ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ

Факультет вычислительной техники
Кафедра «Информационная безопасность»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.О.34 «Криптографические протоколы»

Специальность: 10.05.01 Компьютерная безопасность

Специализация: № 5 «Разработка систем защиты информации компьютерных систем объектов информатизации» (по отрасли или в сфере профессиональной деятельности)

ОПОП по специальности:
Компьютерная безопасность
Квалификация выпускника: специалист по защите информации

Форма обучения - очная
Срок обучения — 5,5 лет

Рязань, 2023 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

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.

2. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1	Введение	ОПК-10 (ОПК-10.3; ОПК-10.4; ОПК-10.6)	экзамен
2	Общие сведения о криптографических протокола	ОПК-10 (ОПК-10.3; ОПК-10.4; ОПК-10.6)	экзамен
3	Криптографические хеш-функции и коды аутентификации	ОПК-10 (ОПК-10.3; ОПК-10.4; ОПК-10.6)	экзамен
4	Схемы электронных подписей	ОПК-10 (ОПК-10.3; ОПК-10.4; ОПК-10.6)	экзамен
5	Протоколы идентификации и аутентификации	ОПК-10 (ОПК-10.3; ОПК-10.4; ОПК-10.6)	экзамен
6	Протоколы распределения ключей	ОПК-10 (ОПК-10.3; ОПК-10.4; ОПК-10.6)	экзамен

3. 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:

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 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%

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)	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 экзамен выносится два теоретических вопроса. Максимально студент может набрать 10 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно». Шкала перевода баллов в оценки:

от 8 до 10 баллов - «отлично»;

от 6 до 7 баллов - «хорошо»;

от 3 до 5 баллов - «удовлетворительно»;

менее 3 баллов - «неудовлетворительно»

4. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

4.1. Промежуточная аттестация (экзамен)

Коды компетенций/ и индикаторов	Результаты освоения ОПОП Содержание компетенций/ индикаторов
ОПК-10 (ОПК-10.3; ОПК-10.4; ОПК-10.6)	**Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;** **ОПК-10.3** ***Осуществляет анализ работы криптографических протоколов с использованием BAN – логики.*** **ОПК-10.4** ***Проводит анализ методов криптографической защиты информации, используемых в криптографическом протоколе.*** **ОПК-10.6** ***Настраивает современные криптографические протоколы при сетевом взаимодействии.***

а) типовые тестовые вопросы:

1. Какой федеральный орган государственной власти регулирует процесс лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств:

– ФСБ России (+);
– ФСТЭК России;
– Правительство РФ;
– Министерство обороны РФ.

2. Какой нормативный документ содержит информацию, касающуюся требований лицензирования деятельности по разработке шифровальных (криптографических) средств:

– Приказ ФСТЭК № 17;
– Постановление Правительства РФ № 313 (+);
– Федеральный закон «Об информации, информационных технологиях и защите информации» № 149-ФЗ;
– Указ Президента РФ № 646.

3. Режим защиты информации путем использования СКЗИ может устанавливаться:

– только обладателем информации конфиденциального характера;
– только собственником (владельцем) информационных ресурсов;
– уполномоченными лицами обладателей и (или) собственников информации;
– всеми вышеописанными субъектами (+).

4. Какие виды электронных подписей бывают согласно ФЗ «Об электронной подписи» № 63-ФЗ:

– простая электронная подпись (+);
– усиленная электронная подпись (+);
– персональная электронная подпись;
– совместимая электронная подпись.

5. Кем определяет уполномоченный федеральный орган в сфере использования ЭП согласно ФЗ «Об электронной подписи» № 63-ФЗ:

– Правительством РФ (+);
– ФСБ России;
– ФСТЭК России;
– Президент РФ.

6. В соответствии с СТР-К криптографические средств защиты информации могут использоваться для передачи информации по каналам связи, выходящим за:

– управляемую зону;
– контролируемую зону (+);
– охраняемую зону;
– оберегаемую зону.

7. На какой стадии создания системы защиты информации происходит закупка криптографических средств защиты информации в соответствии с СТР-К:

– на предпроектной стадии;
– на стадии проектирования и реализации ОИ (+);
– на стадии ввода в действие СЗИ;

– на стадии анализа.

8. В соответствии с Приказом ФСБ РФ № 66 необходимость криптографической защиты информации конфиденциального характера при ее обработке и хранение без передачи по каналам связи, а также выбор применяемых СКЗИ определяются (несколько вариантов):

– обладателем данной информации (+);

– пользователем (потребителем данной информации) (+);

– уполномоченным органом;

– нормативными документами.

9. Какими из названных функций обладает криптографический протокол:

– обеспечение доступности;

– обеспечение невозможности отказа и неотслеживаемости;

– обеспечение конфиденциальности (+);

– обеспечение неотказуемости.

10. При перехвате противником сообщения и навязывания его в более поздний момент времени, какую атаку выполняет нарушитель:

– задержка передачи сообщения;

– повторное навязывание сообщений (+);

– подмена;

– атака с известным сеансовым ключом.

11. Какие из перечисленных видов криптографических протоколов относятся к группе протоколов идентификации (аутентификации) участников:

– односторонней аутентификации (+);

– сложной аутентификации;

– двусторонней (взаимной) аутентификации (+);

– комбинированной аутентификации.

12. Какой постулат, применяемый в BAN-логике выглядит таким образом «*P said X»:*

– P когда-либо посылал сообщение, содержащее X, и при этом P доверял X в момент его передачи (+);

– P верит в то, что X истинно;

– кто-либо послал P сообщение, содержащее X, и P может прочитать и повторить (возможно после проведения процедуры расшифрования);

– P имеет права на X.

13. Какие параметры используются в стандарте электронной подписи ГОСТ Р 34.10:

– p-большое простое число длиной от 509 до 512 бит либо от 1020 до 1024 бит (+);

– простой сомножитель числа (p-1), имеющий длину 402…256 бит (+);

– x – некоторое число, большее q;

– a – любое число, меньшее (p-1), при чем такое, что $a^q \bmod p == 1$ (+).

14. Какие из схем относятся с цифровыми подписями с дополнительными функциональными свойствами:

– схема слепой подписи (+);

– схема параллельной подписи;

– схема однозначной подписи;

– схема достоверной подписи.

15. Реализацию каких функций обеспечивает процесс управления ключами:

– распределение ключей (+);

– уничтожение ключей;

– конвертирование ключей;

– генерация ключей (+).

16. Какие протоколы включает в себя схема разделения ключей:

– протокол формирования долей (разделения секрета) и распределения их между пользователями (+);

– протокол достоверности пользователей при разделении секрета;

– протокол восстановления секрета группой пользователей;

– протокол синхронизации секрета.

б) типовые теоретические вопросы:

1. Какие документы в сфере криптографической защиты информации Вы знаете?
2. Назовите виды шифровальных (криптографических) средств (средствам криптографической защиты информации.
3. Какую информацию должен содержать сертификат ключа проверки электронной подписи?
4. Назовите виды электронных подписей и опишите их.
5. При каких условиях использование криптографических средств защиты информации обязательно в соответствии с законодательством РФ.
6. Основные понятия криптографического протокола. Конфиденциальность. Целостность. Аутентификация. Цифровая подпись
7. Свойства, характеризующие безопасность протоколов.
8. BAN-логика.
9. Требования к криптографическим хеш-функциям.
10. Хеш-функция MD4 и MD5.

Типовые контрольные задания или иные материалы

Типовые задания и вопросы для зачета по дисциплине (сводный список)

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. Формальные методы анализа криптопротоколов. Использование специализированных языков и инструментариев. Применение экспертных систем

18. Ban-логика. Формальные модели

19. Требования к криптографическим хеш-функциям

20. Бесключевые хеш-функции

21. Основы построения хеш-функций

22. Хеш-функция на основе блочного алгоритма

23. Хеш-функция md5

24. Алгоритм md4

25. Стандарты на хеш-функции

26. Хеш –функции, задаваемые ключом

27. Коды аутентификации сообщений-MAC

28. Определение схемы цифровой подписи

29. Алгоритм цифровой подписи RSA

30. Алгоритм цифровой подписи Эль Гамаля (EGSA)

31. Алгоритм цифровой подписи Шнорра(SCHNORR)

32. Алгоритм цифровой подписи DSA

33. Отечественный стандарт цифровой подписи ГОСТ Р 34.10

34. Схема подписи Fiat-Shamir

35. Инфраструктура открытых ключей PKI.

36. Основные компоненты PKI.

37. Рекомендации X.509.

38. Схемы слепой подписи.

39. Схемы неоспоримой подписи.

40. Протокол дезавуирования для схемы неоспоримой подписи (Д. Чома).

41. Неотрицаемые цифровые подписи. Подписи уполномоченного свидетеля. Групповая подпись. Доверенная подпись.

42. Протоколы аутентификации на основе паролей. Общие положения.

43. Типовые схемы идентификации и аутентификации пользователя. Схема 1.

44. Типовые схемы идентификации и аутентификации пользователя. Схема 2.

45. Противодействие пассивному перехвату пароля.

46. Противодействие несанкционированному воспроизведению.

47. Генерация одноразовых паролей.

48. Схема парольной защиты S-KEY.

49. Протоколы идентификации типа «запрос-ответ» и рукопожатие. Метод «запрос-ответ».

50. Метод «запрос-ответ» с использованием симметричного шифрования.

51. Метод «запрос-ответ» с использованием ассиметричных алгоритмов шифрования.

52. Протоколы «рукопожатия».

53. Понятие протоколов интерактивного доказательства и доказательства знания.

54. Протоколы с нулевым разглашением.

55. Схема Фейге, Фиата и Шамира.

56. Протокол Гиллу-Кискатра

57. Протокол Шнорра.

58. Протоколы с самосертифицируемыми ключами.

Составил
старший преподаватель кафедры
«Информационная безопасность» Т.И. Калинкина