ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Криптографические методы защиты информации

Код модуля
1156863(1)

Модуль
Информационные технологии

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Агафонов Алексей Владимирович	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
3	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Криптографические методы защиты информации

1.	**Объем дисциплины в зачетных единицах**	5	
2.	**Виды аудиторных занятий**	Лекции Практические/семинарские занятия Лабораторные занятия	
3.	**Промежуточная аттестация**	Экзамен	
4.	**Текущая аттестация**	Контрольная работа	1
		Домашняя работа	1
		Отчет по лабораторным работам	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Криптографические методы защиты информации

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	**Планируемые результаты обучения (индикаторы)**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**
ОПК-10 -Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности	З-1 - Различать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в телекоммуникационных системах З-2 - Объяснять особенности применения криптографических методов и средств защиты информации для защиты систем электронного документооборота П-1 - Иметь опыт использования и исследования криптографических средств защиты информации,	Домашняя работа Контрольная работа Лабораторные занятия Лекции Отчет по лабораторным работам Практические/семинарские занятия Экзамен

	разрабатываемых различными фирмами-производителями, при решении профессиональных задач У-1 - Анализировать программные модели средств криптографической защиты информации	
ОПК-9 -Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	З-1 - Различать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в телекоммуникационных системах З-2 - Объяснять особенности применения криптографических методов и средств защиты информации для защиты систем электронного документооборота П-1 - Иметь опыт использования и исследования криптографических средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач У-1 - Анализировать программные модели средств криптографической защиты информации	Домашняя работа Контрольная работа Лабораторные занятия Лекции Отчет по лабораторным работам Практические/семинарские занятия Экзамен

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.4		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	6,4	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		

Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.3		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа	6,10	100
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям–нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0.3		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
отчет по лабораторным работам	6,16	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -1		
Промежуточная аттестация по лабораторным занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено**		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		
Текущая аттестация на онлайн-занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено		
Промежуточная аттестация по онлайн-занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено**		

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	**Сроки − семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)

2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Практические/семинарские занятия

Примерный перечень тем

1. Исторические шифры. Шифр сдвига. Шифр замены. Шифр Вернама
2. Вычислительно защищенная криптосистема. Абсолютно стойкая криптосистема.
3. Симметричные криптосистемы. Основные принципы современных симметричных алгоритмов
4. Принцип Керкхоффа для криптосистемы
5. Схема порогового разделения. Пороговая схема Шамира

LMS-платформа − не предусмотрена

5.1.3. Лабораторные занятия

Примерный перечень тем

1. Теорема Шеннона об абсолютно стойкой криптосистеме. Энтропия
2. Расстояние единственности. Ложный ключ. Фиктивный ключ
3. Принцип Керкхоффа для криптосистемы
4. Генераторы псевдослучайных чисел
5. Биграммный шифр «два прямоугольника» и метод вскрытия

LMS-платформа − не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Контрольная работа

Примерный перечень тем

1. Нормативно-правовое регулирование в сфере применения средств криптографической защиты информации

2. Методы и средства криптографической защиты компьютерной информации.

Примерные задания

устный опрос , примерные вопросы:

Формула Эйлера. Основные алгоритмы вычисления НОД. Китайская теорема об остатках.

Односторонние функции. Шифр RSA. Цифровая подпись. Система электронного голосования

1. Вычислить подпись Эль-Гамаля для сообщения. Использовать параметры p=79, g=15, параметры x=5 и k=31 системы цифровой подписи и подписываемый текст ШАР. Использовать первый учебный алгоритм хэширования. Ответ введите в формате (N1,N2), например, (23,12) или (33,5) - в скобках и без пробелов.

Ответ:

(27,47)

(47,27)

(55,77)

2. Вычислить подпись Эль-Гамаля для сообщения. Использовать параметры p=79, g=15, параметры x=12 и k=47 системы цифровой подписи и подписываемый текст ЛУЧ. Использовать первый учебный алгоритм хэширования. Ответ введите в формате (N1,N2), например, (23,12) или (33,5) - в скобках и без пробелов.

Ответ:

(41,52)

(41,44)

(52,41)

3. Вычислить подпись Эль-Гамаля для сообщения. Использовать параметры p=79, g=15, параметры x=28 и k=7 системы цифровой подписи и подписываемый текст ОВАЛ. Использовать первый учебный алгоритм хэширования. Ответ введите в формате (N1,N2), например, (23,12) или (33,5) - в скобках и без пробелов.

Ответ:

(71,5)

(71,6)

(71,4)

4. Вычислить подпись Эль-Гамаля для сообщения. Использовать параметры p=79, g=15, параметры x=7 и k=23 системы цифровой подписи и подписываемый текст ТОР. Использовать первый учебный алгоритм хэширования. Ответ введите в формате (N1,N2), например, (23,12) или (33,5) - в скобках и без пробелов.

Ответ:
(61,70)
(66,70)
(54,70)

5. Вычислить подпись Эль-Гамаля для сообщения. Использовать параметры p=79, g=15, параметры x=8 и k=35 системы цифровой подписи и подписываемый текст МЕЧ. Использовать первый учебный алгоритм хэширования. Ответ введите в формате (N1,N2), например, (23,12) или (33,5) - в скобках и без пробелов.
Ответ:
(17,18)
(18,19)
(19,20)

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Криптографические системы, основанные на физических механизмах защиты информации

Примерные задания

1.Изучить теоретический материал для решения задачи по домашней работе
2. Построить алгоритм реализации защиты информации
3. Реализовать механизм защиты информации в криптографической системе
4. Подготовить отчет по выполненной работе
5. Защитить домашнюю работу преподавателю

LMS-платформа − не предусмотрена

5.2.3. Отчет по лабораторным работам

Примерный перечень тем

1. Теорема Шеннона об абсолютно стойкой криптосистеме. Энтропия
2. Расстояние единственности. Ложный ключ. Фиктивный ключ
3. Биграммный шифр «два прямоугольника» и метод вскрытия

Примерные задания

Изучение систем защиты конфиденциальной информации
Изучение и применение библиотек СКЗИ
Разработка средства криптографической защиты информации на базе библиотек СКЗИ
Анализ полученных данных и формирование отчета по домашней работе.

LMS-платформа − не предусмотрена

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Экзамен

Список примерных вопросов

1. Основные понятия, термины, определения. Криптология, криптография, криптоанализ, аутентификация, идентификация. Основные причины использования криптосистем. Симметричная криптосистема

2. Исторические шифры. Шифр сдвига. Шифр замены. Полиалфавитный шифр. Шифр Виженера. Шифр Вернама. Недостатки исторических шифров. (Информационная стойкость)

3. Информационная стойкость криптографических систем Вычислительно защищенная криптосистема. Основные проблемы вычислительно защищенной криптосистемы. Абсолютно стойкая (совершенная) криптосистема

4. К какому классу криптосистем - вычислительно защищенной или абсолютно стойкой относятся следующие криптосистемы: Шифр сдвига. Шифр замены. Шифр Виженера. Шифр Вернама ?

5. Понятие "абсолютной стойкости" в терминах теории вероятности. Теорема Шеннона: критерий абсолютной стойкости шифра. Интерпретация на примере шифра Вернама.

6. Энтропия случайной величины. Свойства энтропии. совместная энтропия двух случайных величин. Условная энтропия двух случайных величин. Неопределенность ключа.

7. Энтропия естественного языка. Расстояние единственности шифра.

8. Криптосистема с секретным ключом. Принцип Керкхоффа. Поточные и блочные шифры

9. Поточные шифры. Генератор ключевого потока. Свойства генератора ключевого потока. Генератор псевдослучайных чисел, основанный на использовании алгебраических свойств М-последовательностей

10. Статистические тесты генераторов ключевого потока.

11. Блочные шифры. Алгоритм DES. Перестановки. Раунды. Алгоритм Фейстеля при шифровании и дешифровании.

12. Сравнение блочных и поточных шифров. Методы организации процедуры исправления ошибок.

13. Статичный ключ. Эфемерный ключ. Распределение ключей. Основные пути решения проблемы распределения ключей. (физические методы, Протоколы с секретным ключом, Протоколы с открытым ключом, современные физические методы).

14. Разделение секрета. Схема порогового разделения секрета. (T, W) - пороговая схема Шамира

15. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Барроуза

LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	**Контрольно-оценочные мероприятия**
Формирование информационной культуры в	целенаправленная работа с информацией	Технология формирования уверенности и	ОПК-10	У-1	Домашняя работа Контрольная работа

сети интернет	для использования в практических целях	готовности к самостоятельной успешной профессиональной деятельности			Лабораторные занятия Лекции Отчет по лабораторным работам Практические/семинарские занятия Экзамен