**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.12 «Криптографические протоколы»**

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: способность 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; 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;

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 выполнению заданий практических занятий. Кроме того, преподавателем учитываются ответы студента на вопросы по соответствующим видам занятий при текущем контроле:

* контрольные опросы по результатам самостоятельной работы;
* задания по практическим занятиям.

Принимается во внимание:

**знание** обучающимися:

* современных тенденций в развитии криптографических протоколов; (ОПК-2, ПК-5);
* базовых протоколов проверки подлинности и обмена ключами (ОПК-2, ПК-5);
* основныех криптологических аспектов проектирования и развертывания технологии PKI в корпоративных сетях (стандарт X.509); протоколов разделения секрета (ОПК-2, ПК-5);
* протоколов обеспечения безопасности в сети Internet (ОПК-2, ПК-5);
* основных подходов к конструированию систем защиты информации с использованием криптографических протоколов различной направленности (ОПК-2, ПК-5);

**наличие умений**:

* проектировать и внедрять схемы аутентификации на основе типовых стандартизированных механизмов (ОПК-2, ПК-5);
* использовать схемы разделения секрета для хранения критической информации (ОПК-2, ПК-5);
* осуществлять распределение аутентифицированных криптографических ключей в корпоративных сетях (ОПК-2, ПК-5);
* анализировать защищенность системы, использующей криптографические протоколы, квалифицированно оценивать информационные риски, возникающие при использовании конкретных криптографических протоколов в защищаемой информационной системе (ОПК-2, ПК-5);

**обладание**:

* навыками настройки параметров протоколов используемых для аутентификации и обмена ключами в операционных системах (ОПК-2, ПК-5);
* способами использования и администрирования современных средств электронной цифровой подписи (ОПК-2, ПК-5);
* навыками самостоятельной работы с современными международными стандартами криптографических протоколов (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 протоколах;  |
| **Продвинутый уровень:**грамотно использовать математические методы для анализа криптографических протоколов;  |
| **Эталонный уровень:**квалифицированно выбирать и грамотно использовать математические методы для построения систем защиты информации с использованием криптографических протоколов;  |
| 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 протоколов. |
| **Продвинутый уровень:**уметь конфигурировать криптографические протоколы. |
| **Эталонный уровень:**квалифицированно участвовать в разработке и конфигурировании криптографических протоколов.настраивать криптографические протоколы в соответствии с требованиями к их эксплуатации для конкретной системы 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. | Общие сведения о криптографических протоколах | ОПК-2 | зачет |
| 2. | Виды современных протоколов | ОПК-2, ПК-5 | зачет, экзамен |
| 3. | Нормативно-правовые документы в области криптографических протоколов | ОПК-2, ПК-5, ПК-18 | экзамен |

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

**Задания в рамках практических занятий студентов** для совершенствования полученных знаний, получения и развития умений и навыков, предусмотренных компетенциями, закрепленными за дисциплиной. Перечень тем практических занятий приведен в Приложении 1.

**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, индивидуальными заданиями практических 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 2 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. Функции — сервисы безопасности.
2. Понятие криптографического протокола
3. Конфиденциальность
4. Целостность
5. Аутентификация
6. Невозможность отказа от авторства (цифровая подпись)
7. Свойства, характеризующие безопасность протоколов
8. Аутентификация (нешироковещательная)
9. Аутентификация при рассылке по многим адресам или при подключении к службе подписки/уведомления. Авторизация (доверенной третьей стороной)
10. Свойства совместной генерации ключа. Конфиденциальность. Анонимность
11. Ограниченная защищенность от атак типа «отказ в обслуживании». Инвариантность отправителя. Невозможность отказа от ранее совершенных действий. Безопасное временное свойство
12. Новые свойства безопасности
13. Основные атаки на безопасность протоколов
14. Классификация атак на безопасность протоколов
15. Основные виды криптографических протоколов
16. Другие подходы к классификации криптографических протоколов
17. Методы анализа криптографических протоколов
18. BAN - логика
19. Основные атаки на безопасность протоколов
20. Классификация атак на криптографические протоколы
21. Наиболее известные атаки на криптографические протоколы
22. Классификация криптографических протоколов.
23. Протокол аутентификации сообщений, схема ЦП, задача распределения ключей, протокол обмена секретами, протокол привязки к биту.
24. Протокол подбрасывания монеты, примитивный (простой) криптопротокол, прикладной криптопротокол. Другие подходы к классификации криптографических протоколов.
25. Протокол с арбитром (посредником). Доказательство интерактивное, доказательство знания.
26. Классификация криптопротоколов по области применения.
27. Система электронных платежей, протокол подписания контракта, протокол сертифицирования электронной почты, протокол голосования.
28. Формальные методы анализа криптопротоколов. Использование специализированных языков и инструментариев. Применение экспертных систем.
29. Ban-логика. Формальные модели.
30. Требования к криптографическим хеш-функциям.
31. Бесключевые хеш-функции.
32. Основы построения хеш-функций.
33. Хеш-функция на основе блочного алгоритма.
34. Хеш-функция md5.
35. Алгоритм md4.
36. Стандарты на хеш-функции.
37. Хеш –функции, задаваемые ключом.
38. Коды аутентификации сообщений-МАС.
39. Определение схемы цифровой подписи.
40. Алгоритм цифровой подписи RSA.
41. Алгоритм цифровой подписи Эль Гамаля (EGSA).
42. Алгоритм цифровой подписи Шнорра (SCHNORR).
43. Алгоритм цифровой подписи DSA.
44. Отечественный стандарт цифровой подписи ГОСТ Р 34.10.
45. Схема подписи Fiat-Shamir.
46. Инфраструктура открытых ключей PKI.
47. Рекомендации Х.509.
48. Схемы слепой подписи.
49. Схемы неоспоримой подписи.
50. Неотрицаемые цифровые подписи. Подписи уполномоченного свидетеля. Групповая подпись. Доверенная подпись.

Фонд оценочных средств входит в состав рабочей программы дисциплины «Криптографические протоколы» (Б1.3.Б.12) 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

Перечень тем практических занятий

1. Формализация свойств, характеризующих безопасность протоколов, и анализ известных криптографических протоколов на соответствие данным свойствам.

Литература для теоретической подготовки: [3, 6].

1. Анализ схем электронных подписей.

Литература для теоретической подготовки: [3, 6].

1. Исследование атак на криптографические протоколы с целью определение методов противодействия данным атакам.
	1. Литература для теоретической подготовки: [3, 6].
2. Изучение подходов к распределению ключей в ассиметричных криптосистемах
	1. Литература для теоретической подготовки: [3, 6].
3. Груп­по­вые про­то­ко­лы. Про­то­ко­лы раз­де­ле­ния сек­ре­та и рас­пре­де­ле­ния клю­чей для те­ле­кон­фе­рен­ции.
	1. Литература для теоретической подготовки: [1, 4, 5].
4. Протокол подписания контракта. Про­то­ко­лы элек­трон­ных пла­те­жей и циф­ро­вых де­нег.

Литература для теоретической подготовки: [1, 5].

Приложение 2

**Темы самостоятельных работ**

Для самостоятельных занятий рекомендуются следующие темы:

**Тема 1**. Предварительное распределение ключей.

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

**Тема 2.** Пересылка ключей.

Литература для теоретической подготовки: [2,].

**Тема 4.** Открытое распределение ключей.

Литература для теоретической подготовки: [1, 2].

**Тема 5.** Схема разделения секрета.

Литература для теоретической подготовки: [5].

**Тема 6. С**ертификаты.

Литература для теоретической подготовки: [ 5].

**Тема 7.** Центры сертификации.

Литература для теоретической подготовки: [5].

**Тема 8.** Груп­по­вые про­то­ко­лы. Про­то­ко­лы раз­де­ле­ния сек­ре­та и рас­пре­де­ле­ния клю­чей для те­ле­кон­фе­рен­ции

Литература для теоретической подготовки: [3].

**Тема 9.** Протокол подписания контракта. Про­то­ко­лы элек­трон­ных пла­те­жей и циф­ро­вых де­нег.

Литература для теоретической подготовки: [3].