ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Теоретические аспекты информационной безопасности

Код модуля	Модуль
1156422(1)	Теоретические аспекты информационной безопасности

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Баранский Виталий Анатольевич	доктор физико-математических наук, профессор	Профессор	алгебры и фундаментальной информатики
2	Копейцев Вячеслав Ефимович	без ученой степени, без ученого звания	Старший преподаватель	департамент математики, механики и компьютерных наук

Согласовано:

Управление образовательных программ Ю.Д. Маева

Авторы:

- **Баранский Виталий Анатольевич**, **Профессор**, **алгебры и фундаментальной информатики**
- **Копейцев Вячеслав Ефимович**, **Старший преподаватель**, **департамент математики, механики и компьютерных наук**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Теоретические аспекты информационной безопасности

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

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Теоретические аспекты информационной безопасности

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-2 -Способен математически корректно ставить естественнонаучные задачи, обрабатывать научную информацию и результаты исследований, определять закономерности предметной области (Математика и компьютерные науки)	Д-2 - Демонстрировать умения анализировать и обобщать информацию, делать логические умозаключения З-3 - Классифицировать основные методы решения прикладных задач, современные методы информационных технологий	Домашняя работа Зачет Лекции
ПК-4 -Способен разрабатывать и реализовывать алгоритмы на базе	П-3 - Осуществлять обоснованный выбор используемых методов защиты информации	Домашняя работа Зачет Лекции

современных языков программирования и пакетов прикладных программ, осуществлять обоснованный выбор программно-аппаратных средств (Математика и компьютерные науки)	У-3 - Определять оптимальные методы обеспечения защиты информации	
ПК-4 -Готовность к разработке алгоритмов и реализации их на базе языков программирования и пакетов прикладных программ, осуществлять выбор программно-аппаратных средств (Математическое обеспечение и администрирование информационных систем)	П-3 - Осуществлять обоснованный выбор используемых методов защиты информации У-3 - Определять оптимальные методы обеспечения защиты информации	Домашняя работа Зачет Лекции
ПК-5 -Способность собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям (Математическое обеспечение и администрирование информационных систем)	Д-2 - Демонстрировать умения анализировать и обобщать информацию, делать логические умозаключения З-3 - Классифицировать основные методы решения прикладных задач, современные методы информационных технологий	Домашняя работа Зачет Лекции

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 – 1		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
активность на занятиях	17	*10*
домашняя работа	16	*90*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.6		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.4**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрено		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– не предусмотрено		
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 –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**	**Шкала оценивания**

	обучения (выполненное оценочное задание)	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)

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

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Домашняя работа

Примерный перечень тем

1. Алгоритмы шифрования.

2. Безопасные протоколы прикладного уровня.

Примерные задания

Студенту выдается зашифрованное сообщение:

Фхн энщхужетнн пелиао цнсжур месйтдйчцд ихшзнс, учцчудюнс уч тйзу ж ерщежнчй те

щнпцнхужеттуй ьнцру фумныно. Энщх Ыймехд султу преццнщнынхужечб пеп энщх

фуицчетужпн, фхн ёурйй шмпуо преццнщнпеынн — энщх фхуцчуо месйта. Энщх темжет

ж ьйцчб хнсцпузу нсфйхечухе Зед Грнд Ыймехд, нцфурбмужежэйзу йзу ирд цйпхйчтуо фйхйфнцпн.

Известно, что исходный текст построен над тем же алфавитом, что и зашифрованный.

Ставится задача применить методы частотного анализа и расшифровать сообщение.

Задача: трое студентов решили создать собственную реализацию криптосистемы Диффи-

Хеллмана, алгоритм они реализовали следующим образом:

1. Стороны договариваются о параметрах алгоритма p и g
2. Стороны, 1, 2 и 3 генерируют свои ключи — a, b и c соответственно.
3. Сторона 1 вычисляет pa = t и посылает 2.
4. Сторона 2 вычисляет tb = s и посылает его 3.
5. Сторона 3 вычисляет tc = u и получает тем самым общий секретный ключ.
6. Сторона 2 вычисляет gb и посылает его 3.
7. Сторона 3 вычисляет (gb)c = gbc и посылает его 2.
8. Сторона 2 вычисляет (gbc)a = gbca = gabc — общий секретный ключ.
9. Сторона 3 вычисляет gc и посылает его стороне 1.
10. Сторона 1 вычисляет (gca)b = gcab = gabc и также получает общий секретный ключ.

Однако, данная система не работает, где-то в реализации были допущены ошибки. Задача:

найти данные ошибки и исправить так, чтобы криптосистема обеспечивала должный уровень

защиты передаваемой информации.

LMS-платформа − не предусмотрена

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

5.3.1. Зачет

Список примерных вопросов

1. 1. Формат исполняемых файлов PE-EXE. 2. Техники динамического импортирования стороннего кода, методы обнаружения и ана- лиза подобных файлов. 3. Основные техники анализа приложений с использованием дизассемблера. 4. Основные техники анализа приложений с использованием отладчика. 5. Изменения, происходящие с загруженным в память исполняемым файлом в результате создания процесса операционной системой. 6. Формат исполняемых файлов ELF. 7. Бинарные уязвимости в исполняемых файлах, методы обнаружения и борьбы с ними. 8. Настройка средств ОС для минимизации рисков инцидентов информационной безопас- ности. 9. Настройка сторонних защитных средств для минимизации рисков инцидентов информа- ционной безопасности. 10. Принципы работы и архитектура типового антивирусного решения. 11. История криптографии, основные этапы развития. 12. Симметричная криптография, основные алгоритмы, преимущества и недостатки. 13. Основные методы атак на симметричные шифры и техники борьбы с ними. 14. Ассиметричная криптография, схема Диффи-Хеллмана, основные алгоритмы, преиму- щества и недостатки. 15. Основные методы атак на асимметричные шифры и техники борьбы с ними.

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**
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-4	У-3 П-3	Домашняя работа Зачет Лекции