ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Кафедра «Информационная безопасность»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.О.37 «Основы построения защищенных компьютерных сетей»

Направление подготовки – 10.05.00 «Компьютерная безопасность»

Специальность – 10.05.01 «Компьютерная безопасность»

Специализация: № 5 Разработка систем защиты информации компьютерных систем объектов информатизации" (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника - специалист

Форма обучения – очная

Рязань 2025 г.

1 ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур), предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной профессиональной образовательной программы.

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций, обучающихся целям и требованиям основной профессиональной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных, общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины (модуля), организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков, приобретенных обучающимися в ходе выполнения индивидуальных заданий на практических занятиях. Количество практических работ и их тематика определена рабочей программой дисциплины.

Результат выполнения каждого индивидуального задания должен соответствовать всем критериям оценки в соответствии с компетенциями, установленными для заданного раздела дисциплины.

Промежуточный контроль по дисциплине осуществляется проведением теоретического зачета. Форма проведения - тестирование, письменный опрос по теоретическим вопросам и выполнение практических заданий.

2 ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Сформированность каждой компетенции (или ее части) в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1) пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

2) продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

3) эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

Уровень освоения компетенций, формируемых дисциплиной:

Описание критериев и шкалы оценивания тестирования:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 85 до 100%
2 балла (продвинутый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 70 до 84%
1 балл (пороговый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 50 до 69%
0 баллов	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 0 до 49%

Описание критериев и шкалы оценивания теоретического вопроса:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	выставляется студенту, который дал полный ответ на вопрос, показал глубокие систематизированные знания, смог привести примеры, ответил на дополнительные вопросы преподавателя
2 балла (продвинутый уровень)	выставляется студенту, который дал полный ответ на вопрос, но на некоторые дополнительные вопросы преподавателя ответил только с помощью наводящих вопросов
1 балл (пороговый уровень)	выставляется студенту, который дал неполный ответ на вопрос в билете и смог ответить на дополнительные вопросы только с помощью преподавателя
0 баллов	выставляется студенту, который не смог ответить на вопрос

Описание критериев и шкалы оценивания практического задания:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	Задача решена верно
2 балла (продвинутый уровень)	Задача решена верно, но имеются неточности в логике решения
1 балл (пороговый уровень)	Задача решена верно, с дополнительными наводящими вопросами преподавателя
0 баллов	Задача не решена

На промежуточную аттестацию (экзамен) выносится тест (10 вопросов), два теоретических вопроса и 2 задачи. Максимально студент может набрать 15 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» выставляется студенту, который набрал в сумме 15 баллов (выполнил все задания на эталонном уровне). Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «хорошо» выставляется студенту, который набрал в сумме от 10 до 14 баллов при условии выполнения всех заданий на уровне не ниже продвинутого. Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «удовлетворительно» выставляется студенту, который набрал в сумме от 5 до 9 баллов при условии выполнения всех заданий на уровне не ниже порогового. Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «неудовлетворительно» выставляется студенту, который набрал в сумме менее 5 баллов или не выполнил всех предусмотренных в течение семестра практических заданий.

3 ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)/ индикатора	Вид, метод, форма оценочного мероприятия
1	Введение	ОПК-2 (ОПК-2.1, ОПК-2.2), ОПК-5 (ОПК-5.3), ОПК-15 (ОПК-15.4, ОПК-15.5), ОПК-16 (ОПК-16.1, ОПК-16.2)	экзамен
2	Основы законодательства РФ в области информационной безопасности компьютерных сетей	ОПК-2 (ОПК-2.1, ОПК-2.2), ОПК-5 (ОПК-5.3), ОПК-15 (ОПК-15.4, ОПК-15.5), ОПК-16 (ОПК-16.1, ОПК-16.2)	экзамен
3	Технологии построения локальных защищенных компьютерных сетей	ОПК-2 (ОПК-2.1, ОПК-2.2), ОПК-5 (ОПК-5.3), ОПК-15 (ОПК-15.4, ОПК-15.5), ОПК-16 (ОПК-16.1, ОПК-16.2)	зэкзамен
4	Технологии построения распределенных защищенных компьютерных сетей	ОПК-2 (ОПК-2.1, ОПК-2.2), ОПК-5 (ОПК-5.3), ОПК-15 (ОПК-15.4, ОПК-15.5), ОПК-16 (ОПК-16.1, ОПК-16.2)	экзамен

4 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

4.1. Промежуточная аттестация в форме экзамена

Код компетенции/ индикаторов	Результаты освоения ОПОП Содержание компетенций
ОПК-2 (ОПК-2.1, ОПК-2.2)	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности ОПК-2.1 Анализирует информационную инфраструктуру объектов профессиональной деятельности ОПК-2.2 Выбирает основные защитные механизмы и средства обеспечения информационной безопасности объектов профессиональной деятельности

Типовые тестовые вопросы:

1. Как называется состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства?
а) информационная безопасность
б) государственная безопасность
+ в) национальная безопасность
г) общественная безопасность

2. Какой орган исполнительной власти осуществляет контроль в области криптографической защиты информации?
а) Роскомнадзор
б) ФСТЭК России
+ г) ФСБ России
д) МВД России

3. Обладатели информации (впоследствии – заявители), в соответствии с Федеральным законом Российской Федерации "Об информации, информационных технологиях и о защите информации" от 27.07.2006 №149-ФЗ, в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:
+ а) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации
б) несвоевременное обнаружение фактов несанкционированного доступа к информации;
в) возможность воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
г) непостоянный контроль за обеспечением уровня защищенности информации.

4. Какое наименование Федерального закона от 27 июля 2006 г. N 149-ФЗ
а) «О безопасности критической информационной инфраструктуры Российской Федерации»
б) «О персональных данных»
+ в) «Об информации, информационных технологиях и о защите информации»
г) «О государственной тайне»

5. Целью защиты объекта информатизации является:
+ а) предотвращение утечки информации по техническим каналам и защиты ее от несанкционированного доступа или непреднамеренного воздействия на нее;
б) подтверждение соответствия реализованной на объекте информатизации системы защиты информации уровню безопасности информации, заданному владельцем объекта информатизации, исходя из требований по защите информации, установленных законодательством Российской Федерации;
в) обеспечение конфиденциальности, целостности, доступности, подлинности и безотказности информации;
г) ничего из вышеперечисленного.

6. Согласно ФЗ N 149-ФЗ «Об информации, информационных технологиях и о защите информации» понятие «Информация» - это:
+ а) сведения (сообщения, данные) независимо от формы их представления;
б) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
в) возможность получения информации и ее использования;
г) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

7. Согласно ФЗ N 149-ФЗ «Об информации, информационных технологиях и о защите информации» понятие «Информационная система» - это:
а) сведения (сообщения, данные) независимо от формы их представления;

б) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
в) возможность получения информации и ее использования;
+ г) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

8. Что служит документальным основанием для начала сертификационных испытаний технического средства защиты информации?
а) договор с федеральным органом сертификации
+ б) решение на проведение сертификационных испытаний
в) разрешение на проведение сертификационных испытаний
г) оплата госпошлины

9. В Федеральном законе Российской Федерации "О лицензировании отдельных видов деятельности" от 04.05.2011 № 99-ФЗ сказано, что основанием для включения плановой проверки лицензиата в ежегодный план проведения плановых проверок является:
+ а) истечение одного года со дня принятия решения о предоставлении лицензии или переоформлении лицензии;
б) истечение двух лет со дня окончания последней плановой проверки лицензиат;
в) истечение четырех лет со дня окончания последней плановой проверки лицензиата;
г) ничего из вышеперечисленного.

10. По документам ФСТЭК количество классов защищенности средств вычислительной техники от НСД к информации
а) 9
+ б) 6
в) 8
г) 7

Типовые теоретические вопросы:

1. Основные этапы разработки политики безопасности.
2. Основные нормативные документы по разработке политики безопасности.

Типовые практические задания:

1. Дайте общую характеристику известного Вам нормативно-правового акта РФ (реквизиты, структура, регулируемые отношения, субъекты, понятия, приведенные в качестве нормативных и др)
2. Определять место нормативно – правового акта выбранного в задании 1 в системе права РФ.

Код компетенции/ индикаторов	**Результаты освоения ОПОП Содержание компетенций**
ОПК-5 (ОПК-5.3)	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации ОПК-5.3 Применяет основы законодательства РФ в области обеспечения информационной безопасности компьютерных систем

Типовые тестовые вопросы:

1. На каком из уровней OSI не происходит фильтрация
+а) сеансовый
б) сетевой
в) транспортный
г) канальный

2. На каком из уровней модели TCP/IP функционируют протоколы HTTP, RTSP, FTP, DNS

+ а) прикладной
б) транспортный
в) сетевой
г) канальный

3. Что из нижеперечисленного не входит в классификацию сетевых атак?

а) пассивная атаки
б) нарушение конфиденциальности ИР
в) атака по запросу атакуемого объекта
+ г) атака с заминкой

4. Какой из этих протоколов относится к группе протоколов междоменной маршрутизации?

а) EIGRP
б) OSPF
в) RIP
+ г) EGP

5. Автономная система (AS) - это:

+ а) часть сети Интернет, охватывающая определенное административно-территориальное образование
б) локальная сеть, не связанная с глобальными сетями
в) сеть или несколько сетей, использующих один и тот же протокол маршрутизации
г) локальная сеть с автономными источниками питания

6. Фильтр пакетов (вид межсетевого экрана) использует для принятия решений:

а) информацию канального уровня
б) информацию сетевого уровня
+ в) информацию транспортного уровня
г) информацию прикладного уровня

7. Режим trunk будет установлен в том случае, если соседний порт находится в режимах *on, desirable, auto* если сам порт находится в режиме

+ а) desirable
б) trunk
в) nonegotiate
г) auto

8. Какой из этих протоколов не относится к протоколам состояния каналов связи?

а) OSPF
+ б) BGP
в) CARP
г) IS-IS

9. Какого типа области не существует в OSPF-сетях?

+ а) совсем не тупиковая область
б) тупиковая область
в) полностью, но не совсем тупиковая область
г) не совсем тупиковая область

10. Какого типа VPN не существует?
а) Канального уровня
б) Сетевого уровня
+ в) Прикладного уровня
г) Сеансового уровня

Типовые теоретические вопросы:

1. Модель OSI. Семь уровней модели OSI.
2. Виртуальные локальные сети VLAN.
3. Виртуальные локальные сети. Протокол VTP.
4. Маршрутизация. Основные понятия. Статическая маршрутизация.

Типовые практические задания:

1. Для подсети используется маска 255.255.255.0. Сколько различных адресов компьютеров допускает эта маска?
2. Маска имеет значение 255.255.255.224, IP-адрес - 162.198.0.155. Определить порядковый номер устройства в сети.

Код компетенции/ индикаторов	**Результаты освоения ОПОП Содержание компетенций**
ОПК-15 (ОПК-15.4, ОПК-15.5)	Способен администрировать компьютерные сети и контролировать корректность их функционирования ОПК-15.4 Использует и настраивает средства защиты информации в компьютерных сетях ОПК-15.5 Проводит анализ и выбор средств защиты информации компьютерных систем и сетей

Типовые тестовые вопросы:

1. Конфигурация из нескольких компьютеров, выполняющих общее приложение, называется
а) суперсервером
+ б) кластером
в) сервером
г) сетью

2. Из перечисленного субъектами для монитора обращений являются: 1) терминалы; 2) программы; 3) файлы; 4) задания; 5) порты; 6) устройства
а) 1, 2, 3
б) 2, 3, 5
+ в)1, 2, 5
г) 4, 5, 6

3. Из перечисленного система защиты электронной почты должна: 1) обеспечивать все услуги безопасности; 2) обеспечивать аудит; 3) поддерживать работу только с лицензионным ПО; 4) поддерживать работу с почтовыми клиентами; 5) быть кроссплатформенной
а) 2, 3, 4
б) 1, 3, 5
+ в) 1, 4, 5
г) 1, 2, 3

4. Система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую, называется
+ а) брандмауэром
б) браузером
в) маршрутизатором
г) фильтром

5. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это
а) аудит
+ б) аутентификация
в) авторизация
г) идентификация

6. Сетевой службой, предназначенной для централизованного решения задач аутентификации и авторизации в крупных сетях, является
а) SendMail
б) Net Logon
+ в) Kerberos
г) Network DDE

7. Основу политики безопасности составляет
а) программное обеспечение
б) управление риском
+ в) способ управления доступом
г) выбор каналов связи

8. Присвоение субъектам и объектам доступа уникального номера, шифра, клда и т.п. с целью получения доступа к информации — это
+ а) идентификация
б) аудит
в) аутентификация
г) авторизация

9. Адаптивная безопасность сети обеспечивается следующими из предложенных элементами: (1) технологиями анализа защищенности, (2) технологиями обнаружения атак, (3) технологиями управления рисками
+ а) 1,2,3
б) 2
в) 1,3
г) ничем из перечисленного
10. Типовая архитектура системы обнаружения атак включает в себя
а) система специального реагирования на обнаруженные атаки
+б) модули-датчики, предназначенные для сбора необходимой информации о функционировании ИС
в) все модули, не выполняющие функции управления компонентами системы обнаружения атак.
г) база данных, содержащая информацию о пользователях системы

Типовые теоретические вопросы:

1. Назовите защитные механизмы. Как их можно классифицировать?
2. Охарактеризуйте динамический и статический анализ безопасности приложения. В чем их принципиальная разница?

Типовые практические задания:

1. Определить требования к политике безопасности РГРТУ
2. Составить испытание программных средств на наличие компьютерных вирусов

Код компетенции/ индикаторов	Результаты освоения ОПОП Содержание компетенций
ОПК-16 (ОПК-16.1, ОПК-16.2)	Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях ОПК-16.1 Определяет информационную инфраструктуру и информационные ресурсы компьютерных систем и сетей, подлежащие защите ОПК-16.2 Выявляет угрозы безопасности компьютерных систем и сетей

1. Аттестационные комиссии формируются:
+ а) органом по аттестации, как из числа штатных сотрудников органа по аттестации, так и специалистов других предприятий и организаций;
б) органом по аттестации только из числа штатных сотрудников;
в) органом по аттестации из числа штатных сотрудников, имеющие достаточные теоретические знания в области защиты информации, необходимые для аттестации конкретного объекта информатизации, но не имеющие практический опыт проведения аналогичных работ и не участвующие непосредственно в деятельности заявителей;
г) ничего из вышеперечисленного.

2. Перечень сведений, относимых к государственной тайне утверждается:
а) Правительством РФ
б) ФСТЭК
в) ФСБ
+ г) Президентом РФ

3. Какое наименование Федерального закона от 27 июля 2006 г. N 149-ФЗ
а) «О безопасности критической информационной инфраструктуры Российской Федерации»
б) «О персональных данных»
+ в) «Об информации, информационных технологиях и о защите информации»
г) «О государственной тайне»

4. Сфера действия Федерального закона от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
а) Применение информационных технологий;
+ б) Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также - критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.
в) Обеспечение защиты информации;
г) Осуществление права на поиск, получение, передачу, производство и распространение информации.

5. Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне

а) Е5
б) Е7
в) Е4
+г) Е6

6. По документам ФСТЭК количество классов защищенности автоматизированных систем от НСД
а) 8
б) 7
+ в) 9
г) 6

7. Каждое сертифицированное средство защиты информации подлежит маркированию специальным номерным защитным знаком соответствия, который производитель (заявитель) получает:
+ а) во ФСТЭК России;
б) в ФСБ России;
в) в Центре сертификации;
г) ничего из вышеперечисленного.

8. Как называется юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности?
а) соискатель лицензии
б) правообладатель
в) регулятор
+ г) лицензиат

9. Что служит документальным основанием для начала сертификационных испытаний технического средства защиты информации?
а) договор с федеральным органом сертификации
+ б) решение на проведение сертификационных испытаний
в) разрешение на проведение сертификационных испытаний
г) оплата госпошлины

10. Какой участник системы сертификации создает системы сертификации в целом?
+ а) федеральный орган по сертификации
б) центральный орган системы сертификации
в) испытательная лаборатория
г) изготовитель

Типовые теоретические вопросы:

1. Основные этапы разработки политики безопасности.
2. Основные нормативные документы по разработке политики безопасности.

Типовые практические задания:

1. Определить требования политики безопасности паспортного стола
2. Определить требования политики безопасности пункта скорой помощи

4.2. Задания курсового проекта

Для заданного варианта задания на курсовой проект работу необходимо решить следующие задачи построения защищенной компьютерной сети.

Темы курсового проекта

1. Проектирование вычислительной сети, защищенной от наводок извне, утечки за счет ПЭМИ, проблем в системе электропитания.
2. Проектирование сети организации, состоящей из нескольких изолированных подразделений,с разграничением доступа и приоритезацией трафика на основе VLAN.
3. Проектирование сети на основе технологии IPv6, обеспечивающей сосуществование IPv4 и IPv6 и переход на IPv6.
4. Проектирование сети, защищенной прокси-сервером, с функциями разграничения доступа и анонимизации.
5. Проектирование сети, защищенной с помощью технологии трансляции адресов NAT с возможностью сокрытия структуры сети и препятствования выявлению ОС сетевых хостов.
6. Развертываие сети на основе технологии IPsec
    a. в режиме AH;
    b. в режиме ESP;
    c. в режиме тоннеля;
    d. в режиме точка-точка.
7. Обеспечение доступа к системе по протоколу SSH
    a. в режиме консоли команд;
    b. с идентификацией и аутентификацией по сертификату пользователя;
    c. в режиме проброса портов;
    d. в режиме sftp-сервера;
    e. в режиме scp-сервера.
8. Создание VPN тоннеля на основе протокола L2TP
    a. на уровне 3 (IP);
    b. на уровне 2 (Ethernet).
9. Создание виртуального распределенного коммутатора (Virtual Distributed Switch).
10. Обеспечение идентификации/аутентификации и ограничение времени работы клментов с помощью сервера RADIUS.
11. Построение защищенной сети с использованием технологии 802.1X
    a. в режиме PSK;
    b. в режиме Enterprise.
12. Обеспечение доступности с помощью шейпинга трафика узлов сети.
13. Сбор информации о хосте/сети с помощью сканера Nmap.
14. Создание реплицируемого DNS-сервера.
15. Создание DNS-зоны с использованием технологии DNSsec.
16. Построение защищенной системы IP-телефонии.
17. Обеспечение доступности высоконагруженного web-сайта с помощью программы nginx.
18. Обеспечение доверенного источника точного времени сети с помощью протокола NTP.
19. Создание удостоверяющего центра для защиты сети с помощью OpenSSL
20. Создание защищенного WEB-сервера с помощью протокола HTTPS.

Критерии выполнения курсовой работы

Результаты курсового проектирования оцениваются с учетом:

1) качества и полноты выполнения пояснительной записки;
2) наличия работающей программы;
3) уровня ответов студента.

Составил
к.т.н., доцент кафедры
«Информационная безопасность» Ю.В. Конкин