ПРИЛОЖЕНИЕ

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

Б.О.21 «Спецдисциплина № 1 – Техническая защита информации»
Направление подготовки – 10.00.00 «Компьютерная безопасность»

Специальность – 10.05.01 «Компьютерная безопасность»

Специализация №8 «Информационная безопасность объектов информатизации на базе компьютерных систем»

Квалификация выпускника - специалист

Форма обучения - очная

Рязань, 2021 г.

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 и лабораторных работах. При оценивании результатов освоения практических занятий и применяется шкала оценки «зачтено – не зачтено». 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.

Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1.	Тема 1. Введение в техническую защиту информации	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	зачет
2.	Тема 2. Утечка информации посредством ПЭМИН	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	зачет
3.	Тема 3. Утечка информации по цепям электропитания и заземления	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	зачет
4.	Тема 4. Технические каналы утечки акустической речевой информации	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	зачет
5.	Тема 5. Технические каналы утечки видовой информации	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	зачет
6.	Тема 6. Демаскирующие признаки объектов	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	зачет
7.	Тема 7. Методы выявления технических каналов утечки информации	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	зачет
8.	Тема 8. Средства выявления каналов утечки информации	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	зачет
9.	Тема 9. Методы и средства защиты информации от утечки по прямому акустическому каналу	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	экзамен

10.	Тема 10. Методы и средства защиты информации от утечки за счет ПЭМИН	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	экзамен
11.	Тема 11. Методы и средства защиты информации от утечки по проводным каналам	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	экзамен
12.	Тема 12. Методы и средства защиты информации видимого и инфракрасного спектров	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	экзамен
13.	Тема 13. Методы и средства выявления закладочных устройств	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	экзамен
14.	Тема 14. Технический контроль эффективности мер защиты информации	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	экзамен
15.	Тема 15. Сертификация средств защиты информации	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	экзамен
16.	Тема 16. Аттестация объектов информатизации	ОПК-8.7, ОПК-9.3, ОПК-9.4, ОПК 9.9	экзамен

Показатели и критерии обобщенных результатов обучения

Коды компетен-ции	Результаты освоения ООП. Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОПК-8.7	Использует при решении профессиональных задач знания математического аппарата теории информации, математических моделей сигнала, моделей и характеристик источников сообщений и каналов связи	Знать: методы применения к решению профессиональных задач знаний теории информации, математических моделей сигнала, моделей и характеристик сообщений и каналов связи Уметь: применять методы математического аппарата теории связи, модели сигнала и источников сообщений, каналов связи при решении профессиональных задач Владеть: навыками применения методов математического аппарата теории связи, моделей сигнала и источников сообщений, каналов связи при решении профессиональных задач
ОПК-9.3	Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов и средств защиты информации от утечки по техническим каналам	Знать: методы и инструменты решений задач профессиональной деятельности с учетом актуального состояния и тенденций развития методов и средств защиты информации от утечки по техническим каналам Уметь: применять на практике актуальные и перспективные методы и инструменты защиты информации от утечки по техническим каналам при решении решений задач профессиональной деятельности Владеть: навыками использования актуальных и перспективных методов и инструментов защиты информации от утечки по техническим каналам при решении решений задач профессиональной деятельности
ОПК-9.4	Решает задачи профессиональной деятельности, используя радиотехнические системы, с учетом текущего состояния развития методов и средств защиты информации от утечки по техническим каналам	Знать: актуальные и перспективные методы и средства использования радиотехнических систем при решении профессиональных задач Уметь: использовать актуальные и перспективные методы и средства радиотехнических систем при решении профессиональных задач Владеть: навыками использования актуальных и перспективных методов и средств радиотехнических систем при решении профессиональных задач
ОПК-9.9	Использует средства защиты информации от утечки по техническим каналам при решении профессиональных задач	Знать: методы использования средств защиты информации от утечки по техническим каналам, необходимые для решения профессиональных задач Уметь: применять средства защиты информации от утечки по техническим каналам для решения профессиональных задач Владеть: навыками использования средств защиты информации от утечки по техническим каналам при решении профессиональных задач

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 (зачет) 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 «зачтено», «не зачтено».

Шкала оценки сформированности компетенций

В процессе оценки сформированности знаний, умений и навыков обучающегося по дисциплине, производимой на этапе промежуточной аттестации в форме теоретического зачета, используется оценочная шкала «зачтено – не зачтено»:

Оценки «зачтено» заслуживает обучающийся, продемонстрировавший полное знание материала изученной дисциплины, усвоивший основную литературу, рекомендованную рабочей программой дисциплины; показавшему систематический характер знаний по дисциплине, ответившему на все вопросы билета или допустившему погрешность в ответе вопросы, но обладающему необходимыми знаниями для их устранения под руководством преподавателя;

Дополнительным условием получения оценки «зачтено» могут стать хорошие успехи при выполнении практических работ, систематическая активная работа на практических занятиях.

Оценка «зачтено» выставляется студенту, набравшему 8 и более баллов при промежуточной аттестации

Оценки «не зачтено» заслуживает обучающийся, продемонстрировавший серьезные пробелы в знаниях основного материала изученной дисциплины, не ответивший на все вопросы билета и дополнительные вопросы. Как правило, оценка «не зачтено» ставится обучающимся, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине (формирования и развития компетенций, закрепленных за данной дисциплиной).

Оценка «не зачтено» выставляется студенту, набравшему менее 8 баллов при промежуточной аттестации

На промежуточную аттестацию (экзамен) выносится тест, 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.

Код компетенции	Результаты освоения ОПОП Содержание компетенций
ОПК-8.7	Использует при решении профессиональных задач знания математического аппарата теории информации, математических моделей сигнала, моделей и характеристик источников сообщений и каналов связи

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. В соответствии с ГОСТом Р 53114-2008 "Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения", введенным в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. N 532-ст, цель информационной безопасности (организации) – это:
а) обеспечение конфиденциальности, целостности, доступности, подлинности и безотказности информации;
+ б) заранее намеченный результат обеспечения информационной безопасности организации в соответствии с установленными требованиями в политике информационной безопасности (организации)
в) обеспечение подлинности, подотчётности, невозможности отказа, достоверности;
г) а), б), в) – верны.

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. Согласно ФЗ N 149-ФЗ «Об информации, информационных технологиях и о защите информации» обладатель информации при осуществлении своих прав обязан:
а) соблюдать права и законные интересы иных лиц;
б) принимать меры по защите информации;
в) ограничивать доступ к информации, если такая обязанность установлена федеральными законами;
+г) а), б), в) – верны

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. 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.

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	Результаты освоения ОПОП Содержание компетенций
ОПК-9.3	Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов и средств защиты информации от утечки по техническим каналам

Типовые тестовые вопросы:

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

Код компетенции	Результаты освоения ОПОП Содержание компетенций
ОПК-9.4	Решает задачи профессиональной деятельности, используя радиотехнические системы, с учетом текущего состояния развития методов и средств защиты информации от утечки по техническим каналам

Типовые тестовые вопросы:

1. Формирование политики безопасности организации относится к:
+ а) организационным мерам обеспечения безопасности
б) техническим мерам обеспечения безопасности
в) техническим мерам обеспечения безопасности
г) правовым мерам обеспечения безопасности

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

3. С точки зрения ФСТЭК основной задачей средств безопасности является обеспечение
а) сохранности информации
+ б) защиты от НСД
в) простоты реализации
г) надежности функционирования

4. На какой срок выдается лицензия на техническую защиту конфиденциальной информации?
а) 1 год
б) 5 лет
в)3 года
+ г) бессрочная

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. Преднамеренной угрозой безопасности информации является
+ а) несанкционированное копирование конфиденциальной информации
б) наводнение
в) повреждение кабеля, по которому идет передача, в связи с погодными условиями
г) ошибка администратора

7. По способу выявления атаки системы обнаружения атак принято делить на следующие категории:
а) обнаружение атак на уровне хоста и обнаружение атак на уровне приложения
+ б) обнаружение аномального поведения и обнаружение злоупотреблений
в) обнаружение атак на уровне сети и обнаружение атак на уровне хоста
г) обнаружение атак на уровне сети и обнаружение атак на уровне приложения

8. Контролируемая зона - это
а) Охраняемая территория
+ б) Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.
в) Пространство (территория, здание, часть здания), в котором исключено пребывание лиц, не имеющих постоянного или разового допуска.
г) Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц.

9. Технический канал утечки информации:
а) Получение защищаемой информации заинтересованными субъектами с нарушением установленных нормативными документами прав разграничения доступа к защищаемой информации.
б) Неконтролируемое распространение защищаемой информации в результате получения защищаемой информации иностранными разведками.
в) Получение защищаемой информации заинтересованными субъектами с нарушением установленных нормативными документами прав разграничения доступа к защищаемой информации
+г) Совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

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

Типовые теоретические вопросы:

1. Какие меры технической защиты информации применимы на объектах информатизации на базе компьютерных сетей?
2. Какие способы технической защиты информации применяются для защиты от утечки по техническим каналам?

Типовые практические задания:

1. Настроить выбранное техническое средство защиты информации по заданию преподавателя
2. Составить план мероприятий по организации технической защиты информации от утечки по техническим каналам

составил
доцент кафедры
«Информационная безопасность» А.А. Бубнов

Заведующий кафедрой
«Информационная безопасность» В.Н. Пржегорлинский