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
«Оценка и контроль обеспечения информационной 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 «Оценка и контроль обеспечения информационной 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	Обнаружение узлов сети. icmp echo request.	2	ПК-9, ПК-10	Контрольные вопросы и задания
2	Обнаружение узлов сети средствами протокола tcp (tcp-ping).	2	ПК-9, ПК-10	Контрольные вопросы и задания
3	Обнаружение узлов сети средствами протокола arp (arp-ping).	2	ПК-9, ПК-10	Контрольные вопросы и задания
4	Дополнительные средства определения маршрутов ip-пакетов - nmap, tracemap, mrt, идентификация статуса tcp-портов (tcp-connect. syn-scan).	2	ПК-9, ПК-10	Контрольные вопросы и задания
5	Методы скрытого сканирования (stealth tcp scanning methods).	2	ПК-9, ПК-10	Контрольные вопросы и задания
6	Сканирование ip протокола. Идентификация прикладных служб. метод анализа стандартных приглашений (banner grabbing).	2	ПК-9, ПК-10	Контрольные вопросы и задания
7	Идентификация прикладных сетевых служб методом анализа особенностей реализации (smtp).	2	ПК-9, ПК-10	Контрольные вопросы и задания
8	Идентификация службы электронной почты.	2	ПК-9, ПК-10	Контрольные вопросы и задания
9	Активное исследование стека tcp/ip.	2	ПК-9, ПК-10	Контрольные вопросы и задания

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

Комплект оценочных средств по дисциплине «Оценка и контроль обеспечения информационной безопасности» 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 с оценкой, позволяющие провести процедуру измерения уровня знаний и умений обучающихся.

2. Перечень компетенций, формируемых в процессе изучения дисциплины «Оценка и контроль обеспечения информационной 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 экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента;		
Знать	Уметь	Владеть
- основные понятия, цели и задачи администрирования безопасности информационных систем, сущность и составляющие; - принципы организации и этапы процессов администрирования безопасности; факторы, влияющие на организацию защиты информации; - методы анализа и оценки угроз защищаемой информации; - технологические и организационные вопросы администрирования безопасности информационной системы, администрирование системы защиты; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - методы концептуального проектирования технологий обеспечения информационной безопасности	- определять состав программно-технических средств защиты информации; - выявлять угрозы защищаемой информации информационной системы, определять степень их опасности, разрабатывать стратегию администрирования системой защиты информации объектов с учетом условий ее функционирования; - использовать методы и средства, необходимые для организации управления и функционирования системы защиты информации; - реализовывать планы функционирования системы защиты информации, осуществлять ее текущее администрирование; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности	- современными программными средствами, в которых реализованы методы защиты информации информационных систем; - решать задачи профессиональной области, используя известные математические методы, программные и аппаратно-технические решения; - навыками управления информационной безопасностью простых объектов

ПК-10 – способностью оформлять научно-технические отчеты, обзоры, готовить публикации по результатам выполненных исследований, научные доклады.		
Знать	Уметь	Владеть
	- определять состав программно-технических средств защиты информации; - выявлять угрозы защищаемой информации информационной системы, определять степень их опасности, разрабатывать стратегию администрирования системой защиты информации объектов с учетом условий ее функционирования; - использовать методы и средства, необходимые для организации управления и функционирования системы защиты информации; - реализовывать планы функционирования системы защиты информации, осуществлять ее текущее администрирование; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности	- современными программными средствами, в которых реализованы методы защиты информации информационных систем; - решать задачи профессиональной области, используя известные математические методы, программные и аппаратно-технические решения; - 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 «Оценка и контроль обеспечения информационной безопасности»

Текущий контроль знаний, согласно «Положению о рейтинговой системе комплексной оценки знаний студентов в ВлГУ» (далее Положение) в рамках изучения дисциплины «Оценка и контроль обеспечения информационной 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 «Оценка и контроль обеспечения информационной безопасности» (письменный рейтинг-контроль)

Семестр 2

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

- Что понимается под идентификацией узлов корпоративной сети передачи данных?
- Какие протоколы стека TCP/IP могут применяться при идентификации узлов?
- Протокол ICMP. Назначение, формат пакета протокола ICMP.
- Назовите основные способы обнаружения узлов сети средствами протокола ICMP.
- Синтаксис и основные опции утилиты ping.
- Назовите основные недостатки применения утилиты ping при решении задачи идентификации узлов КСПД.
- Технология PING SWEEP, достоинства и недостатки.
- Синтаксис и основные опции утилиты fping.
- Синтаксис и основные режимы сетевого сканера nmap.
- Методы обнаружения узлов сети средством информационных запросов TimeStamp Request, Information Request, Address Mask Request.
- Протокол TCP, назначение, TCP соединение, флаги.
- Формат сегмента протокола TCP, TCP-порты.

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

- TCP-sweep. Достоинства и недостатки метода TCP-sweep.
- Синтаксис и основные опции утилиты hping3.
- Протокол UDP. Режим передачи данных без установления соединения.
- Формат дейтаграммы протокола UDP, UDP -порты.
- Метод UDP Discovery. Достоинства и недостатки метода.
- Протокол IP. Адресация.
- Формат пакета протокола IP.
- Метод идентификации с помощью IP фрагментов.
- Метод идентификации отправкой IP пакета ошибочной длины.
- Метод идентификации отправкой IP пакета неподдерживаемого протокола.
- Протокол ARP. Адресация канального уровня ISO OSI.
- Формат дейтаграммы ARP.
- Синтаксис и основные опции утилиты arping.

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

- Протокол ARP. Адресация канального уровня ISO OSI.
- Формат дейтаграммы ARP.
- Синтаксис и основные опции утилиты arping.
- Метод arping. Достоинства и недостатки.
- Методы определения маршрутов передачи данных в сетях TCP/IP.
- Утилиты определения маршрутов передачи данных в сетях TCP/IP.
- Метод определения маршрута Record Route. Достоинства и недостатки метода.
- Утилита traceroute. Принцип определения маршрутов.
- Использование протоколов ICMP и TCP при определении маршрутов.
- Утилита tcptraceroute.
- Сканер nmap как инструмент исследования топологии.
- Утилита tracemap. Визуализация маршрутов.
- Утилита диагностики сети mtr. Синтаксис и основные опции mrt.

Регламент проведения лабораторных работ

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Оценка и контроль обеспечения информационной 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 3 балла.

Критерии оценки для выполнения лабораторной работы:

- 2,4-3 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;

- 1,4-2,3 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;

- 0,7-1,3 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;

- 0,2-0,6 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 0,2 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 «Оценка и контроль обеспечения информационной безопасности» (лабораторные работы)

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

Лабораторная работа №1.Обнаружение узлов сети. ICMP echo request (Утилита PING)
-Что понимается под идентификацией узлов корпоративной сети передачи данных?
-Протокол ICMP. Назначение, формат пакета протокола ICMP.
-Назовите основные способы обнаружения узлов сети средствами протокола ICMP.
-Синтаксис и основные опции утилиты ping.
Лабораторная работа №2. Обнаружение узлов сети. ICMP echo request (Утилиты FPING и NMAP)
-Режимы идентификации версий прикладных служб сканера nmap
-Режимы OS fingerprinting сканера nmap.
-Синтаксис и основные опции утилиты fping.
-Синтаксис и основные режимы сетевого сканера nmap.
Лабораторная работа №3. Обнаружение узлов сети. Информационные ICMP сообщения
-Протокол ICMP. Назначение, формат пакета протокола ICMP.
Назовите основные способы обнаружения узлов сети средствами протокола ICMP.
Лабораторная работа №4. Обнаружение узлов сети средствами протокола TCP (TCP-PING)
-Протокол TCP, назначение, TCP соединение, флаги.
-Формат сегмента протокола TCP, TCP-порты.
-TCP-sweep. Достоинства и недостатки метода TCP-sweep.
Лабораторная работа №5. Обнаружение узлов сети средствами протоколов UDP (UDP-PING), IP
-Протокол UDP. Режим передачи данных без установления соединения.
-Формат дейтаграммы протокола UDP, UDP -порты.
-Метод UDP Discovery. Достоинства и недостатки метода.
Лабораторная работа №6. Обнаружение узлов сети средствами протокола ARP (ARP-PING)
-Протокол ARP. Адресация канального уровня ISO OSI.
-Формат дейтаграммы ARP.
-Синтаксис и основные опции утилиты arping.
Лабораторная работа №7. Основные средства определения маршрутов ip-пакетов - ping, traceroute
-Утилита traceroute. Принцип определения маршрутов.
-Утилита tcptraceroute.
-Сканер nmap как инструмент исследования топологии.
-Утилита tracemap. Визуализация маршрутов.
Лабораторная работа №8. Дополнительные средства определения маршрутов ip-пакетов - nmap, tracemap, mrt
-Использование протоколов ICMP и TCP при определении маршрутов.

-Утилита tcptraceroute.
-Сканер nmap как инструмент исследования топологии.
-Утилита tracemap. Визуализация маршрутов.
Лабораторная работа №9. Идентификация статуса tcp-портов (tcp-connect. Syn-scan)
-Методы определения маршрутов передачи данных в сетях TCP/IP.
-Утилиты определения маршрутов передачи данных в сетях TCP/IP.
-Метод Half-open SYN flag scanning.
Лабораторная работа №10. Методы скрытого сканирования (stealth tcp scanning methods)
-Состояния TCP соединения.
-Метод TCP Connect Scanning.
-Режим сканирования TCP Connect сканера nmap.
Лабораторная работа №11. Методы скрытого сканирования (ack probe scanning, tcp fragmentation scanning)
-ACK flag probe scanning.
-TCP fragmentation scanning.
-Режимы Stealth TCP scanning сканера nmap
Лабораторная работа №12. Методы сканирования udp-портов (udp port scanning). Сканирование ip протокола
-Реализация UDP Port Scanning сканером nmap. Опции и режимы сканера.
-Реализация UDP Port Scanning средствами утилит hping3 и netcat. Опции и режимы.
-Задача идентификации сетевых служб. Соответствие TCP/UDP-портов и сетевых служб.

Регламент проведения самостоятельной работы

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Оценка и контроль обеспечения информационной 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 «Оценка и контроль обеспечения информационной безопасности» (самостоятельная работа)

2 семестр:

№ пп	Раздел (тема) дисциплины	Виды СРС	Формы контроля СРС	Баллы по СРС
1	Обнаружение узлов сети. icmp echo request.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
2	Обнаружение узлов сети средствами протокола tcp (tcp-ping).	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
3	Обнаружение узлов сети средствами протокола arp (arp-ping).	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
4	Дополнительные средства определения маршрутов ip-пакетов - nmap, tracemap, mrt, идентификация статуса tcp-портов (tcp-connect. syn-scan).	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
5	Методы скрытого сканирования (stealth tcp scanning methods).	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
6	Сканирование ip протокола. Идентификация прикладных служб. метод анализа стандартных приглашений (banner grabbing).	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
7	Идентификация прикладных сетевых служб методом анализа особенностей реализации (smtp).	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
8	Идентификация службы электронной почты.	Работа с учебниками (учебными пособиями). Работа с конспектом лекций.	Письменный или устный опрос, проверка конспектов	3
9	Активное исследование стека tcp/ip.	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 (2 семестр):

1. Что понимается под идентификацией узлов корпоративной сети передачи данных?
2. Какие протоколы стека TCP/IP могут применяться при идентификации узлов?
3. Протокол ICMP. Назначение, формат пакета протокола ICMP.
4. Назовите основные способы обнаружения узлов сети средствами протокола ICMP.
5. Синтаксис и основные опции утилиты ping.
6. Назовите основные недостатки применения утилиты ping при решении задачи идентификации узлов КСПД.
7. Технология PING SWEEP, достоинства и недостатки.
8. Синтаксис и основные опции утилиты fping.
9. Синтаксис и основные режимы сетевого сканера nmap.

10. Методы обнаружения узлов сети средством информационных запросов TimeStamp Request, Information Request.
11. Протокол TCP, назначение, TCP соединение, флаги.
12. Формат сегмента протокола TCP, TCP-порты.
13. TCP-sweep. Достоинства и недостатки метода TCP-sweep.
14. Синтаксис и основные опции утилиты hping3.
15. Протокол UDP. Режим передачи данных без установления соединения.
16. Формат дейтаграммы протокола UDP, UDP -порты.
17. Метод UDP Discovery. Достоинства и недостатки метода.
18. Протокол IP. Адресация.
19. Формат пакета протокола IP.
20. Метод идентификации с помощью IP фрагментов.
21. Метод идентификации отправкой IP пакета ошибочной длины.
22. Метод идентификации отправкой IP пакета неподдерживаемого протокола.
23. Протокол ARP. Адресация канального уровня ISO OSI.
24. Формат дейтаграммы ARP.
25. Синтаксис и основные опции утилиты arping.
26. Метод arping. Достоинства и недостатки.
27. Методы определения маршрутов передачи данных в сетях TCP/IP.
28. Утилиты определения маршрутов передачи данных в сетях TCP/IP.
29. Метод определения маршрута Record Route. Достоинства и недостатки метода.
30. Утилита traceroute. Принцип определения маршрутов.
31. Использование протоколов ICMP и TCP при определении маршрутов.
32. Утилита tcptraceroute.
33. Сканер nmap как инструмент исследования топологии.
34. Утилита tracemap. Визуализация маршрутов.
35. Утилита диагностики сети mtr. Синтаксис и основные опции mrt.
36. Методы идентификации TCP портов узла КСПД.
37. Состояния TCP соединения.
38. Метод TCP Connect Scanning.
39. Режим сканирования TCP Connect сканера nmap.
40. Метод Half-open SYN flag scanning.
41. Режим сканирования Half-open SYN flag сканера nmap.
42. Достоинства и недостатки методов Stealth TCP scanning.
43. Методы Inverse TCP flag scanning.
44. ACK flag probe scanning.
45. TCP fragmentation scanning.
46. Режимы Stealth TCP scanning сканера nmap.
47. Методы идентификации UDP-портов узла КСПД.
48. Реализация UDP Port Scanning сканером nmap. Опции и режимы сканера.
49. Реализация UDP Port Scanning средствами утилит hping3 и netcat. Опции и режимы.
50. Задача идентификации сетевых служб. Соответствие TCP/UDP-портов и сетевых служб.
51. Методы идентификации версий прикладных служб. Services fingerprinting.
52. Метод banner grabbing. Достоинства и недостатки метода.
53. Методы анализа особенностей реализации прикладной службы.
54. Метод mail-bouncing. Идентификация службы электронной почты.
55. Сканер amap. Синтаксис, опции и режимы работы.
56. Утилита strobe. Синтаксис, опции и режимы работы.
57. Режимы идентификации версий прикладных служб сканера nmap.
58. Задача идентификации типа и версии ОС исследуемого узла КСПД.
59. Особенности методов активного исследования реализации стека протоколов TCP/IP. Достоинства и недостатки.

60. Суть метода TCP|FIN сканирования.
61. Суть метода исследования флагом BOGUS.
62. Суть метода исследования поля Window TCP заголовка принятого пакета.
63. Суть метода исследования изменения ISN ACK-пакета.
64. Утилита Xpobe2. Синтаксис, опции.
65. Режимы OS fingerprinting сканера nmap.
66. Особенности методов пассивного исследования реализации стека протоколов TCP/IP. Достоинства и недостатки.
67. Утилита p0f. Синтаксис, опции.

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

2 семестр

№	Пункт	Максимальное число баллов
1	Письменный рейтинг-контроль 1	10
2	Письменный рейтинг-контроль 2	10
3	Письменный рейтинг-контроль 3	10
4	Посещение занятий студентом	5
5	Дополнительные баллы (бонусы)	2
6	Лабораторные работы	36
7	Выполнение семестрового плана самостоятельной работы	27
	Всего	100

4. Показатели, критерии и шкала оценивания компетенций промежуточной аттестации знаний по учебной дисциплине «Оценка и контроль обеспечения информационной безопасности»

Регламент проведения промежуточного контроля (зачета с оценкой)

Промежуточная аттестация по итогам освоения дисциплины (зачет с оценкой) 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 с оценкой):

- 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 « Оценка и контроль обеспечения информационной безопасности» (зачёт)

Перечень вопросов к зачету:

1. Что понимается под идентификацией узлов корпоративной сети передачи данных?
2. Какие протоколы стека TCP/IP могут применяться при идентификации узлов?
3. Протокол ICMP. Назначение, формат пакета протокола ICMP.
4. Назовите основные способы обнаружения узлов сети средствами протокола ICMP.
5. Синтаксис и основные опции утилиты ping.
6. Назовите основные недостатки применения утилиты ping при решении задачи идентификации узлов КСПД.
7. Технология PING SWEEP, достоинства и недостатки.
8. Синтаксис и основные опции утилиты fping.
9. Синтаксис и основные режимы сетевого сканера nmap.
10. Методы обнаружения узлов сети средством информационных запросов TimeStamp Request, Information Request, Address Mask Request.
11. Протокол TCP, назначение, TCP соединение, флаги.
12. Формат сегмента протокола TCP, TCP-порты.
13. TCP-sweep. Достоинства и недостатки метода TCP-sweep.
14. Синтаксис и основные опции утилиты hping3.
15. Протокол UDP. Режим передачи данных без установления соединения.
16. Формат дейтаграммы протокола UDP, UDP -порты.
17. Метод UDP Discovery. Достоинства и недостатки метода.
18. Протокол IP. Адресация.
19. Формат пакета протокола IP.
20. Метод идентификации с помощью IP фрагментов.
21. Метод идентификации отправкой IP пакета ошибочной длины.
22. Метод идентификации отправкой IP пакета неподдерживаемого протокола.
23. Протокол ARP. Адресация канального уровня ISO OSI.
24. Формат дейтаграммы ARP.
25. Синтаксис и основные опции утилиты arping.
26. Метод arping. Достоинства и недостатки.
27. Методы определения маршрутов передачи данных в сетях TCP/IP.
28. Утилиты определения маршрутов передачи данных в сетях TCP/IP.
29. Метод определения маршрута Record Route. Достоинства и недостатки метода.
30. Утилита traceroute. Принцип определения маршрутов.
31. Использование протоколов ICMP и TCP при определении маршрутов.
32. Утилита tcptraceroute.
33. Сканер nmap как инструмент исследования топологии.
34. Утилита tracemap. Визуализация маршрутов.
35. Утилита диагностики сети mtr. Синтаксис и основные опции mrt.