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

ФТД.О.03 «Методы и средства криптографической защиты информации»

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.

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
	Введение	ОПК-10 (ОПК-10.1)	зачет
	Введение в криптографию	ОПК-10 (ОПК-10.1; ОПК-10.5)	зачет
	Основные классы шифров и их свойства	ОПК-10 (ОПК-10.1)	зачет
	Надежность шифров	ОПК-10 (ОПК-10.1)	экзамен
	Методы синтеза и анализа симметричных криптосистем	ОПК-10 (ОПК-10.1)	экзамен
	Криптографические хеш-функции	ОПК-10 (ОПК-10.1)	экзамен
	Электронная подпись	ОПК-10 (ОПК-10.2)	экзамен
	Средства криптографической защиты информации	ОПК-10 (ОПК-10.1; ОПК-10.2, ОПК-10.5)	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

4. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

4.1. Промежуточная аттестация (экзамен)

Код компетенции	Результаты освоения ОПОП Содержание компетенций
ОПК-10	**Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства**

(ОПК-10.1; ОПК-10.2; ОПК-5)	**криптографической защиты информации при решении задач профессиональной деятельности**. ***ОПК-10.1. Применяет алгоритмы функционирования криптографических систем;.*** ***ОПК-10.2. Применяет алгоритмы функционирования электронной подписи;*** ***ОПК-10.5 Использует методы и средства криптографической защиты информации при решении задач профессиональной деятельности.***

а) типовые тестовые вопросы:

1. Выберите зарубежные стандарты информационной безопасности:
   - «Проектирование решения по руководству информацией и технологиями» (+);
   - ASA X3.9-1966;
   - ISO 2240;
   - «COBIT 2019 Бизнес-модель: Задачи руководства и управления» (+);
   - ГОСТ Р ИСО/МЭК 15408-2012.
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. Задачами криптографии являются
– сокрытие сведений о передаче информации;
– обеспечение конфиденциальности, целостности, невозможности отказа от авторства (+);
– обеспечение доступности информации;
– защита информации от взлома.

10. На основании каких документов разрабатывается модель угроз?
– Приказ ФСТЭК России от 25 декабря 2017 г. N 23 (+);
– Приказ ФСТЭК России от 11 февраля 2013 г. N 17 (+);
– Приказ ФСТЭК России от 25 декабря 2017 г. N 239 (+);
– Приказ ФСТЭК России от 14 марта 2014 г. N 31 (+);
– «Методический документ. Методика оценки угроз безопасности информации» (+).

11. Что такое модель угроз?
– документ, содержащий перечень и описание угроз безопасности информации (+);
– перечень угроз безопасности информации;
– перечень требований по защите информации от угроз безопасности;
– база данных, содержащая перечень и описание угроз безопасности информации.

12. Что такое модель нарушителя:
– абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа. (+);
– описание субъекта атаки на автоматизированную систему;
– предположение о возможности нарушителя;
– описание функций нарушителя.

13. Какие виды моделей нарушителя существуют?:
– вербальная (+);
– формульная;

– векторная;
– матричная.

14. При анализе атаки на объект выделяют:
– источник атаки (+):
– среду проведения атаки;
– объект атаки (+);
– технические средства для проведения атаки.

15. Контролируемая зона - это:
– пространство пребывания сотрудников организации во время рабочего дня;
– пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств (+);
– пространство, в котором ведется видеонаблюдение;
– охраняемая территория, здание, часть здания, помещение;
– помещение, в котором размещены технические средства объекта информатизации.

16. Виды информационной безопасности:
– персональная, корпоративная, государственная (+)
– клиентская, серверная, сетевая;
– локальная, глобальная, смешанная;
– частная, комплексная.

17. Цели информационной безопасности – своевременное обнаружение, предупреждение:
– инсайдерства в организации;
– несанкционированного доступа (+);
– чрезвычайных ситуаций;
– перекодирования информации.

18. Сертификат соответствия - это:
– документ в бумажном виде, содержащий сведения о физическом лице;
– документ, содержащий электронную подпись физического лица;
– документ, удостоверяющий соответствие объекта требованиям технических регламентов, нормативных документам по защите информации (+);
– документ, содержащий подпись удостоверяющего центра.

19. СКЗИ бывают следующих классов:
– А1;
– К1 (+);
– В2;
– Д2.

20. На время отсутствия пользователей СКЗИ должны:
– удаляться;
– быть не активны (выключен монитор);
– при наличии технической возможности быть выключены, отключены от линии связи и убраны в опечатываемые хранилища (+);
– быть заблокированы.

21. Кем осуществляется контроль за соблюдением правил пользования СКЗИ и условий их использования?

- обладателем и пользователем(потребителем) защищаемой информации;
- ФСБ России;
- ФСБ России, обладателем и пользователем (потребителем) защищаемой информации (+);
- ФСТЭК России.

22. Владелец сертификата ключа подписи обязан:

- хранить в тайне закрытый ключ электронной подписи (+);
- хранить в тайне открытый и закрытый ключ электронной подписи;
- хранить в тайне открытый ключ электронной подписи;

23. Что подтверждает юридическую значимость электронной подписи в документе?

- сертификат ключа проверки электронной подписи (+);
- открытый ключ проверки электронной подписи;
- договор оказания услуг;
- схема достоверной подписи.

24. Удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, обязан аннулировать его:

- по заявлению в письменной форме любого пользователя информационной системы;
- удостоверяющий центр не имеет права аннулировать сертификаты ЭП;
- по заявлению в письменной форме владельца сертификата ключа проверки электронной подписи (+);
- по заявлению руководителя организации, сотрудником которой является владелец сертификата ключа проверки электронной подписи;

25. Имеет ли юридическую силу электронная подпись, если она используется не в соответствии со сведениями, указанными в сертификате:

- нет (+);
- не всегда;
- да.

26. Хэш-функция - это:

- электронная подпись документа;
- документ, содержащий электронную подпись физического лица;
- функция, отображающая строки бит в строки бит фиксированной длины (+);
- строка бит, содержащая электронную подпись.

27. СКЗИ бывают следующих классов:

- А1;
- К1 (+);
- В2;
- Д2.

28. Какой аспект информационной безопасности (помимо трех стандартных: конфиденциальность, целостность и доступность) обеспечивается СЗИ ViPNet?

- идентичность;
- сапоставляемость;

- аутентичность (+);
- равнозначность.

29. Для чего используются асимметричные алгоритмы шифрования в системе ViPNet?
    - получения подписи абонентом;
    - для передачи информации по открытым каналам связи;
    - для обмена ключами шифрования и электронной подписи (+);
    - для туннелирования.
30. В чем состоят проблемы симметричного шифрования?
    - в обеспечении доверенной доставки ключей (+);
    - в сохранении в тайне ключей электронной подписи;
    - в росте количества ключей с ростом числа пользователей (+);
    - в недоверии абонентов друг другу.
31. К какому типу сетей относятся сети ViPNet?
    - виртуальному (+);
    - глобальному;
    - закрытому;
    - корпоративному.
32. Для чего используется Криптекс:
    - для шифрования документа;
    - для получения электронной подписи в удостоверяющем центре;
    - для создания электронной подписи документа (+);
    - для получения сертификата пользователя.
33. Для чего нужна программа КриптоПро CSP:
    - для работы на государственных порталах (+);
    - отправки отчётности в налоговую (+);
    - для регистрации онлайн-кассы в налоговой (+);
    - электронного документооборота с контрагентами (+);
    - — участия в электронных торгах (+).

б) типовые теоретические вопросы:

1. Какие нормативные документы в сфере криптографической защиты информации Вы знаете?
2. Назовите виды шифровальных (криптографических) средств 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. Каков порядок оценки угроз безопасности информации?
7. Перечислите риски информационной безопасности.
8. Виды криптографических систем.
9. Кем проводится оценка угроз безопасности информации?

10. Принципы разработки модели угроз.
11. Схема проведения оценки угроз безопасности информации.
12. Исходные данные для определения негативных последствий от реализации угроз безопасности информации.
13. Основные виды нарушителей безопасности информации, подлежащие оценке.
14. Категории нарушителей безопасности информации.
15. Субъекты информационной безопасности.
16. Основные составляющие информационной безопасности.
17. Основные понятия криптографического протокола. Конфиденциальность. Целостность. Аутентификация. Цифровая подпись.
18. Алгоритм работы СКЗИ VipNet клиент.
19. Тунелирование.
20. Требования к криптографическим хеш-функциям.
21. Хеш-функция MD4 и MD5.
22. Построение VPN-сетей.
23. Принципы работы СКЗИ КриптоПРО.
24. Алгоритм работы СКЗИ VipNet клиент.
25. Работа программы VipNet Coordinator.
26. . Инфраструктура открытых ключей PKI.
27. Кроссертификация удостоверяющих центров.
28. Технологии аутентификации.

Типовые контрольные задания или иные материалы

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

1. Основные понятия и определения.
2. Основные понятия и определения по ключу и ключевым документам.
3. Основные задачи криптографии.
4. Конфиденциальность.
5. Симметричные и ассиметричные криптосистемы.
6. Виды криптосистем.
7. Целостность.
8. Аутентификация.
9. Электронная подпись.
10. Управление секретными ключами. Предварительное распределение ключей.
11. Открытое распределение ключей.
12. Схема разделения секрета.
13. Инфраструктура открытых ключей. Сертификаты.
14. Центры сертификации.
15. Международные стандарты по информационной безопасности.
16. Российские нормативно-правовые документы по защите информации.
17. Российские нормативно-правовые документы по криптографической защите информации.
18. Требования к лицензиату в области криптографической защиты информации.

19. Документы для получения лицензии в области криптографической защиты информации.
20. Понятие симметричной криптосистемы.
21. Понятие ассиметричной криптосистемы.
22. Алгоритм Диффи-Хелмана.
23. Криптографический алгоритм «Магма»
24. Криптографический алгоритм «Кузнечик»
25. Инфраструктура открытых ключей PKI.
26. Электронная подпись и ее применение.
27. Виды электронных подписей.
28. Средства шифрования информации на жестких дисках (на примере Secret Disk).
29. Установка и настройка СКЗИ КриптоПро.
30. Использование КриптоПро при передаче информации в вычислительных сетях.
31. Установка и настройка СКЗИ VipNet клиента.
32. Использование СКЗИ VipNet при передаче информации в вычислительных сетях.
33. Межсетевые экраны СКЗИ «Континент».

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