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
«Защита корпоративных информационных систем»

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 «Защита корпоративных информационных систем» 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	Сетевая разведка. Первичный сбор информации о КИС.	3	ПК-2, ПК-14, ПК-15	Контрольные вопросы и задания
2	Методики и программные средства обнаружения активных узлов корпоративной сети.	3	ПК-2, ПК-14, ПК-15	Контрольные вопросы и задания
3	Методики сканирования сетей.	3	ПК-2, ПК-14, ПК-15	Контрольные вопросы и задания
4	Инвентаризация ресурсов КИС. Подходы и методики.	3	ПК-2, ПК-14, ПК-15	Контрольные вопросы и задания
5	Анализ сетевого трафика. Методики и программные средства.	3	ПК-2, ПК-14, ПК-15	Контрольные вопросы и задания
6	Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде.	3	ПК-2, ПК-14, ПК-15	Контрольные вопросы и задания
7	Программные средства проведения атак типа отказ в обслуживании на ресурсы КИС.	3	ПК-2, ПК-14, ПК-15	Контрольные вопросы и задания
8	Атаки на беспроводные сети КИС. Безопасность беспроводной сети КИС.	3	ПК-2, ПК-14, ПК-15	Контрольные вопросы и задания
9	Методологии тестирования на проникновение.	3	ПК-2, ПК-14, ПК-15	Контрольные вопросы и задания

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

Комплект оценочных средств по дисциплине «Защита корпоративных информационных систем» включает:

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 «Защита корпоративных информационных систем» 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 механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; - основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; - методы аттестации уровня защищенности информационных систем; - основные методы управления информационной безопасностью; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем	- строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем; - разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; - разрабатывать частные политики информационной безопасности информационных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; - оценивать информационные риски в информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности	- методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления информационной безопасностью информационных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; - навыками управления информационной безопасностью простых объектов

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 механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; - основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; - методы аттестации уровня защищенности	- строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем; - разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; - разрабатывать частные политики информационной безопасности информационных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; - оценивать информационные риски в информационных системах;	- методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления информационной

информационных систем; - основные методы управления информационной безопасностью; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем	- разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности	безопасностью информационных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; - навыками управления информационной безопасностью простых объектов

ПК-15 – способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.		
Знать	Уметь	Владеть
основные механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; - основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; - методы аттестации уровня защищенности информационных систем; - основные методы управления информационной безопасностью; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем	- строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем; - разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; - разрабатывать частные политики информационной безопасности информационных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; - оценивать информационные риски в информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности	- методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления информационной безопасностью информационных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; - 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 «Защита корпоративных информационных систем»

Текущий контроль знаний, согласно «Положению о рейтинговой системе комплексной оценки знаний студентов в ВлГУ» (далее Положение) в рамках изучения дисциплины «Защита корпоративных информационных систем» 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 (3 семестр)

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 «Защита корпоративных информационных систем» (письменный рейтинг-контроль)

3 семестр:

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

1. Методологии Penetration Testing.
2. Понятие Footprinting. Этапы.
3. Методы сканирования корпоративной сети.
4. Методики и программные средства обнаружения активных узлов корпоративной сети.
5. Методики и программные средства сканирования TCP/UDP портов узлов корпоративной сети.
6. Методики и программные средства идентификации сетевых служб на узлах корпоративной сети.
7. Методики и программные средства идентификации операционных систем на узлах корпоративной сети.

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

1. Методики и программные средства построения сетевых диаграмм КИС.
2. Инвентаризация ресурсов КИС. Подходы и методики.
3. Инвентаризация ресурсов Linux узлов КИС.
4. Инвентаризация ресурсов Windows узлов КИС.
5. Применение специальных сетевых протоколов для инвентаризации ресурсов КИС.
6. Анализ сетевого трафика. Методики и программные средства.
7. Особенности анализа сетевого трафика в коммутируемой среде.
8. Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде.

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

1. Атаки типа отказ в обслуживании на ресурсы КИС.
2. Программные средства проведения атак типа отказ в обслуживании на ресурсы КИС.
3. Атаки на беспроводные сети КИС.
4. Программные средства проведения атак на беспроводные сети КИС.
5. Сканеры уязвимостей и методики их применения.
6. Особенности применения сканера OpenVAS.
7. Программные средства анализа защищенности баз данных.
8. Программные средства анализа защищенности WEB приложений.

Регламент проведения лабораторных работ

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

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 2 балла.

Критерии оценки для выполнения лабораторной работы:

- 1,8-2 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;

- 1,5-1,7 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;

- 0,9-1,4 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;

- 0,1-0,8 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 (зачет).

Оценочные средства для текущего контроля знаний по учебной дисциплине «Защита корпоративных информационных систем» (лабораторные работы)

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)

- Способы обнаружения узлов в сети
- Общий функционал утилиты Ping
- Общий функционал утилиты FPING
- Общий функционал утилиты NMAP

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

- Способы обнаружения узлов в сети
- Типы пакетов ICMP
- Данные информационного запроса
- Правила генерации ICMP-пакетов

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

- Способы обнаружения узлов в сети
- Обнаружение узлов с помощью утилиты TCP PING
- Описание процесса подключения к различным tcp портам
- Сравнение UDP-PING и TCP-PING

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

- Способы обнаружения узлов в сети
- Описание процесса подключения к различным udp портам
- Сравнение UDP-PING и TCP-PING

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

- Способы обнаружения узлов в сети
- Особенности утилиты arping
- Генерация ARP запросов и ответов

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

- Для каких целей предназначена программа traceroute?
- Основные способы определения маршрутов ip адреса
- Описание команды ping

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

- Определение маршрута с помощью утилита NMAP
- Определение маршрута с помощью утилиты TRACEMAP
- Определение маршрута с помощью утилиты MRT

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

- Назовите основные приемы сканирования tcp портов
- Идентификация статуса через TCP-CONNECT
- Идентификация статуса через SYN-SCAN

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

- Для каких целей применяются методы скрытого сканирования?
- Сравнение различных приемов сканирования
- Наиболее эффективные методы скрытого и полускрытого сканирования

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

- Описание процесса идентификации прикладных сетевых служб
- Что такое SMTP?
- Где применяется SMTP?
- Что нужно для запуска SMTP сервера?

Регламент проведения самостоятельной работы

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

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 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 «Защита корпоративных информационных систем» (самостоятельная работа)

3 семестр:

№ пп	Раздел (тема) дисциплины	Виды СРС	Формы контроля СРС	Баллы по СРС
1	Сетевая разведка. Первичный сбор информации о КИС.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
2	Методики и программные средства обнаружения активных узлов корпоративной сети.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
3	Методики сканирования сетей.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
4	Инвентаризация ресурсов КИС. Подходы и методики.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
5	Анализ сетевого трафика. Методики и программные средства.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
6	Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
7	Программные средства проведения атак типа отказ в обслуживании на ресурсы КИС.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
8	Атаки на беспроводные сети КИС. Безопасность беспроводной сети КИС.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	1
9	Методологии тестирования на проникновение.	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 (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.
- Построение карты сети. Программные средства Drawing Network Diagrams.
- 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.
- OpenVAS.
- Сканеры уязвимостей. Уязвимости БД.
- Средства анализа защищенности БД.
- Сканеры уязвимостей. Уязвимости WEB приложений.
- Средства анализа защищенности WEB приложений.

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

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	2
5	Дополнительные баллы (бонусы)	1
6	Лабораторные работы	18
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 «Защита корпоративных информационных систем»

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 «Защита корпоративных информационных систем» (зачёт)

- Методологии Penetration Testing.
- Понятие Footprinting. Этапы.
- Методы сканирования корпоративной сети.
- Методики и программные средства обнаружения активных узлов корпоративной сети.
- Методики и программные средства сканирования TCP/UDP портов узлов корпоративной сети.
- Методики и программные средства идентификации сетевых служб на узлах корпоративной сети.
- Методики и программные средства идентификации операционных систем на узлах корпоративной сети.
- Методики и программные средства построения сетевых диаграмм КИС.
- Инвентаризация ресурсов КИС. Подходы и методики.
- Инвентаризация ресурсов Linux узлов КИС.
- Инвентаризация ресурсов Windows узлов КИС.
- Применение специальных сетевых протоколов для инвентаризации ресурсов КИС.
- Анализ сетевого трафика. Методики и программные средства.
- Особенности анализа сетевого трафика в коммутируемой среде.
- Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде.
- Атаки типа отказ в обслуживании на ресурсы КИС.
- Программные средства проведения атак типа отказ в обслуживании на ресурсы КИС.
- Атаки на беспроводные сети КИС.
- Программные средства проведения атак на беспроводные сети КИС.
- Сканеры уязвимостей и методики их применения.
- Особенности применения сканера OpenVAS.
- Программные средства анализа защищенности баз данных.
- Программные средства анализа защищенности WEB приложений.