ПРИЛОЖЕНИЕ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Кафедра «Информационная безопасность»

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ**

по дисциплине

**ФТД.В.03 «Криптографические средства защиты информации»**

Специальность: 10.05.01 Компьютерная безопасность

Специализация: № 8 Информационная безопасность объектов информатизации

на базе компьютерных систем в защищенном исполнении

ОПОП по специальности:

Компьютерная безопасность

Квалификация выпускника: специалист по защите информации

Форма обучения - очная

Срок обучения — 5,5 лет

Рязань, 2020 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-9, ПК-2, ПК-5, ПК-10, ПК-18 | зачет |
|  | Стандарты информационной безопасности | ОПК-9, ПК-2, ПК-5, ПК-10, ПК-18 | зачет |
|  | Криптографическая защита информации | ОПК-9, ПК-2, ПК-5, ПК-10, ПК-18 | зачет |
|  | Средства криптографической защиты информации | ОПК-9, ПК-2, ПК-5, ПК-10, ПК-18 | зачет |

**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-9 | Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации. |

**Типовые тестовые вопросы:**

1. Дискреционная политика безопасности - это:

* полномочное управление доступом;
* матричное управление доступом;
* управление доступом разграниченное во времени;
* иерархическое управление;
* избирательное управление (+).

1. Системы, безопасность которых была оценена, но оказалась не удовлетворяющей требованиям более высоких разделов, принадлежат:

* категории А;
* категории В;
* категории С;
* категории D (+).

1. Мандатное управление доступом к выбранным субъектам и объектам характерно для систем:

* класса В1 и выше (+);
* класса В1 и ниже;
* класса С2;
* класса D.

1. При принудительном управлении доступом субъект может записывать информацию в объект, если:

* метка безопасности объекта доминирует над меткой субъекта (+);
* метка безопасности субъекта доминирует над меткой объекта;
* метка безопасности субъекта совпадает с меткой безопасности объекта;
* есть разрешение администратора системы безопасности.

1. При принудительном управлении доступом субъект может читать информацию из объекта, если:

* уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта (+);
* уровень секретности субъекта не выше, чем у объекта, а все категории, перечисленные в метке безопасности субъекта, присутствуют в метке объекта;
* уровень секретности субъекта не выше, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта;
* уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности субъекта, присутствуют в метке объекта.

1. Перечислите классы безопасности в порядке ужесточения требований:

* А, B, C, D;
* C1, C2, B1, B2, B3, A1 (+);
* D, C, B, A (+);
* A1, B3, B2, B1, C2, C1.

1. Системы, безопасность которых была оценена, но оказалась не удовлетворяющей требованиям более высоких разделов, принадлежат:

* категории А;
* категории В;
* категории С;
* категории D (+).

1. Обязательными качествами для монитора обращений являются:

* изолированность (+);
* полнота (+);
* верифицируемость (+);
* надежность.

1. Конкретная реализация монитора обращений, обладающая гарантированной неизменностью, – это:

* монитор безопасности;
* периметр безопасности;
* ядро безопасности (+);
* механизм реализации безопасности.

1. Граница доверенной вычислительной базы – это:

* монитор безопасности;
* периметр безопасности (+);
* ядро безопасности;
* механизм реализации безопасности

**Типовые теоретические вопросы:**

1. Виды политик безопасности.
2. Мандатное разграничение доступа.
3. Дискреционная модель разграничения доступа.
4. Зарубежные стандарты информационной безопасности.
5. Российские стандарты информационной безопасности.
6. Основные положения Доктрины информационной безопасности Российской Федерации.

|  |  |
| --- | --- |
| **Код компетенции** | **Результаты освоения ОПОП**  **Содержание компетенций** |
| ПК-2 | Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности ин-формации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований |

**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.

1. 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.

1. 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 (+).

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

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

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

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

1. 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.

1. 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.

1. 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.

**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.

|  |  |
| --- | --- |
| **Код компетенции** | **Результаты освоения ОПОП**  **Содержание компетенций** |
| 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 |

**Типовые тестовые вопросы:**

1. 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.

1. СКЗИ бывают следующих классов:

* А1;
* К1 (+);
* В2;
* Д2.

1. 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.

1. 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.

1. 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;

1. Что подтверждает юридическую значимость электронной подписи в документе?

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

1. 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;

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

* нет (+);
* не всегда;
* да.

**Типовые теоретические вопросы:**

1. Основные понятия криптографического протокола. Конфиденциальность. Целостность. Аутентификация. Цифровая подпись
2. Алгоритм работы СКЗИ VipNet клиент.
3. Тунелирование.
4. Требования к криптографическим хеш-функциям.
5. Хеш-функция MD4 и MD5.
6. Построение VPN-сетей.

|  |  |
| --- | --- |
| **Код компетенции** | **Результаты освоения ОПОП**  **Содержание компетенций** |
| ПК-10 | Способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации |

**Типовые тестовые вопросы:**

1. Система, которая обеспечивает управление доступом к информации таким образом, что только авторизованные лица или процессы, действующие от их имени, получают право работы с информацией, – это:

* безопасная система;
* доверенная система (+);
* защищенная система;
* авторизованная система.

1. Система, использующая аппаратные и программные средства для обеспечения одновременной обработки информации разной категории секретности группой пользователей без нарушения прав доступа, – это:

* безопасная система;
* доверенная система (+);
* защищенная система;
* авторизованная система.

1. Управление доступом, основанное на сопоставлении меток безопасности субъекта и объекта, – это:

* субъективное управление доступом;
* добровольное управление доступом;
* принудительное управление доступом (+);
* групповое управление доступом.

1. Как называется защита систем передачи и хранения информации от навязывания ложных данных?

* верификация;
* имитозащита (+);
* разграничение доступа;
* шифрование.

1. Невозможность получения сервиса законным пользователем называется:

* DoS-атакой (+);
* Replay-атакой;
* «man-in-the-middle»;
* атакой «дней рождения».

1. В чем заключается основная проблема использования симметричных алгоритмов?

* сложность реализации на ЭВМ;
* легкость криптоанализа таких шифров с появлением ЭВМ;
* трудности при передаче ключей и управлении ими (+);
* применение этих алгоритмов на ЭВМ требует значительных вычислитель-ных ресурсов.

1. К какому классу шифров относится шифр Цезаря?

* шифр перестановки (+);
* простой подстановочный шифр;
* шифр вертикальной перестановки;
* поворотная решетка.

1. Чтобы расшифровать сообщение с помощью асимметричного алгоритма шифрования используются:

* открытый ключ отправителя (+);
* открытый ключ получателя;
* закрытый ключ отправителя;
* закрытый ключ получателя.

**Типовые теоретические вопросы:**

1. Структурная схема симметричных криптографических систем.
2. Принципы построения криптографических алгоритмов.
3. Требования к современным алгоритмам блочных шифров
4. Понятие политики безопасности.
5. Виды политики безопасности.
6. Алгоритм Диффи-Хелмана.

|  |  |
| --- | --- |
| **Код компетенции** | **Результаты освоения ОПОП**  **Содержание компетенций** |
| 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 |

**Типовые тестовые вопросы:**

1. 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.

1. СКЗИ бывают следующих классов:

* А1;
* К1 (+);
* В2;
* Д2.

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

* идентичность;
* сапоставляемость;
* аутентичность (+);
* равнозначность.

1. 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.

1. 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.

1. К какому типу сетей относятся сети ViPNet?

* виртуальному (+);
* глобальному;
* закрытому;
* корпоративному.

1. Для чего используется Криптекс:

* для шифрования документа;
* для получения электронной подписи в удостоверяющем центре;
* для создания электронной подписи документа (+);
* для получения сертификата пользователя.

1. 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 (+).

**Типовые теоретические вопросы:**

1. Принципы работы СКЗИ КриптоПРО.
2. Алгоритм работы СКЗИ VipNet клиент.
3. Работа программы VipNet Coordinator.
4. . Инфраструктура открытых ключей PKI.
5. Кроссертификация удостоверяющих центров.
6. 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. Пересылка ключей.
12. Открытое распределение ключей.
13. Схема разделения секрета.
14. Инфраструктура открытых ключей. Сертификаты.
15. Центры сертификации.
16. Международные стандарты по информационной безопасности.
17. Российские нормативно-правовые документы по защите информации.
18. Российские нормативно-правовые документы по криптографической защите информации.
19. Требования к лицензиату в области криптографической защиты информации.
20. Документы для получения лицензии в области криптографической защиты информации.
21. Понятие симметричной криптосистемы.
22. Понятие ассиметричной криптосистемы.
23. Алгоритм Диффи-Хелмана.
24. Криптографический алгоритм «Магма»
25. Криптографический алгоритм «Кузнечик»
26. Инфраструктура открытых ключей PKI.
27. Электронная подпись и ее применение.
28. Виды электронных подписей.
29. Средства шифрования информации на жестких дисках (на примере Secret Disk).
30. Установка и настройка СКЗИ КриптоПро.
31. Использование КриптоПро при передаче информации в вычислительных сетях.
32. Установка и настройка СКЗИ VipNet клиента.
33. Использование СКЗИ VipNet при передаче информации в вычислительных сетях.
34. Межсетевые экраны СКЗИ «Континент».

Составил

старший преподаватель кафедры

«Информационная безопасность» Т.И. Калинкина

Заведующий кафедрой

«Информационная безопасность» В.Н. Пржегорлинский