ПРИЛОЖЕНИЕ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Рязанский государственный радиотехнический университет имени В.Ф. Уткина»

КАФЕДРА «ЭЛЕКТРОННЫЕ ВЫЧИСЛИТЕЛЬНЫЕ МАШИНЫ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

«ЗАЩИТА ИНФОРМАЦИИ СПЕЦИАЛЬНЫХ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ ОБЪЕКТОВ»

Специальность

27.05.01 Специальные организационно-технические системы

Специализация

Информационные технологии и программное обеспечение в специальных организационно-технических системах

Квалификация (степень) выпускника — инженер-системотехник

Форма обучения — очная, очно-заочная

1. ОБЩИЕ ПОЛОЖЕНИЯ

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

Цель – оценить соответствие знаний, умений и владений, приобретенных обучающимся в процессе изучения дисциплины, целям и требованиям ОПОП в ходе проведения промежуточной аттестации.

Промежуточный контроль по дисциплине осуществляется путем проведения экзамена, зачета. Форма проведения экзамена – тестирование и выполнение практических заданий. При необходимости, проводится теоретическая беседа с обучаемым для уточнения оценки. Выполнение заданий на практических занятиях в течение семестра и заданий на самостоятельную работу является обязательным условием для допуска к экзамену.

2. ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции (или её части)	Наименование оценочного средства
Тема 1 Основы компьютерных сетей	ПК-2.1, ПК-2.3	Зачет
Тема 2 Адресация в сетях	ПК-2.1, ПК-2.3	Зачет
Тема 3 Технологии канального уровня	ПК-2.1, ПК-2.3	Зачет
Тема 4 Технологии коммутации	ПК-2.1, ПК-2.3	Экзамен
Тема 5 Технологии маршрутизации	ПК-2.1, ПК-2.3	Экзамен
Тема 6 Глобальные сети	ПК-2.1, ПК-2.3	Экзамен
Тема 7 Беспроводные сети	ПК-2.1, ПК-2.3	Экзамен

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Сформированность каждой компетенции 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.

Описание критериев и шкалы оценивания промежуточной аттестации

а) описание критериев и шкалы оценивания тестирования:

За каждый тестовый вопрос назначается максимально 1 балл в соответствии со следующим правилом:

- 1 балл – ответ на тестовый вопрос полностью правильный;
- 0,5 балла – отчет на тестовый вопрос частично правильный (выбраны не все правильные варианты, указаны частично верные варианты);
- 0 баллов – ответ на тестовый вопрос полностью не верный.

б) описание критериев и шкалы оценивания решения практического задания:

Шкала оценивания	Критерий
5 баллов (эталонный уровень)	Задание выполнено верно, полностью самостоятельно, без дополнительных наводящих вопросов преподавателя
3 балла (продвинутый уровень)	Задание выполнено верно, но имеются технические неточности
1 балл	Задание выполнено верно, с дополнительными наводящими

(пороговый уровень)	вопросами преподавателя
0 баллов	Задание не выполнено

На промежуточную аттестацию (экзамен) выносится 20 тестовых вопросов, два практических задания. Максимально студент может набрать 30 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 25 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 18 до 24 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 10 до 17 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 10 баллов или не выполнил всех предусмотренных в течение семестра практических заданий.

На промежуточную аттестацию (зачет) выносится 20 тестовых вопросов. Максимально студент может набрать 20 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «зачтено» и «не зачтено».

Оценка «зачтено» 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 «не зачтено» выставляется студенту, который набрал в сумме менее 15 баллов или не выполнил всех предусмотренных в течение семестра практических заданий.

4. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

4.1. Промежуточная аттестация

Коды компетенций	Результаты освоения ОПОП Содержание компетенций
ПК-2	Способен осуществлять проектирование и модернизацию информационно-коммуникационной системы
ПК-2.1	Выполняет прогнозирование и оценку текущих требований к информационно-коммуникационной системе
ПК-2.3	Разрабатывает дизайн информационно-коммуникационной системы, в том числе с учетом требований информационной безопасности

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

11. Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев
а) D
б) A
в) B
+г) C

12. Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне
а) E5
б) E7
в) E4
+г) E6

13. Согласно «Европейским критериям» минимальную адекватность обозначает уровень
а) E1
б) E7
+ в) E0
г) E6

14. Согласно «Оранжевой книге» уникальные идентификаторы должны иметь
а) наиболее важные субъекты
б) наиболее важные объекты
+в) все субъекты
г) все объекты

15. Согласно «Оранжевой книге» минимальную защиту имеет группа критериев
а) C
б) A
в) B
+г) D

16. Организационные требования к системе защиты
а) управленческие и идентификационные
б) административные и аппаратурные
+ в) административные и процедурные
г) аппаратурные и физические

17. Надежность СЗИ определяется
а) усредненным показателем

+ б) самым слабым звеном
в) количеством отраженных атак
г) самым сильным звеном

18. Если средство защиты способно противостоять отдельным атакам, то согласно «Европейским критериям» безопасность считается
а) низкой
б) средней
в) стандартной
+ г) базовой

19. Из перечисленных классов: 1) обнаруживаемые операционной системой при загрузке; 2) качественные и визуальные; 3) аппаратные; 4) обнаруживаемые средствами тестирования и диагностики — признаки присутствия программной закладки в компьютере можно разделить на
а) 1,4
б) 1,3
в) 2,3
+ г) 2,4

20. Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются: 1) аутентификация; 2) идентификация; 3) целостность; 4) контроль доступа; 5) контроль трафика; 6) причастность
+ а) 1,3,4,6
б) 2,5,6
в) 1,2,3,4
г) 1,3,5

21. 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

22. 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

23. 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

24. Сетевой службой, предназначенной для централизованного решения задач аутентификации и авторизации в крупных сетях, является

а) SendMail
б) Net Logon
+ в) Kerberos
г) Network DDE

25. Основу политики безопасности составляет
а) программное обеспечение
б) управление риском
+ в) способ управления доступом
г) выбор каналов связи
26. 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

27. 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
28. 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. Основные этапы разработки политики безопасности.
2. Основные нормативные документы по разработке политики безопасности.
3. Назовите защитные механизмы. Как их можно классифицировать?
4. Охарактеризуйте динамический и статический анализ безопасности приложения. В чем их принципиальная разница?

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