ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ
Криптографические алгоритмы и протоколы

Код модуля	Модуль
1156042(0)	Криптографические методы защиты информации

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Каннер Татьяна Михайловна		старший преподаватель	МФТИ
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

- **Каннер Татьяна Михайловна, старший преподаватель, МФТИ**
- **Пономарева Ольга Алексеевна, Доцент,**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Криптографические алгоритмы и протоколы

1.	**Объем дисциплины в зачетных единицах**	3	
2.	**Виды аудиторных занятий**	Лекции Практические/семинарские занятия	
3.	**Промежуточная аттестация**	Зачет	
4.	**Текущая аттестация**	Контрольная работа	1
		Домашняя работа	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Криптографические алгоритмы и протоколы

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**
ПК-4 -Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем	З-4 - Применять основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах П-2 - Разрабатывать программное обеспечение, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации У-1 - Оценивать сложность алгоритмов и вычислений У-4 - Проводить комплексное тестирование аппаратных и программных средств	Домашняя работа Зачет Контрольная работа Лекции Практические/семинарские занятия

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 – 0.50		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	2,7	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.50		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа	2,16	100
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям– **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрено		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -не предусмотрено		
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. Протоколы обмена ключами и способы их реализации
2. Протоколы идентификации/аутентификации ключами и способы их реализации
3. Особенности протоколов защиты данных в сети Internet
4. Протоколы разделения секретов. Протоколы с нулевым разглашением и доказательство нулевого разглашения. Примеры реализации

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. Способы криптографической защиты информации
2. Криптосистемы с секретным ключом.
3. Инфраструктура открытых ключей
4. Поточные и блочные алгоритмы
5. Криптографические протоколы и основные требования к ним
6. Протоколы обмена ключами
7. Протоколы генерации и распределения ключей

Примерные задания

1. Что такое шифрование?

а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого+

б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств

в) удобная среда для вычисления конечного пользователя

2. Что такое кодирование?

а) преобразование обычного, понятного текста в код+

б) преобразование

в) написание программы

3. Для восстановления защитного текста требуется:

а) ключ

б) матрица

в) вектор

4. Сколько лет назад появилось шифрование?

а) четыре тысячи лет назад+

б) две тысячи лет назад

в) пять тысяч лет назад

5. Первое известное применение шифра:

а) египетский текст+

б) русский

в) нет правильного ответа

6. Секретная информация, которая хранится вWindows:

а) пароли для доступа к сетевым ресурсам+

б) пароли для доступа в Интернет+

в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере+

7. Что такое алфавит?

а) конечное множество используемых для кодирования информации знаков+

б) буквы текста

в) нет правильного ответа

8. Что такое текст?

а) упорядоченный набор из элементов алфавита+

б) конечное множество используемых для кодирования информации знаков

в) все правильные

9. Выберите примеры алфавитов:

а) Z256 – символы, входящие в стандартные коды ASCII и КОИ-8+

б) восьмеричный и шестнадцатеричный алфавиты+

в) AEE

10. Что такое шифрование?

а) преобразовательный процесс исходного текста в зашифрованный+

б) упорядоченный набор из элементов алфавита

в) нет правильного ответа

11. Что такое дешифрование?

а) на основе ключа шифрованный текст преобразуется в исходный+

б) пароли для доступа к сетевым ресурсам

в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

12. Что представляет собой криптографическая система?

а) семейство T преобразований открытого текста, члены его семейства индексируются символом k+

б) программу

в) систему

13. Что такое пространство ключей k?

а) набор возможных значений ключа+

б) длина ключа

в) нет правильного ответа

14. На какие виды подразделяют криптосистемы?

а) симметричные+

б) ассиметричные+

в) с открытым ключом+

15. Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:

а) 1+

б) 2

в) 3

16. Количество используемых ключей в системах с открытым ключом:

а) 2+

б) 3

в) 1

17. Ключи, используемые в системах с открытым ключом:

а) открытый+

б) закрытый+

в) нет правильного ответа

18. Выберите то, как связаны ключи друг с другом в системе с открытым ключом:

а) математически+

б) логически

в) алгоритмически

19. Что принято называть электронной подписью?

а) присоединяемое к тексту его криптографическое преобразование+

б) текст

в) зашифрованный текст

20. Что такое криптостойкость?

а) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа+

б) свойство гаммы

в) все ответы верны

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Хэш-функции
2. Ассиметричное шифрование
3. Протоколы с нулевым разглашением
4. Криптопротоколы в сети интернет

Примерные задания

1. Написать математическое описание метода шифрования.
2. Составить алгоритм работы ключа шифрования.
3. Написать программный код данного ключа шифрования.
4. Проверить правильность работы программы и оформить отчет по домашней работе.

LMS-платформа − не предусмотрена

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

5.3.1. Зачет

Список примерных вопросов

1. Предмет и задачи. Определение шифра, понятие стойкости.
2. Предположения об исходных условиях криптоанализа
3. Предположения об исходных условиях криптоанализа
4. История криптографии. Криптография древности, частотный критоанализ.
5. Криптография нового времени.
6. Криптография XX века. Принцип Керкгоффса
7. Понятие абсолютной стойкости или теоретико-информационной стойкости. Одноразовый блокнот
8. Понятие псевдослучайности
9. Поточные шифры. Синхронные и самосинхронизирующиеся шифры
10. Требования к поточным шифрам: Постулаты Голомба, профиль линейной сложности
11. Методы построения больших периодов в поточных шифрах. Регистры сдвигов с линейной обратной связью
12. Статистические тесты.
13. Семантическая стойкость. CPA модель атаки.

14. Требования к блочным шифрам. PRP и PRF.
15. Способы построение блочных шифров: подстановки, перестановки, сети фейстеля
16. Детерминированные и недерминированные алгоритмы шифрования.
17. Влияние случайности на стойкость. Слабости блочных шифров
18. HMAC. Хэш-функции. Требования к хэш-функциям
19. Аутентифицированное шифрование
20. Понятие алгоритма с открытым ключом.
21. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана
22. Управление ключами. Групповые ключи. Попарные ключи. Использование мастерключей
23. Протоколы обмена ключами. С сервером, без сервера
24. Известные атаки на протоколы обмена ключами.
25. K-надежные схемы распределения ключей
26. Протоколы разделения секрета
27. Пороговая криптография
28. Протоколы цифровых денег и электронного голосования
LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.