ПРИЛОЖЕНИЕ

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

Кафедра «Вычислительная и прикладная математика»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ
«Защита информации»

Направление подготовки
09.03.03 «Прикладная информатика»
Направленность (профиль) подготовки
Прикладная информатика

Квалификация выпускника – бакалавр

Форма обучения – очная, заочная

Рязань

1 ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов и процедур, предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной образовательной программы.

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

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

Контроль знаний обучающихся проводится в форме промежуточной аттестации – зачета в 8-м семестре.

2 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.

Уровень освоения компетенций, формируемых дисциплиной

а) 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 75 до 84%
1 балл (пороговый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 60 до 74%
0 баллов	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 0 до 59%

б) 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

в) описание критериев и шкалы оценивания практического задания:

Шкала оценивания	**Критерий**
3 балла (эталонный уровень)	Задание решено верно
2 балла (продвинутый уровень)	Задание решено верно, но имеются технические неточности в выполнении
1 балл (пороговый уровень)	Задание решено верно, с дополнительными наводящими вопросами преподавателя
0 баллов	Задание не решено

На зачет выносится: тестовое задание, 1 практическое задание и 1 теоретический вопрос.

Студент может набрать максимум 9 баллов.

Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «зачтено», «не зачтено».

Оценка «зачтено» выставляется студенту, который набрал в сумме не менее 5 баллов. Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий и лабораторных работ.

Оценка «не зачтено» выставляется студенту, который набрал в сумме менее 5 баллов, либо имеет к моменту проведения промежуточной аттестации несданные практические, либо лабораторные работы.

2 ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ

Контролируемые разделы (темы) дисциплины	**Код контролируемой компетенции (или ее части)**	**Наименование оценочного средства**
Раздел 1. Базовые понятия области защиты информации и безопасности информационных систем.		
Проблема информационной безопасности общества. Основные термины и определения данной предметной области. Задачи по защите информации и информационных систем. Уровни формирования режима информационной безопасности. Обзор нормативно-правовых документов в области защиты информации. Государственные стандарты РФ – руководящие документы Гостехкомиссии России по защите информации. /Тема/	ОПК-3.2 ОПК-3.3	Зачет
Проблема информационной безопасности общества. Основные термины и определения данной предметной области. Задачи по защите информации и информационных систем. Уровни формирования режима информационной безопасности. Обзор нормативно-правовых документов в области защиты информации. Государственные стандарты РФ – руководящие документы Гостехкомиссии России по защите информации. Оценка рисков в сфере информационной безопасности. Основные методы средства, механизмы защиты информации. /Лек/	ОПК-3.2 ОПК-3.3	Зачет

Раздел 2. Угрозы информационной безопасности		
Исследование причин нарушения безопасности. Понятие угрозы информационной безопасности. Классификация угроз по различным классификационным признакам. Понятие уязвимости информации. Современные виды угроз. Понятие, виды, классификация, этапы реализации типовых сетевых атак. Технические каналы утечки информации. Каналы несанкционированного доступа к информации. /Тема/	ОПК-3.2 ОПК-3.3	Зачет
Исследование причин нарушения безопасности. Понятие угрозы информационной безопасности. Классификация угроз по различным классификационным признакам. Понятие уязвимости информации. Современные виды угроз. Понятие, виды, классификация, этапы реализации типовых сетевых атак. Технические каналы утечки информации. Каналы несанкционированного доступа к информации. /Лек/	ОПК-3.2 ОПК-3.3	Зачет
Раздел 3. Общие подходы к проблеме защиты информации. Основные методы и средства защиты безопасности		
Общие подходы к проблеме защиты информации. Основные методы и средства защиты безопасности /Тема/	ОПК-3.2 ОПК-3.3	Зачет
Теоретические основы информационной безопасности. Понятия «объект», «субъект», «сущность», «процесс». Понятие модели безопасности. Виды моделей безопасности в зависимости от реализуемых функций защиты. Понятие политики безопасности. Мандатная, дискреционная, ролевая политики безопасности. /Лек/	ОПК-3.2 ОПК-3.3	Зачет

4 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

4.1 Промежуточная аттестация (зачет)

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.2 Понимает основные требования информационной безопасности

а) типовые тестовые вопросы закрытого типа

1. Защита информации (ЗИ) – это:

деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

деятельность, направленная на предотвращение несанкционированного доступа к защищаемой информации;

приемы, способы и методы применения технических и программных средств при выполнении функций обработки информации;

единица информационного ресурса АС, доступ к которой регламентируется правилами разграничения доступа.

2. Уровни формирования режима информационной безопасности:

гражданский, административный (организационный), программно-технический;

законодательный, административный (организационный), программно-правовой;

законодательно-правовой, административный (организационный), программно-технический;

3. Канал атаки – это:

пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств;

среда переноса между субъектом и объектом атаки действий, осуществляемых при проведении атаки;

4. Эффективная программа безопасности требует сбалансированного применения:

технических и нетехнических методов;

контрмер и защитных механизмов;

физической безопасности и технических средств защиты;

процедур безопасности и шифрования;

5. Как расшифровывается аббревиатура DSA?

Digital Simantick Algorithm;

Digital Signature Algorithm;

Digital Simplix Algorithm

6. Авторизация – это

аутентификация плюс предоставление индивидуальных прав доступа;

система, имеющая защиту от попыток нарушения правил разграничения доступа

когда всякий субъект доступа действует в рамках предписанных ему полномочий.

7. Потенциально возможное происшествие, которое может быть преднамеренным или непреднамеренным и может оказать нежелательное воздействие на систему - это

угроза;

атака;

взлом.

8. Что такое Kerberos?

криптографический алгоритм с открытым ключом;

криптографический алгоритм с закрытым ключом;

***это сетевой протокол аутентификации*;**

9. Авторизация - это …

аутентификация плюс предоставление индивидуальных прав доступа;

система, имеющая защиту от попыток нарушения правил разграничения доступа.

когда всякий субъект доступа действует в рамках предписанных ему полномочий.

программа, обладающая способностью к самовоспроизведению и мешающая нормальной работе компьютера.

10. Классификация компьютерных вирусов по среде обитания:

резидентные, нерезидентные;

сетевые, файловые, загрузочные, файлово-загрузочные;

макровирусы, стелс-вирусы, троянский конь, бэкдор.

б) типовые тестовые вопросы открытого типа

1. Как называется наука о защите информации с помощью шифрования? (Криптография)
2. Как называется программно-криптографическая проверка целостности и конфиденциальности документов, а также установление лица, отправившего документ (Электронно-цифровая подпись (ЭЦП)).
3. Что такое «Троянские программы»? (Вредоносное программное обеспечение)
4. Степень соответствия результатов защиты информации поставленной цели (Эффективность)
5. Как называется событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности обрабатываемой в ней информации? (Угроза безопасности)
6. Как называется набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа? (Политика безопасности)
8. Как классифицировать искусственные угрозы исходя из их мотивов (непреднамеренные (случайные) и преднамеренные (умышленные)).
9. Опишите шифрование подстановки.

Шифр подстановки - это метод шифрования, в котором элементы исходного открытого текста заменяются зашифрованным текстом в соответствии с некоторым правилом. Элементами текста могут быть отдельные символы (самый распространенный случай), пары букв, тройки букв, комбинирование этих случаев и т. д. В классической криптографии различают четыре типа шифра подстановки:

- одноалфавитный шифр подстановки (шифр простой замены) -- шифр, при котором каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита;
- однозвучный шифр подстановки похож на одноалфавитный за

исключением того, что символ открытого текста может быть заменен одним из нескольких возможных символов;

- полиграммный шифр подстановки заменяет не один символ, а целую группу. Примеры: шифр Плейфера, шифр Хилла;
- полиалфавитный шифр подстановки состоит из нескольких шифров простой замены.

В качестве альтернативы шифрам подстановки можно рассматривать перестановочные шифры. В них элементы текста переставля- ются в ином от исходного порядке, а сами элементы остаются неизменными. Напротив, в шифрах подстановки элементы текста не меняют свою последовательность, а изменяются сами.

10. Опишите шифры традиционных симметричных криптосистем

Шифры традиционных симметричных криптосистем можно разделить на следующие основные виды.

1. Шифры замены.
2. Шифры перестановки.
3. Шифры гаммирования.

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.3 Решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности

а) типовые тестовые вопросы закрытого типа

1. . RSA — криптографический алгоритм с

открытым ключом;

закрытым ключом.

2. Где применяются средства контроля динамической целостности?

анализе потока финансовых сообщений;

обработке данных;

при выявлении кражи, дублирования отдельных сообщений.

3. Какие трудности возникают в информационных системах при конфиденциальности?

сведения о технических каналах утечки информации являются закрытыми;

на пути пользовательской криптографии стоят многочисленные технические проблемы;

все ответы правильные.

4. Окно опасности - это…

промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется;

комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области;

формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере;

5. По каким компонентам классифицируется угрозы доступности:

отказ пользователей;

отказ поддерживающей инфраструктуры;

ошибка в программе.

6. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности;

обрабатывать большой объем программной информации;

нет правильного ответа.

7. Конфиденциальную информацию можно разделить:

предметную;

служебную;

глобальную

8. Отказ, ошибки, сбой - это:

случайные угрозы;

преднамеренные угрозы;

природные угрозы

9. Побочное влияние - это…

негативное воздействие на систему в целом или отдельные элементы;

нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент;

нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций;

б) типовые тестовые вопросы открытого типа

1. Как называется наука о методах получения исходного значения зашифрованной информации, не имея доступа к секретной информации (ключу), необходимой для этого (Криптоанализ).

2. Опишите шифр Гронсфельда

Шифр Гронсфельда представляет собой модификацию шифра Цезаря с числовым ключом. При реализации данного шифра под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Получение символа шифротекста осуществляют также, как это делается в шифре Цезаря, при этом смещение символа открытого текста производят на количество позиций, соответствующего цифре ключа, стоящей под ним.

3. Опишите шифр простой замены Атбаш,

Шифр Атбаш, используемый для еврейского алфавита. и получил оттуда свое название. Шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю и т. д.

Шифр Атбаш для английского алфавита:

Исходный алфавит: ABCDEFGHIjKLMNOPQRSTUVWXYZ

Алфавит замены: ZYXWVUTSRQPONMLKJIHGFEDCBA

4. Используя шифр Цезаря, зашифровать следующие фразы:

а) Делу время - потехе час (Еёмф гсёна - рпуёцё шбт)

б) С Новым годом (Т Опгьн дпепн)

в) Первое сентября (Рёсгпё тёоуавса)

(Шифр Цезаря. Этот шифр реализует следующее преобразование текста: каждая буква исходного текста заменяется следующей после нее буквой в алфавите, который считается написанным по кругу.

5. Используя шифр Цезаря, декодировать следующие фразы:

а) Лмбттоьк шбт (Классный час)

б) Вёмпё тпмочё рфтуьой (Белое солнце пустыни)

6. Написать команды для псевдовируса (для текстового редактора или командной строки), используя команды MD, CD и COPY.

(Предположим, что мы находимся в коруевом каталоге диска D:>\ . Пусть имя создаваемой папки будет для простоты 0 (ноль), имя пакетного файла самокопирующимся кодом 1.bat.

Открыть запись файла из командной строки можно так:

D:>\ copy con 1.bat {после нажатия на клавишу Enter командная строка перейдёт в режим ожидания ввода записи и построчного её сохранения}

md 0 {команда создаст папку по имени 0 в текущем каталоге}

copy 1.bat 0 {команда копирует файл по имени 1.bat в созданную папку по имени 0}

cd 0 {команда смещает отзыв операционной системы в папку D:\0>_}

1.bat {команда передаёт управление копии пакетного файла, находящейся в папке D:\0}

Закрыть и сохранить запись в командной строке можно, нажав последовательно функциональную клавишу F6, а затем клавишу ввода Enter. Операционная система выдаст сообщение на русском или английском о том, что скопирован 1 файл.)

7. Найти шифрообозначение вектора $b_1 = 101011$, используя функцию Фейстеля

(Решение: на вход S_1 -бокса подано число 101011. Номер строки – $11_2 = 3_{10}$; Номер столбца – $0101_2 = 5_{10}$. По таблице подстановки для S_1-бокса находим, на пересечении 3-ей строки и 5-го столбца число $6_{10} = 0110_2$. Ответ: 0110 – шифрообозначение для 101011.)

8. Вычислите значение выражения $11^{219} \bmod 91$

(91 = 7*13; φ(91) = 6*12 = 72; (11,91) = 1. По теореме Эйлера имеем: $11^{219} \bmod 91 = 11^{72*3+3} \bmod 91 = (11^{72})^3 * 11^3 \bmod 91 \equiv 11^3 \bmod 91 \equiv 330 \bmod 91 \equiv 57 \bmod 91 = 57$)

9. Зашифруйте сообщение «RSA» с помощью алгоритма RSA, пусть букве А соответствует цифра 1, В - 2, С - 3 и т.д.

(Выбираем простые числа: p = 3; q = 11. Вычисляем модуль n = p * q = 3 * 11 = 33. Вычисляем функцию Эйлера от модуля n: φ(N) = (p – 1)(q – 1) = 2 * 10 = 20. Выбираем открытую экспоненту e = 7. Определяем закрытую экспоненту d: $d * e = 1 \pmod{\varphi(N)} \Rightarrow d = 3$

R=18; S=19; A=1;

Открытый ключ: (e, n) = (7,33)

$C_1 = (18^7) \bmod 33 = 6$

$C_2 = (19^7) \bmod 33 = 13$

$C_3 = (1^7) \bmod 33 = 1$

C = («RSA») = 6, 13, 1

10. Сколько бит памяти займет слово «Микропроцессор»?

(Слово состоит из 14 букв. Каждая буква – символ компьютерного алфавита, занимает 1 байт памяти. Слово занимает 14 байт =14*8=112 бит памяти. Ответ: 112 бит)

4.2 Типовые контрольные вопросы к зачету

1 Дайте определение понятия «Информационная безопасность».
2 Дайте определение понятия «Защита информации».
3 Дайте определение понятия «Информация» с точки зрения информационной
4 безопасности.
5 Назовите свойства информации, наиболее значимые с точки зрения
6 информационной безопасности.
7 Чем определяется уровень (степень) секретности информации или документа?
8 Что такое количественная характеристика информации, какие методы определения
9 данной характеристики существуют?

10 Чем характеризуются прагматические свойства информации?
11 Дайте определение понятия «Информационная система».
12 Что понимают под информационным процессом?
13 Чем характеризуются информационные системы?
14 Что такое обработка информации в информационных системах?
15 Что такое физическая структура информационной системы?
16 Что такое логическая структура информационной системы?
17 Что такое топологическая структура информационной системы?
18 Что такое конфигурация информационной системы?
19 Что такое архитектура информационной системы?
20 Что такое информационный узел?
21 Что такое ресурсы информационной системы?
22 Дайте определение понятия «Угроза безопасности».
23 Дайте определение понятия «Уязвимость информации».
24 Что такое атака на информационную систему?
25 Что такое утечка информации?
26 Что такое разглашение информации?
27 Что такое несанкционированный доступ?
28 Дайте определение понятия «Политика безопасности»?
29 Какую угрозу информации представляют собой хакеры.
30 Что такое бесконтрольный уход информации?
31 Что такое канал утечки?
32 Назовите виды каналов утечки?
33 Назовите классификационные признаки угроз безопасности.
34 Какие виды угроз считаются умышленными, а какие непреднамеренными?
35 Что такое активные угрозы?
36 Что такое пассивные угрозы?
37 Перечислите пути несанкционированного доступа к информации.
38 В чем особенности угроз и уязвимостей корпоративных сетей?
39 Перечислите виды атак в IP-сетях.
40 Перечислите наиболее общие проблемы безопасности информационных систем.
41 Перечислите основные группы методов и средств защиты информации.
42 Что входит в понятие комплексной защиты информации?
43 На какие виды подразделяются средства защиты информации?
44 Перечислите основные средства защиты информации.
45 Перечислите основные методы защиты информации.
46 Перечислите основные механизмы защиты информации.
47 Поясните содержание подходов к обеспечению безопасности информации и информационных систем, изложенные в межгосударственных стандартах информационной безопасности.