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
«Теоретические основы компьютерной безопасности»

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 «Теоретические основы компьютерной безопасности» разработан в соответствие с рабочей программой, входящей в ОПОП направления подготовки 10.04.01 иинформационная безопасность.

№ п/п	Контролируемые разделы (темы) дисциплины	Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Математическая модель комплексного подхода к обеспечению безопасности компьютерной системы. Основы теории защиты информации	1	ПК-9, ПК-13	Контрольные вопросы и задания
2	Методика построения системы защиты информации	1	ПК-9, ПК-13	Контрольные вопросы и задания
3	Методы многопараметрической оценки эффективности системы защиты информации	1	ПК-9, ПК-13	Контрольные вопросы и задания
4	Метод экспертных оценок при анализе эффективности системы защиты информации	1	ПК-9, ПК-13	Контрольные вопросы и задания
5	Угрозы информационной безопасности и оценка вероятности их реализации	1	ПК-9, ПК-13	Контрольные вопросы и задания
6	Модель описания процесса защиты информации Хоффмана – Клементса	1	ПК-9, ПК-13	Контрольные вопросы и задания
7	Вероятностная модель оценки защищенности информационных ресурсов	1	ПК-9, ПК-13	Контрольные вопросы и задания
8	Сбор исходных данных для аудита безопасности информационной системы	1	ПК-9, ПК-13	Контрольные вопросы и задания
9	Выявление уязвимостей и идентификация защитных механизмов информационной системы	1	ПК-9, ПК-13	Контрольные вопросы и задания

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

Комплект оценочных средств по дисциплине «Теоретические основы компьютерной безопасности» включает:

1 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.

2. Перечень компетенций, формируемых в процессе изучения дисциплины «Теоретические основы компьютерной безопасности» 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-9 – способностью проводить аудит информационной безопасности информационных систем и объектов информатизации;		
Знать	Уметь	Владеть
основные концептуальные положения теории ЗИ; - содержание функций ЗИ; - классифи-кацию средств ЗИ; - преимущества и недостатки программных, аппаратных и организа-ционных средств ЗИ; - общее содержание методологии проектирования системы ЗИ; - ме-тодику построения системы ИБ предприятия; - метод экспертных оценок при построении системы ЗИ; - аналитическую зависимость (формулу) для оценки вероятности уязвимости информации; - модель защищенной системы Хоффмана – Клементса; - основные этапы проведения аудита информационной безопасности; - типовой набор угроз информацион-ной безопасности объекта аудита.	решать задачу выбора системы ЗИ методом последовательных уступок; - строить фор-мальную модель метода анализа иерархий при выборе системы ЗИ; - использовать метод экспертных оценок при построении системы ЗИ; - привести ранжированный список угроз по частоте их проявления; - сравнивать качественные и количественные методы оценки уровня защищенности; - определять вероятности защищенности информационных ресурсов; - категорировать критичные информационные ресурсы и информационные процессы предприятия (организации); - заполнять типовые формы отчетов по сбору ис-ходной информации об информационной системе предприятия (организации); - выявлять нарушителей, уязвимости и угрозы информационной безопасности конкретного пред-приятия (организации).	навыками настройки современных средств защиты информации; - программными сред-ствами оценки защищенности компьютерных систем; - навыками управления информа-ционной безопасностью простых объектов

ПК-13 – способностью организовать управление информационной безопасностью.		
Знать	Уметь	Владеть
основные концептуальные положения теории ЗИ; - содержание функций ЗИ; - классифи-кацию средств ЗИ; - преимущества и недостатки программных, аппаратных и организа-ционных средств ЗИ; - общее содержание методологии проектирования системы ЗИ; - ме-тодику построения системы ИБ предприятия; - метод экспертных оценок при построении системы ЗИ; - аналитическую зависимость (формулу) для оценки вероятности уязвимости информации; - модель защищенной системы Хоффмана – Клементса; - основные этапы проведения аудита информационной безопасности; - типовой набор угроз информацион-ной безопасности объекта аудита.	решать задачу выбора системы ЗИ методом последовательных уступок; - строить фор-мальную модель метода анализа иерархий при выборе системы ЗИ; - использовать метод экспертных оценок при построении системы ЗИ; - привести ранжированный список угроз по частоте их проявления; - сравнивать качественные и количественные методы оценки уровня защищенности; - определять вероятности защищенности информационных ресурсов; - категорировать критичные информационные ресурсы и информационные процессы предприятия (организации); - заполнять типовые формы отчетов по сбору ис-ходной информации об информационной системе предприятия (организации); - выявлять нарушителей, уязвимости и угрозы информационной безопасности конкретного пред-приятия (организации).	навыками настройки современных средств защиты информации; - программными сред-ствами оценки защищенности компьютерных систем; - навыками управления информа-ционной 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 «Теоретические основы компьютерной безопасности»

Текущий контроль знаний, согласно «Положению о рейтинговой системе комплексной оценки знаний студентов в ВлГУ» (далее Положение) в рамках изучения дисциплины «Теоретические основы компьютерной безопасности» предполагает письменный рейтинг-контроль, выполнение и защиту лабораторных, а также выполнение самостоятельных работ и курсовой работы. 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 «Теоретические основы компьютерной безопасности» (письменный рейтинг-контроль)

Семестр 1

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

1. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность?

2. Сформулируйте основные концептуальные положения теории ЗИ.
3. Раскройте содержание функции ЗИ. Какие из функций образуют полное множество функций защиты?
4. Сформулируйте определение механизма защиты и назовите их десять классов, образующих репрезентативное множество.
5. Приведите наиболее распространенную на сегодняшний день классификацию средств ЗИ. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств ЗИ?
6. Сформулируйте возможные постановки задачи оптимизации СЗИ.
7. Прокомментируйте основные принципы обеспечения ИБ предприятия
8. Приведите принятую методику построения системы ИБ предприятия
9. Приведите модель решения задачи выбора системы ЗИ методом последовательных уступок.
10. Приведите формальную модель метода анализа иерархий при выборе системы ЗИ.

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

1. В чем заключается сущность метода экспертных оценок при построении системы ЗИ?
2. Приведите описание основных этапов метода экспертных оценок при построении системы ЗИ
3. Приведите ранжированный список угроз по частоте их проявления.
4. Приведите общий подход к оценке уязвимости информационных ресурсов по каналам утечки информации
5. Какие параметры и характеристики входят в вероятностную модель оценки уязвимости защищаемой информации?
6. Выведите аналитическую зависимость (формулу) для оценки вероятности уязвимости информации
7. Сравните качественные и количественные методы оценки уровня защищенности
8. Приведите модель описания процесса защиты информации Хоффмана.
9. Какие множества рассматриваются при описании системы защиты информации с полным перекрытием?
10. Приведите теоретико-множественную модель защищенной системы Клементса.

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

1. Приведите общую модель процесса защиты информации в виде пятимерного кортежа элементов.
2. Приведите основные параметры модели процесса защиты
3. Приведите алгоритм определения вероятности защищенности одного информационного ресурса
4. Что понимают под аудитом информационной безопасности предприятия (организации)?
5. Приведите и прокомментируйте основные этапы проведения аудита информационной безопасности.
6. Назовите основные подсистемы защиты информации и дайте комментарий к их защитным механизмам
7. Заполните типовые формы отчетов по сбору исходной информации об информационной системе предприятия (организации), в котором работаете или проходили производственную практику.
8. В чем заключается методика выявления уязвимостей в анализируемой

информационной системе?

9. Приведите методику идентификации защитных механизмов информационной системы.

10. Какие категории нарушителей следует учитывать при анализе защищенности информационной системы?

Регламент проведения лабораторных работ

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Теоретические основы компьютерной безопасности» 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 8 баллов.

Критерии оценки для выполнения лабораторной работы:

- 6-8 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;

- 4-5 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;

- 2-3 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;

- 0,5-1,9 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 (зачет).

Оценочные средства для текущего контроля знаний по учебной дисциплине «Теоретические основы компьютерной безопасности» (лабораторные работы)

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ (1 семестр):

ЛАБОРАТОРНАЯ РАБОТА 1. Сбор исходных данных для аудита информационной безопасности

1. Что такое аудит информационной безопасности объекта?
2. Что может выступать в качестве объекта аудита информационной безопасности объекта?
3. Где берутся данные для аудита информационной безопасности объекта?
4. Приведите перечень исходных данных, необходимых для аудита безопасности.
5. Назовите виды аудита безопасности.

ЛАБОРАТОРНАЯ РАБОТА 2. Выявление уязвимостей компьютерной системы

1. Что такое уязвимости информационной системы.
2. Что может выступать в качестве уязвимостей информационной системы.
3. Как можно выявить уязвимости информационной системы.
4. Приведите классификацию основных уязвимостей.
5. Назовите причины возникновения уязвимостей.

ЛАБОРАТОРНАЯ РАБОТА 3. Идентификация защитных механизмов

1. Что такое идентификация.
2. Что такое защитный механизм.
3. Приведите примеры защитных механизмов.
4. Назовите основные защитные механизмы, используемые в системах защиты информации.
5. Как происходит идентификация защитных механизмов.

ЛАБОРАТОРНАЯ РАБОТА 4. Идентификация нарушителей

1. Что такое идентификация.
2. Кто такие нарушители.
3. Приведите примеры нарушителей.
4. Как можно идентифицировать нарушителей?
5. Перечислите виды нарушителей.

Регламент проведения самостоятельной работы

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Теоретические основы компьютерной безопасности» 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 3 балла.

Критерии оценки для выполнения работы:

- 2,4-3 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;

- 1,4-2,3 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;

- 0,7-1,3 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;

- 0,2-0,6 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 «Теоретические основы компьютерной безопасности» (самостоятельная работа)

1 семестр:

№ пп	Раздел (тема) дисциплины	Виды СРС	Формы контроля СРС	Баллы по СРС
1	Математическая модель комплексного подхода к обеспечению безопасности компьютерной системы. Основы теории защиты информации	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
2	Методика построения системы защиты информации	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
3	Методы многопараметрической оценки эффективности системы защиты информации	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
4	Метод экспертных оценок при анализе эффективности системы защиты информации	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
5	Угрозы информационной безопасности и оценка вероятности их реализации	Работа с учебниками (учебными пособиями). Работа с конспектом	Письменный или устный опрос, проверка	3

		лекций.	конспектов	
6	Модель описания процесса защиты информации Хоффмана – Клементса	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
7	Вероятностная модель оценки защищенности информационных ресурсов	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
8	Сбор исходных данных для аудита безопасности информационной системы	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
9	Выявление уязвимостей и идентификация защитных механизмов информационной системы	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
			Итого за семестр:	27

Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении СРС (1 семестр):

Раздел 1.

1. Сформулируйте определение механизма защиты и назовите их десять классов, образующих репрезентативное множество.
2. Приведите наиболее распространенную на сегодняшний день классификацию средств ЗИ. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств ЗИ?

Раздел 2.

1. Сформулируйте возможные постановки задачи оптимизации СЗИ.
2. Прокомментируйте основные принципы обеспечения ИБ предприятия
3. Какие должны быть условия успешности решения проблем ИБ?
4. Сформулируйте общие требования к системе ИБ объекта
5. Перечислите рекомендации создателям систем ИБ.

Раздел 3.

1. Приведите модель решения задачи выбора системы ЗИ методом последовательных уступок.
2. Приведите формальную модель метода анализа иерархий при выборе системы ЗИ.

Раздел 4.

1. В чем заключается сущность метода экспертных оценок при построении системы ЗИ?
2. Что предусматривает метод проверки системы ЗИ с применением тестирования или «тестирования на проникновение»?

Раздел 5.

1. Приведите ранжированный список угроз по частоте их проявления.
2. Какие ситуации в работе ИС называют «нештатными»?
3. Приведите общий подход к оценке уязвимости информационных ресурсов по каналам утечки информации
4. Какие параметры и характеристики входят в вероятностную модель оценки уязвимости защищаемой информации?

Раздел 6.

1. Сравните качественные и количественные методы оценки уровня защищенности

2. Приведите модель оценки уровня защищенности, основанную на анализе рисков.
3. Какие множества рассматриваются при описании системы защиты информации с полным перекрытием?

Раздел 7.

1. Приведите основные параметры модели процесса защиты
2. Какие уточнения и допущения модели процесса защиты Вы знаете?
3. Достоинства предлагаемой модели процесса защиты информации в виде пятимерного кортежа элементов

Раздел 8.

1. Заполните типовые формы отчетов по сбору исходной информации об информационной системе предприятия (организации), в котором работаете или проходили производственную практику.

Раздел 9.

1. Проведите сравнительный анализ двух групп оценки рисков информационной безопасности.
2. Выявите нарушителей, уязвимости и угрозы информационной безопасности конкретного предприятия (организации)

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

1 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	6
5	Дополнительные баллы (бонусы)	5
6	Лабораторные работы	32
7	Выполнение семестрового плана самостоятельной работы	27
	Всего	100

4. Показатели, критерии и шкала оценивания компетенций промежуточной аттестации знаний по учебной дисциплине «Теоретические основы компьютерной безопасности»

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

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 « Теоретические основы компьютерной безопасности» (зачёт)

Перечень вопросов к зачету:

1. Сформулируйте основные концептуальные положения теории ЗИ.
2. Раскройте содержание функции ЗИ. Какие из функций образуют полное множество функций защиты?
3. Сформулируйте определение механизма защиты и назовите их десять классов, образующих репрезентативное множество.
4. Сформулируйте возможные постановки задачи оптимизации СЗИ.
5. Прокомментируйте основные принципы обеспечения ИБ предприятия
6. Приведите принятую методику построения системы ИБ предприятия
7. Приведите модель решения задачи выбора системы ЗИ методом последовательных уступок.
8. Приведите формальную модель метода анализа иерархий при выборе системы ЗИ.
9. В чем заключается сущность метода экспертных оценок при построении системы ЗИ?
10. Приведите ранжированный список угроз по частоте их проявления.
11. Приведите общий подход к оценке уязвимости информационных ресурсов по каналам утечки информации
12. Какие параметры и характеристики входят в вероятностную модель оценки уязвимости защищаемой информации?
13. Выведите аналитическую зависимость (формулу) для оценки вероятности уязвимости информации
14. Сравните качественные и количественные методы оценки уровня защищенности
15. Приведите модель описания процесса защиты информации Хоффмана.
16. Приведите теоретико-множественную модель защищенной системы Клементса.
17. Приведите основные параметры модели процесса защиты
18. Приведите алгоритм определения вероятности защищенности одного информационного ресурса
19. Что понимают под аудитом информационной безопасности предприятия (организации)?

20. Приведите и прокомментируйте основные этапы проведения аудита информационной безопасности.
21. Назовите основные подсистемы защиты информации и дайте комментарий к их защитным механизмам
22. Заполните типовые формы отчетов по сбору исходной информации об информационной системе предприятия (организации), в котором работаете или проходили производственную практику.
23. В чем заключается методика выявления уязвимостей в анализируемой информационной системе?
24. Приведите методику идентификации защитных механизмов информационной системы.
25. Какие категории нарушителей следует учитывать при анализе защищенности информационной системы?