**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«Рязанский государственный радиотехнический университет»**

**Факультет вычислительной техники**

**Кафедра «Информационная безопасность»**

|  |  |  |
| --- | --- | --- |
| **СОГЛАСОВАНО****Декан факультета****вычислительной техники****\_\_\_\_\_\_\_\_\_ А.Н. Пылькин****«\_\_\_ »\_\_\_\_\_\_\_\_ 2018 г.** |  | **УТВЕРЖДАЮ****И.о. проректора****по учебной работе**К**.В.Бухенский****«\_\_\_»\_\_\_\_\_\_\_\_ 2018 г.** |
| **Руководитель ОПОП****\_\_\_\_\_\_\_\_ В.Н. Пржегорлинский «\_\_\_»\_\_\_\_\_\_\_\_\_2018 г.** |  |  |

**ОЦЕНОЧНЫЕ СРЕДСТВА**

по дисциплине

**Б1.3.Б.11 «Криптографические методы защиты информации»**

Специальность 10.05.01 - Компьютерная безопасность

Специализация № 8 — Информационная безопасность объектов

информатизации на базе компьютерных систем

ОПОП — «Компьютерная безопасность»

Квалификация выпускника - специалист

Форма обучения - очная

Срок обучения — 5,5 лет

**Рязань 2018**

**1. Перечень компетенций с указанием этапов их формирования**

При освоении дисциплины формируются следующие компетенции:

- ОПК-2: способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов;

- ПК-5; способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

- ПК-18; способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

Указанные компетенции формируются в соответствии со следующими этапами:

1. формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (лекционные занятия, самостоятельная работа студентов);
2. приобретение и развитие практических умений предусмотренных компетенциями (лабораторные работы, самостоятельная работа студентов);
3. закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями, в ходе решения конкретных при выполнении лабораторных работ и их защиты, в процессе сдачи экзамена и зачета.

**2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания**

**Уровень сформированности** каждой компетенции на различных этапах ее формирования в процессе освоения данной дисциплины оценивается в ходе текущего контроля успеваемости и представлен различными видами оценочных средств.

В рамках **текущего контроля** преподавателем оценивается содержательная сторона и качество материалов, приведенных в отчетах студента по лабораторным работам. Кроме того, преподавателем учитываются ответы студента на вопросы по соответствующим видам занятий при текущем контроле:

* контрольные опросы по результатам самостоятельной работы;
* допуски и защиты лабораторных работ;
* задания по практическим занятиям.

Принимается во внимание:

**знание** обучающимися:

* основных криптографических примитивов и способов их использования в ре­шении основных задач защиты информации (ПК-5);
* принципов построения и основных видах симметричных и асиммет­ричных криптографических алгоритмов (ПК-18);
* математических моделей шифров (ПК-5);
* требований к шифрам и основных характеристик шифров (ПК-5);
* криптографических стандартов (ПК-18);
* частотных характеристик открытых текстов и их применение к ана­лизу простейших симметричных криптосистем (ПК-5);

**наличие умений**:

* корректно применять симметричные и асимметричные криптогра­фические алгоритмы (ПК-18);
* применять математические методы описания и исследования крип­тосистем (ОПК-2, ПК-5);

**обладание**:

- информацией о математических методах, используемых в криптографии (ОПК-2);

- навыками применения симметричных и ассиметричных криптографических алгоритмов (ПК-18);

- навыками применения математических методов описания и исследования крип­тосистем (ОПК-2, ПК-5).

**Сформированность** (уровень сформированности) каждой компетенции в рамках освоения данной дисциплины оценивается по трехуровневой **шкале оценивания**:

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.

Критерии **оценивания уровня сформированности компетенции** в процессе выполнения и защиты лабораторных работ, практических занятий а также в ходе опросов по результатам самостоятельной работы:

* получение 41%-60% правильных ответов свидетельствует о достижении порогового уровня сформированности компетенции на данном этапе ее формирования;
* получение 61%-80% правильных ответов свидетельствует о достижении продвинутого уровня сформированности компетенции на данном этапе ее формирования;
* получение 81%-100% правильных ответов свидетельствует о достижении эталонного уровня сформированности компетенции на данном этапе ее формирования.

Сформированность уровня компетенций не ниже порогового является основанием для **допуска обучающегося к промежуточной аттестации** по данной дисциплине.

**Формами промежуточной аттестации** по данной дисциплине являются экзамен и зачет.

При оценивании уровня сформированности компетенции при проведении экзамена и зачета учитываются следующее:

1. Уровень усвоения материала, предусмотренного программой.

2. Умение анализировать материал, устанавливать причинно-следственные связи.

3. Ответы на вопросы: полнота, аргументированность, убеждение, умение.

4. Качество ответа, его логичность, общая эрудиция.

5. Умение решать задачи.

**Экзамен** оценивается по принятой в ФГБОУ ВО «РГРТУ» четырехбалльной системе: «неудовлетворительно», «удовлетворительно», «хорошо» и «отлично». Критерии оценивания промежуточной аттестации в форме экзамена представлены в таблице 1.

Таблица 1 - Критерии оценивания промежуточной аттестации

|  |  |
| --- | --- |
| **Шкала оценивания** | **Критерии оценивания** |
| **«отлично»** | **студент должен**: продемонстрировать глубокое и прочное усвоение знаний материала; исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; правильно формулировать определения; уметь сделать выводы по излагаемому материалу; безупречно ответить не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины; продемонстрировать умение правильно выполнять практические задания, предусмотренные программой;  |
| **«хорошо»** | **студент должен:** продемонстрировать достаточно полное знание материала; продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно излагать материал; уметь сделать достаточно обоснованные выводы по излагаемому материалу; ответить на все вопросы билета; продемонстрировать умение правильно выполнять практические задания, предусмотренные программой, при этом возможно допустить непринципиальные ошибки. |
| **«удовлетворительно»** | **студент должен:** продемонстрировать общее знание изучаемого материала; знать основную рекомендуемую программой дисциплины учебную литературу; уметь строить ответ в соответствии со структурой излагаемого вопроса; показать общее владение понятийным аппаратом дисциплины; уметь устранить допущенные погрешности в ответе на теоретические вопросы и/или при выполнении практических заданий под руководством преподавателя, либо (при неправильном выполнении практического задания) по указанию преподавателя выполнить другие практические задания того же раздела дисциплины. |
| **«неудовлетворительно»** | **ставится в случае:** незнания значительной части программного материала; не владения понятийным аппаратом дисциплины; существенных ошибок при изложении учебного материала; неумения строить ответ в соответствии со структурой излагаемого вопроса; неумения делать выводы по излагаемому материалу. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине (формирования и развития компетенций, закрепленных за данной дисциплиной). Оценка «неудовлетворительно» выставляется также, если студент после начала экзамена отказался его сдавать или нарушил правила сдачи экзамена (списывал, подсказывал, обманом пытался получить более высокую оценку и т.д.).  |

**Зачет** оценивается по двухбальной системе - «зачтено» или «незачтено». Зачет (оценку «зачтено») получают студенты, которые выполнили все предусмотренные учебным графиком лабораторные работы, положительно отчитались о выполненной самостоятельной работе и в ходе зачета при ответе на вопросы продемонстрировали уровень знаний, соответствующий оценке не ниже «удовлетворительно» (см. шкалу выше).

**Критерии оценивания сформированности компетенций по результатам решения задач (лабораторных работ и практических заданий)**

|  |  |
| --- | --- |
| **Компетенция** | **Критерий (студент должен)** |
| ОПК-2- способность корректно применять при решении профессиональ-ных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов | **Пороговый уровень:**уметь определять и понимать математические методы, использованные в криптографических средствах защиты информации;  |
| **Продвинутый уровень:**грамотно использовать математические методы для анализа криптографических алгоритмов;  |
| **Эталонный уровень:**квалифицированно выбирать и грамотно использовать математические методы для построения систем защиты информации с использованием криптографических средств защиты информации;  |
| ПК-5 - способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации | **Пороговый уровень:**понимать принципы функционирования криптографических средств защиты информации. |
| **Продвинутый уровень:**уметь конфигурировать криптографические средства защиты информации; |
| **Эталонный уровень:**квалифицированно участвовать в разработке и конфигурировании средств криптографической защиты информации.выбирать с учетом требований нормативных документов и особенностей системы защиты информации криптографические средства защиты информации;устанавливать и настраивать криптографические средства защиты информации в соответствии с требованиями их эксплуатации для конкретной системы защиты информации; |
| ПК-18 - способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации | **Пороговый уровень:**способность производить установку криптографических средств защиты информации; |
| **Продвинутый уровень:**способность производить установку и настройку криптографических средств защиты информации;  |
| **Эталонный уровень:**способностью производить установку, наладку, тестирование и обслуживание криптографических средств защиты информации;  |

**3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

**3.1. Паспорт фонда оценочных средств по дисциплине**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Контролируемые разделы дисциплины****(результаты по разделам)** | **Код контролируемой компетенции (или её части)** | **Наимено­вание****оценочного****средства** |
|
| 1 | 2 | 3 | 4 |
| 1. | Введение в криптографию | ОПК-2 | Экзамен |
| 2. | Основные классы шифров и их свойства | ОПК-2, ПК-5 | Экзамен |
| 3. | Надежность шифров | ОПК-2, ПК-5, ПК-18 | Экзамен, зачет |
| 4. | Методы синтеза и анализа симметричных криптосистем | ОПК-2, ПК-5, ПК-18 | Зачет |
| 5. | Криптографические хеш-функции | ОПК-2,ПК-5,ПК-18 | Зачет |

3**.2. Типовые контрольные задания или иные материалы**

**Задания в рамках лабораторных работ и практических занятий студентов** для совершенствования полученных знаний, получения и развития умений и навыков, предусмотренных компетенциями, закрепленными за дисциплиной, приведены в соответствующих методических указаниях по выполнению лабораторных работ. Список лабораторных работ приведен в Приложении 1 к данному документу (ФОС), а перечень тем практических занятий - в Приложении 2. Для формирования практических навыков и умений в рамках требуемых компетенций студенты должны сделать и защитить (сдать) все перечисленные в рабочей программе лабораторные работы и выполнить все задания практических занятий. При защите (сдаче) лабораторных работ и отчете о выполнении задании практических занятий студентам задаются вопросы, ответы на которые позволяют оценивать уровень сформированности знаний, умений и навыков, предусмотренных компетенциями, закрепленными за дисциплиной.

**Задания в рамках самостоятельной работы студентов** для получения и развития знаний, умений и навыков, предусмотренных компетенциями, закрепленными за дисциплиной.

В рамках самостоятельной работы студенты изучают материалы лекций и литературу по текущим темам, готовятся к проведению и сдаче лабораторных работ и практических занятий. По завершению каждой самостоятельной работы проводится устный опрос и проверка для определения степени изученности рекомендованных материалов, готовности к выполнению и сдаче лабораторных работ, выполнения графика работ над курсовой работой. Проверка выполняется в соответствие с вопросами рабочей программы дисциплины по текущей самостоятельной работе и графиком выполнения лабораторных работ, индивидуальными заданиями на выполнение лабораторных работ. Для формирования компетенций студенты должны выполнить все перечисленные в рабочей программе самостоятельные работы и отчитаться об их выполнении.

Перечень тем (заданий) для самостоятельной работы обучающихся приведен в Приложении 3 к данному документу (оценочным материалам).

Список **типовых контрольных вопросов** для оценки уровня сформированности знаний, умений и навыков, предусмотренных компетенциями, закрепленными за дисциплиной, которые задаются **во время защиты лабораторных работ (текущий контроль), сдачи зачета и экзамена (промежуточная аттестация)**:

1. Основные этапы развития криптографии
2. Основные понятия и определения.
3. Основные понятия и определения по ключу и ключевым документам.
4. Основные задачи криптографии.
5. Конфиденциальность.
6. Симметричные и ассиметричные криптосистемы.
7. Целостность.
8. Аутентификация.
9. Цифровая подпись.
10. Управление секретными ключами. Предварительное распределение ключей.
11. Пересылка ключей.
12. Открытое распределение ключей.
13. Схема разделения секрета.
14. Инфраструктура открытых ключей. Сертификаты.
15. Центры сертификации.
16. Алгебраическая модель шифра.
17. Вероятностная модель шифра.
18. По-значная модель открытого текста.
19. Вероятностная модель открытого текста.
20. Критерии распознавания открытых текстов.
21. Классификация шифров.
22. Табличные перестановки с заглушками.
23. Элементы криптоанализа в шифрах перестановки. Основные идеи, используемые при вскрытии вертикальных перестановок.
24. Шифры замены.
25. Аффинный шифр.
26. Многобуквенные, многоалфавитные шифры. Шифр Хилла.
27. Криптоанализ аффинного шифра.
28. Дисковые многоалфавитные шифры замены.
29. Шифры гаммирования. Табличное гаммирование.
30. Шифр Вернама.
31. О возможности восстановления знаков гаммы.
32. Суть частотного метода анализа шифров.
33. Для анализа каких шифров можно использовать частотный анализ.
34. Модели источников открытых сообщений.
35. Основные характеристики открытых сообщений.
36. Принцип Керкгоффса.
37. Сколько шифров в таблице Вижинера.
38. в чем отличие расшифрования от дешифрования.
39. Шифр Плейфера.
40. Алгоритм шифрования DES.
41. Алгоритм шифрования AES.
42. К какому классу шифров относится алгоритм DES.
43. Какие математические преобразования лежат в основе алгоритма AES.
44. Как получается раундовый ключ в алгоритме AES.
45. Какие математические преобразования используются в алгоритме шифрования информации ГОСТ 28147-89.
46. Принцип гаммирования, использованного в алгоритме шифрования информации ГОСТ 28147-89.
47. Для чего нужна электронная подпись.
48. Какие алгоритмы электронной подписи знаете?
49. Однонаправленные хэш-функции.
50. Алгоритм Диффи-Хэлмана.
51. Определение понятия гаммы.
52. Понятие сети Фейстеля.
53. Режимы использования блочных шифров.
54. Методы анализа алгоритмов блочного шифрования.
55. Криптографическая стойкость шифров.
56. Теоретическая и практическая стойкость шифров.
57. Подходы к определению криптографической стойкости шифров.
58. Подходы к определению практической стойкости шифров.
59. Имитостойкость шифров.
60. Имитозащита.
61. Характеристики имитостойкости шифров и их оценки.
62. Генераторы псевдослучайных последовательностей.
63. Конгруэнтные генераторы.
64. Генераторы Фибоначчи.
65. Генераторы, основанные на сложности решения задач теории чисел.
66. Генераторы на основе линейных регистров сдвига.
67. Методы анализа криптографических алгоритмов.
68. Классификация методов анализа криптографических алгоритмов.
69. Методы нахождения ключей криптографических алгоритмов: алгоритмические методы, алгебраические методы, статистические методы.
70. Общие сведения о хеш-функциях.
71. Криптографические хеш-функции.
72. Ключевые и бесключевые хеш-функции.
73. Итеративные способы построения хеш-функций.
74. Понятие о стойкости хеш-функций.

Фонд оценочных средств входит в состав рабочей программы дисциплины «Криптографические методы защиты информации» (Б1.3.Б.11) ОПОП 10.05.01 «Компьютерная безопасность», направленность «Информационная безопасность объектов информатизации на базе компьютерных систем».

Составил

старший преподаватель

кафедры «Информационная безопасность» Т.И. Калинкина

Приложение 1

Лабораторный практикум

1. **Лабораторная работа №1.** Использование классических криптоалго-ритмов подстановки и перестановки для защиты текстовой информации **(2 часа).**
2. Литература для теоретической подготовки: [1, 2, 4, 5, 7, 8].
3. **Лабораторная работа №2.** Изучение устройства и принципа работы шифровальной машины «Энигма» **(2 часа).**

Литература для теоретической подготовки: [1, 2, 4, 5, 7, 8].

1. **Лабораторная работа № 3.** Реализация симметричной криптосистемы с использованием блочного алгоритма шифрования **(4 часа).**
2. Литература для теоретической подготовки: [1, 2, 4, 5, 7, 8].
3. **Лабораторная работа № 4.** Современные симметричные блочные шифры. **(4 часа).**
4. Литература для теоретической подготовки: [1, 2, 4, 5, 7, 8].
5. **Лабораторная работа № 5** Электронная цифровая подпись (**4 часа**).
6. Литература для теоретической подготовки: [1, 2, 4, 5, 7, 8].

Приложение 2

Перечень тем практических занятий

1. Некоторые вопросы элементарной теории чисел. Конечные поля и квадратичные вычеты. Некоторые простые криптосистемы.

Литература для теоретической подготовки: [3, 6].

1. Некоторые простые криптосистемы.

Литература для теоретической подготовки: [3, 6].

1. Криптография с открытым ключом. Криптосистема RSA. Дискретное логарифмирование.
	1. Литература для теоретической подготовки: [3, 6].

Приложение 3

**Темы самостоятельных работ**

Для самостоятельных занятий рекомендуются следующие темы:

**Тема 1**. Предварительное распределение ключей.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 2.** Пересылка ключей.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 4.** Открытое распределение ключей.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 5.** Схема разделения секрета.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 6. С**ертификаты.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 7.** Центры сертификации.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 8.** Шифрсистема Шамира.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 9.** Шифрсистема RSA.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 10.** Шифрсистема Эль-Гамаля.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 11.** Шифрсистема Мак-Элиаса.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 12.** Шифрсистема на основе задачи об «укладке рюкзака».

Литература для теоретической подготовки: [2, 4, 5].

**Тема 13.** Примеры имитостойких шифров.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 14.** Имитовставка.

Литература для теоретической подготовки: [2, 4, 5].

 **Тема 15.** Коды аутентификации.

 Литература для теоретической подготовки: [2, 4, 5].

**Тема 16.** Помехоустойчивость шифров.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 17.** Режимы использования поточных шифров.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 18.** Генераторы, основанные на сложности решения задач теории чисел.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 19.** Генераторы на основе линейных регистров сдвига.

1. Литература для теоретической подготовки: [2, 4, 5].
	1. **Тема 20.** Алгебраические и статистические методы нахождения ключей криптографических алгоритмов.
2. Литература для теоретической подготовки: [2, 4, 5].

**Тема 21.** Способы построения хеш-функций.

Литература для теоретической подготовки: [2, 4, 5].

**Тема 22.** Понятие о стойкости хеш-функций.

Литература для теоретической подготовки: [2, 4, 5].