ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА»

Факультет вычислительной техники
Кафедра «Информационная безопасность»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.О.28 «Методы и средства криптографической защиты информации»

Специальность: 10.05.03 Информационная безопасность автоматизированных систем

Специализация: № 8 Разработка автоматизированных систем в защищенном исполнении

ОПОП по специальности:

Информационная безопасность автоматизированных систем

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 и двух экзаменов.

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; ОПК-10.2; ОПК-10.3)	зачет
	Введение в криптографию	ОПК-10 (ОПК-10.1; ОПК-10.2; ОПК-10.3)	зачет
	Основные классы шифров и их свойства	ОПК-10 (ОПК-10.1; ОПК-10.2; ОПК-10.3)	зачет
	Надежность шифров	ОПК-10 (ОПК-10.1; ОПК-10.2; ОПК-10.3)	зачет
	Методы синтеза и анализа симметричных криптосистем	ОПК-10 (ОПК-10.1; ОПК-10.2; ОПК-10.3)	экзамен
	Криптографические хеш-функции	ОПК-10 (ОПК-10.1; ОПК-10.2; ОПК-10.3)	экзамен

	Электронные подписи	ОПК-10 (ОПК-10.1; ОПК-10.2; ОПК-10.3)	экзамен
	Средства криптографической защиты информации (СКЗИ)	ОПК-10 (ОПК-10.1; ОПК-10.2; ОПК-10.3)	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-10.1; ОПК-10.2; ОПК-10.3)	**Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства 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-10.3** ***Использует методы и средства криптографической защиты информации при решении задач профессиональной деятельности***

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. Задачами криптографии являются

– сокрытие сведений о передаче информации;

– обеспечение конфиденциальности, целостности, невозможности отказа от авторства (+);

– обеспечение доступности информации;

– защита информации от взлома.

10. Что такое шифрование?

– способ преобразования открытого текста в шифрованное сообщение (+);

– совокупность тем или иным способом структурированных данных комплексом аппаратно-программных средств;

– перевод знаков сообщения из одной формы отображения в другую;

– замена символов одного алфавита символами другого алфавита.

11. Что такое кодирование?

– преобразование обычного, понятного текста в код (+);

– преобразование информации с использованием ключа;

– написание программы;

– получение числового эквивалента буквы.

12. Для восстановления открытого текста требуется:

– ключ (+);

– матрица;

– вектор;

– функция.

13. Выбор средств криптографической защиты осуществляется:

– по сертификату соответствия (+);

– по лицензии на вид деятельности;

– по аттестату соответствия;

– по требованиям заказчика.

14. Среда функционирования криптосредства - это:

– технические средства, совместно с которыми предполагается штатное функционирование криптосредства:

– аппаратные и программные средства защиты информации, находящиеся в помещении с установленным криптографическим средством;

– технические и программные средства, совместно с которыми предполагается штатное функционирование криптосредства и способные влиять на выполнение требований, предъявляемых к криптосредству (+);

– технические и программные средства, совместно с которыми предполагается функционирование криптосредства.

15. Какие виды электронных подписей существуют:
– собственноручная;
– простая (+);
– открытая;
– юридически значимая;
– квалифицированная (+).

16. Подлежат ли поэкземплярному учету (в журнале учета) используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы?
– да (+);
– нет;
– не всегда;
– только при определенных условиях.

17. Что необходимо сделать с выведенными из действия криптоключами?
– разгласить;
– уничтожить (+);
– скопировать;
– хранить в течение определенного срока;
– сдать в удостоверяющий центр.

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. Какой аспект информационной безопасности (помимо трех стандартных: конфиденциальность, целостность и доступность) обеспечивается СЗИ ViPNet?
– идентичность;
– сапоставляемость;
– аутентичность (+);
– равнозначность.

27. 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.

28. 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.

29. К какому типу сетей относятся сети ViPNet?
– виртуальному (+);
– глобальному;
– закрытому;

– корпоративному.

30. Для чего используется Криптекс:
    – для шифрования документа;
    – для получения электронной подписи в удостоверяющем центре;
    – для создания электронной подписи документа (+);
    – для получения сертификата пользователя.
31. 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 (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. История развития криптографии.
7. Задачи криптографии.
8. Виды криптографических систем.
9. Целостность информации.
10. Аутентификация.
11. Управление секретными ключами. Предварительное распределение ключей.
12. Управление секретными ключами. Пересылка ключей.
13. Управление секретными ключами. Открытое распределение ключей.
14. Управление секретными ключами. Схема разделения секрета.
15. Инфраструктура открытых ключей. Сертификаты.
16. Инфраструктура открытых ключей. Центры сертификации.
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. Пересылка ключей.
12. Открытое распределение ключей.
13. Схема разделения секрета.
14. Инфраструктура открытых ключей. Сертификаты.
15. Центры сертификации.
16. Формальные модели шифров. Алгебраическая модель шифра.
17. Формальные модели шифров. Вероятностная модель шифра.
18. Модели открытых текстов. По-значная модель открытого текста.
19. Математические модели открытых текстов. Вероятностная модель открытого текста.
20. Критерии распознавания открытых текстов.
21. Классификация шифров по различным признакам.
22. Шифры перестановки. Модель шифра перестановки
23. Маршрутные перестановки.
24. Табличные перестановки.
25. Шифры замены. Математическая модель шифра замены. Классификация шифров замены.
26. Поточные шифры простой замены.
27. Основные требования к шифрам.
28. Аффинный шифр.
29. Многоалфавитные шифры замены.
30. Генераторы псевдослучайных чисел.

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

1. Энтропия и избыточность языка.
2. Структурная схема симметричных криптографических систем.

3. Принципы построения криптографических алгоритмов.
4. Требования к современным алгоритмам блочных шифров
5. Криптографический алгоритм ГОСТ 28147-89
6. Режимы работы криптографического алгоритма ГОСТ 28147-89
7. Криптографический алгоритм «Магма»
8. Криптографический алгоритм «Кузнечик»
9. Сети Фейсталя
10. Криптографический алгоритм DES
11. Криптографический алгоритм 3DES
12. Криптографический алгоритм AES.
13. Расширение ключа алгоритма AES
14. Проблема распределения ключей симметричного алгоритма
15. Алгоритм Диффи-Хелмана
16. Криптографический алгоритм «Магма»
17. Криптографический алгоритм «Кузнечик»
18. Инфраструктура открытых ключей PKI.
19. Электронная подпись и ее применение.
20. Виды электронных подписей.
21. Средства шифрования информации на жестких дисках (на примере Secret Disk).
22. Установка и настройка СКЗИ КриптоПро.
23. Использование КриптоПро при передаче информации в вычислительных сетях.
24. Установка и настройка СКЗИ VipNet клиента.
25. Использование СКЗИ VipNet при передаче информации в вычислительных сетях.
26. Межсетевые экраны СКЗИ «Континент».

Оценочные материалы составлены в соответствии с рабочей программой дисциплины «Методы и средства криптографической защиты информации» по специальности 10.05.03 Информационная безопасность автоматизированных систем.

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

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО ЗАВЕДУЮЩИМ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**08.08.24** 05:26 (MSK)	Простая подпись
ПОДПИСАНО ЗАВЕДУЮЩИМ ВЫПУСКАЮЩЕЙ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**08.08.24** 05:26 (MSK)	Простая подпись