенных информационных систем.

- Что такое защищенная информационная система?
- Стандарты защиты информационных технологий
- Сравнительный анализ стандартов информационной безопасности

Лабораторная работа № 2. Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев

- Что такое защищенная компьютерная система?
- Классификация защищенности компьютерной системы
- Общие критерии требований безопасности информации

Лабораторная работа № 3. Анализ рисков для информационной системы предприятия (организации) и построение модели угроз безопасности

- Что такое информационная система предприятия?
- Методики анализа рисков информационной безопасности
- Модели угроз безопасности

Лабораторная работа № 4. Порядок сертификации средств защиты информации для разработчика СЗИ.

- Документы по сертификации средств защиты информации
- Общий порядок сертификации
- Особенности сертификации СЗИ

Лабораторная работа № 5. Порядок лицензирования в области создания средств защиты информации и защищенных информационных систем для руководителя предприятия (организации) – соискателя лицензии

- Нормативно-правовое обеспечение проблем лицензирования
- Положение о сертификации средств защиты информации
- Лицензирование деятельности предприятия по технической защите информации

Лабораторная работа № 6. Разработка профиля защиты и построение политик безопасности для компьютерной системы предприятия (организации)

- Каковы основные политики безопасности для компьютерной системы предприятия?
- Этапы разработки профиля защиты
- Разработка и реализация политика безопасности предприятия

Лабораторная работа № 7. Проведение аттестационных испытаний компьютерных систем в защищенном исполнении, и выдача «Аттестата соответствия»

- Что такое Аттестат соответствия требованиям безопасности информации?
- Испытания компьютерных систем в защищенном исполнении
- Положение по аттестации объектов информатизации

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ (3 семестр):

Лабораторная работа № 1. Обнаружение узлов корпоративной СЕТИ. ICMP ECHO REQUEST (Утилиты FPING и NMAP)

Лабораторная работа № 2. Обнаружение узлов корпоративной сети. Информационные ICMP сообщения

Лабораторная работа № 3. Обнаружение узлов корпоративной сети средствами протокола TCP (TCP-PING)

Лабораторная работа № 4. Обнаружение узлов корпоративной сети средствами протоколов UDP (UDP-PING), IP

Лабораторная работа № 5. Обнаружение узлов корпоративной сети средствами протокола ARP (ARP-PING)

Лабораторная работа № 6. Основные средства определения маршрутов IP-пакетов - PING, TRACEROUTE

Лабораторная работа № 7. Дополнительные средства определения маршрутов IP-ПАКЕТОВ - NMAP, TRACEMAP, MRT

Лабораторная работа № 8. Идентификация статуса TCP-портов (TCP-CONNECT. SYN-SCAN)

Лабораторная работа № 9. Методы скрытого сканирования (STEALTH TCP SCANNING METHODS)

Лабораторная работа № 10. Идентификация прикладных сетевых служб методом анализа особенностей реализации (SMTP)

Регламент проведения самостоятельной работы

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Защищенные информационные системы» предполагается выполнение заданий СРС, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

Критерии оценки выполнения самостоятельной работы (2 семестр)

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.

Критерии оценки выполнения самостоятельной работы (3 семестр)

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

Критерии оценки для выполнения работы:

- 1,9-2 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;

- 0,9-1,8 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;

- 0,5-0,9 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 «Защищенные информационные системы» (самостоятельная работа)

2 семестр:

№ пп	Раздел (тема) дисциплины	Виды СРС	Формы контроля СРС	Баллы по СРС
1	Информационные технологии и информационные системы. Примеры информационных технологий и информационных систем	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
2	Проектирование и разработка защищенных информационных технологий	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
3	Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
4	Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
5	Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1

6	Классы в системе общих критериев. Классы защищенности в системе общих критериев. Понятие аудита политики безопасности.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
7	Гарантии безопасности компьютерных систем в системе общих критериев. Понятие гарантии безопасности. Уровни гарантий.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
8	Каналы утечки и их анализ в системе общих критериев. Виды каналов утечки информации.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
9	Безопасное функционирование в системе общих критериев. Управление конфигурацией.	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):

- ITIL – Компонент «Поддержка услуг».
- ITIL – Компонент «Предоставление услуг».
- ITIL — основа концепции управления ИТ-службами.
- Service Desk — цели, возможности, реализации.
- Аудит инфраструктуры РИС/КАС.
- Аутсорсинг.

3 семестр:

№ пп	Раздел (тема) дисциплины	Виды СРС	Формы контроля СРС	Баллы по СРС
1	Основные угрозы безопасности информации в компьютерных системах.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	2
2	Модель угроз. Анализ критичных технологий. Требования, предъявляемые к разработке модели угроз.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
3	Государственная политика в области безопасности компьютерных систем. Система лицензирования и сертификации средств защиты.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	2
4	Разработка политик безопасности для защищенных компьютерных систем. Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	2
5	Порядок аттестации защищенных компьютерных систем. Понятие аттестации защищенных компьютерных систем.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	2
6	Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	2

	концепции управления ИТ-службами.			
7	Порядок внедрения SLM-системы. Service Desk — цели, возможности, реализации. Microsoft Operations Framework (MOF).	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	2
8	Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС, техническое задание, эскизный проект, технический проект, рабочая документация	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	2
9	Методы и методики оценки качества ЗИС. Требования к эксплуатационной документации ЗИС. Порядок приемки защищенных ЗИС	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	2
			Итого за семестр:	18

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении СРС (3 семестр):

- Методология Penetration Testing. Open Source Security Testing Methodology Manual (OSSTMM).
- Методология Penetration Testing. Information Systems Security Assessment Framework (ISSAF).
- Методология Penetration Testing. Open Web Application Security Project (OWASP).
- Методология Penetration Testing. Web Application Security Consortium Threat Classification (WASC-TC).
- Стандарт Penetration Testing. Penetration Testing Execution Standard (PTES).
- Footprinting. Цели, задачи Footprinting. Этапы Footprinting и Reconnaissance.
- Footprinting. Открытые источники и пассивный сбор информации.
- Footprinting. Активный сбор информации.
- Footprinting. Программные инструменты Footprinting и Reconnaissance.
- Сканирование сети. Обнаружение узлов сети. Методы и программные средства.
- Сканирование сети. Обнаружение открытых портов узла сети. Методы и программные средства.
- Сканирование сети. Типы сканирования (Full Open Scan, Half-open Scan, Xmas Tree Scan). Особенности использования рассматриваемых типов сканирования.
- Сканирование сети. Типы сканирования (FIN Scan, NULL Scan, ACK Scanning). Особенности использования рассматриваемых типов сканирования.
- Сканирование сети. Типы сканирования (UDP Scanning, ARP Scan). Особенности использования рассматриваемых типов сканирования.
- Services fingerprinting. Методы Services fingerprinting.
- Services fingerprinting. Программные инструменты Services fingerprinting.
- OS Fingerprinting. Методы OS Fingerprinting. Banner Grabbing.
- OS Fingerprinting. Методы OS Fingerprinting. Пассивное исследование стека в задаче идентификации ОС.
- OS Fingerprinting. Методы OS Fingerprinting. Активное исследование стека в задаче идентификации ОС.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация ресурсов OS Windows. Методы и средства.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация ресурсов OS Linux/Unix. Методы и средства.

- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация посредством SNMP.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация LDAP.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация SMTP.
- Sniffing. Цели и задачи анализа трафика. Программные инструменты анализа трафика.
- Sniffing атаки в коммутируемой сетевой среде. MAC Flooding. ARP Poisoning.
- Sniffing атаки в коммутируемой сетевой среде. MAC Spoofing.
- Sniffing атаки в коммутируемой сетевой среде. Методы и средства защиты от Sniffing атак.
- Атаки DOS. Цели и задачи атак DOS. Типы атак DOS.
- Атаки DOS. Service Request Floods. SYN Attack/Flood. ICMP Flood Attack. Программные средства проведения атак.
- Атаки DOS. Ping of Death. Teardrop. Smurf. Fraggle. Программные средства проведения атак.
- Атаки Buffer Overflow. Принципы.
- Атаки DDOS. Особенности реализации.
- Беспроводные сети. Угрозы и уязвимости Wireless Networks.
- Беспроводные сети. Аутентификация Wi-fi.
- Беспроводные сети. Атаки деаутентификации (Deauthentication Attack).
- Сканеры уязвимостей. Идентификация уязвимостей в сетях.
- Сканеры уязвимостей. Уязвимости БД.
- Средства анализа защищенности БД.
- Сканеры уязвимостей. Уязвимости WEB приложений.
- Средства анализа защищенности WEB приложений.

Регламент проведения курсового проекта (3 семестр)

Примерные темы заданий к курсовой работе

1. Разработка защищенного АРМ администратора безопасности.
2. Организация антивирусной защиты ЛВС.
3. Построение комплексной системы защиты информации IP-сети.
4. Анализ особенностей защиты информации в мультисервисных сетях.
5. Исследование методов построения защищенных Интернет приложений.
6. Разработка системы управления учетными записями пользователей для различных предметных областей.
7. Анализ и разработка методов построения отказоустойчивого файлового сервера организации различного профиля.
8. Разработка проекта ИТ-приложения на современном предприятии (по выбору) с проработкой механизмов защиты.
9. Разработка защищенной АС структурного подразделения на современном предприятии (по выбору).
10. Разработка проекта защищенной распределенной АС подразделения на территориально-распределенном предприятии (по выбору).

Критерии оценки выполнения курсового проекта

№п/п	Расшифровка критериев	Количество баллов
1	Представление результатов курсовой работы (доклад, ответы на вопросы)	20
2	Качество оформления пояснительной записки и графического материала (в т.ч. презентации). Нормоконтроль в соответствии с требованиями ГОСТ.	30
3	Промежуточная аттестация (оцениваются результаты работы: степень выполнения, соответствие поставленной задаче,	25

	график работ, устранение замечаний и т.п.)	
4	Финальная аттестация (оцениваются результаты работы: степень выполнения, соответствие поставленной задаче, разработанное ПО и т.п.)	25
	Общее количество баллов	100

Баллы округляются в большую строну. Результаты курсового проекта определяются следующими оценками: «зачтено» и «незачтено» по следующей шкале:

«Зачтено» - от 61 балла.

«Незачтено» - 60 и менее баллов.

При неудовлетворительной оценке за курсовой проект обучающийся не получает положительную оценку при промежуточном контроле по дисциплине (экзамене).

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	10
5	Дополнительные баллы (бонусы)	7
6	Лабораторные работы	35
7	Выполнение семестрового плана самостоятельной работы	18
	Всего	100

3 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	0,5
5	Дополнительные баллы (бонусы)	0,5
6	Лабораторные работы	20
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 «Защищенные информационные системы»

Регламент проведения промежуточного контроля (зачета)

Промежуточная аттестация по итогам освоения дисциплины (зачет) проводится перед экзаменационной сессией. Зачет проставляется студенту после выполнения студентом семестрового плана самостоятельной работы.

Критерии оценивания при проставлении зачета (2 семестр)

Критерии оценки для промежуточного контроля (зачета):

- оценка «отлично» (соответствует 91-100 баллов по шкале рейтинга) выставляется обучающемуся, если соблюдаются критерии: теоретическое содержание оцениваемой части дисциплины освоено полностью, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены в установленные сроки, качество их выполнения оценено числом баллов, близким к максимальному;

- оценка «хорошо» (соответствует 74-90 баллов по шкале рейтинга) выставляется обучающемуся, если соблюдаются критерии: теоретическое содержание курса освоено полностью, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками или с нарушением установленных сроков;

- оценка «удовлетворительно» (соответствует 61-73 баллов по шкале рейтинга) выставляется обучающемуся, если соблюдаются критерии: теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки;

- оценка «неудовлетворительно» (соответствует менее 60 баллов по шкале рейтинга) выставляется обучающемуся, если соблюдаются критерии: теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки.

Оценочные средства для промежуточной аттестации по учебной дисциплине «Защищенные информационные системы» (зачёт)

1. Типы компьютерных систем, как элементов информационных технологий.
2. Основные принципы успешного функционирования информационной (компьютерной) системы.
3. Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений.
4. Основные принципы и методы защиты информационных процессов в компьютерных системах.
5. Понятие защищенной информационной технологии.
6. Основные подходы, используемые при проектировании защищенных информационных технологий.
7. Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении.
8. Государственные стандарты на разработку и создание информационных систем в защищенном исполнении.
9. CASE-технологии создания информационных систем.
10. Стандарт ITIL.

11. Построение гарантированно защищенных баз, данных и их оценка по стандарту «Оранжевая книга».
12. Американский стандарт по защите информации «Оранжевая книга».
13. Понятие гарантии защиты.
14. Критерии оценки защищенности баз данных.
15. Содержание классов защищенности.
16. Требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения гарантированно защищенных информационных систем.
17. Вопросы гарантий и эффективности в европейском стандарте ITSEC.
18. Европейский стандарт по защите информации ITSEC.
19. Понятие гарантии защиты в соответствии с европейским стандартом ITSEC.
20. Критерии оценки защищенности в соответствии с европейским стандартом ITSEC. Содержание классов защищенности в соответствии с европейским стандартом ITSEC.
21. Функциональные требования по защите информации, предъявляемые в каждом классе защищенности в соответствии с европейским стандартом ITSEC.
22. Принципы и методы построения защищенных информационных систем.
23. Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты.
24. Функции поддержки политики безопасности. Гарантии безопасности.
25. Требования по безопасности информационных технологий. Классы защищенности.
26. Компоненты подсистем поддержки политики безопасности.
27. Содержание типовой политики безопасности.
28. Классы защищенности в системе общих критериев. Понятие аудита политики безопасности.
29. Требования к подсистемам аудита.
30. Подсистемы подтверждения подлинности отправки и получения сообщения.
31. Подсистемы разграничения доступа.
32. Подсистемы идентификации и аутентификации.
33. Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы.
34. Подсистемы защиты связи.
35. Требования к подсистемам, предъявляемые в каждом классе защищенности.
36. Гарантии безопасности компьютерных систем в системе общих критериев.
37. Понятие гарантии безопасности. Уровни гарантий.
38. Гарантии проектирования защищенных информационных систем.
39. Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.
40. Каналы утечки и их анализ в системе общих критериев.
41. Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности.
42. Методология анализа каналов утечки информации.
43. Безопасное функционирование в системе общих критериев.
44. Управление конфигурацией. Безопасная установка систем защиты информационных технологий.
45. Безопасная модернизация информационных технологий.

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 (3 семестр)

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 «Защищенные информационные системы» (экзамен)

Перечень вопросов для промежуточного контроля (экзамена)

1. Ценности, опасности, потери, риски, угрозы в компьютерных системах.
2. Основные угрозы информации в компьютерных системах.
3. Специфика возникновения угроз в открытых сетях.
4. Особенности защиты информации на узлах компьютерной сети.
5. Системные вопросы защиты программ и данных.
6. Анализ рисков. Модель противника, возможности противника.
7. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.
8. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.
9. Требования к защите автоматизированных систем от НСД.
10. Модель угроз. Анализ критичных технологий.
11. Требования, предъявляемые к разработке модели угроз.
12. Структура модели угроз безопасности информации.
13. Анализ критичных технологий обработки информации.
14. Система лицензирования и сертификации средств защиты.
15. Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.
16. Нормативная база и ответственность за защиту информации в компьютерных системах.
17. Основные руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа.
18. Разработка политик безопасности для защищенных компьютерных систем.
19. Требования, предъявляемые к разработке политик безопасности.
20. Дискреционная и многоуровневая политика безопасности.
21. Политика мандатного доступа.
22. Политика защиты целостности информационных ресурсов.
23. Понятие аттестации защищенных компьютерных систем.
24. Руководящие документы ФСТЭК России по аттестации.
25. Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
26. Содержание этапов аттестационных испытаний.
27. Контроль эффективности защитных мероприятий в системе аттестации.
28. Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.
29. Современная структура ITIL.
30. Преимущества внедрения ITSM.
31. Бизнес-ориентированное управление ИТ на современном предприятии.
32. Порядок внедрения SLM-системы.
33. Service Desk — цели, возможности, реализации.
34. Microsoft Operations Framework (MOF).
35. Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС. Техническое задание, эскизный проект, технический проект, рабочая документация, ввод в действие.
36. Сопровождение ЗИС.
37. Методы и методики оценки качества ЗИС.
38. Требования к эксплуатационной документации ЗИС.
39. Порядок приемки защищенных ЗИС, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД.
40. Особенности эксплуатации ЗИС на объекте защиты.