

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ**

Математические основы защиты информации и информационной
безопасности

Код модуля
1157606

Модуль
Специальные технологии разработки ПО

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Корнякова Елена Михайловна		Старший преподаватель	Интеллектуальных информационных технологий

Согласовано:

Управление образовательных программ

Е.А. Смирнова

Авторы:

- **Корнякова Елена Михайловна, Старший преподаватель, Интеллектуальных информационных технологий**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ **Математические основы защиты информации и информационной безопасности**

1.	Объем дисциплины в зачетных единицах	3	
2.	Виды аудиторных занятий	Лекции Лабораторные занятия	
3.	Промежуточная аттестация	Экзамен	
4.	Текущая аттестация	Контрольная работа	1
		Домашняя работа	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ **Математические основы защиты информации и 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
ОПК-2 -Способен самостоятельно ставить, формализовывать и решать задачи, относящиеся к профессиональной деятельности, используя методы моделирования и математического анализа	Д-1 - Проявлять ответственность и настойчивость в достижении цели З-1 - Сделать обзор основных методов моделирования и математического анализа, применимых для формализации и решения задач профессиональной деятельности П-1 - Решать самостоятельно сформулированные практические задачи, относящиеся к профессиональной деятельности методами	Контрольная работа Лабораторные занятия Лекции Экзамен

	<p>моделирования и математического анализа, в том числе с использованием пакетов прикладных программ</p> <p>У-1 - Самостоятельно сформулировать задачу области профессиональной деятельности, решение которой требует использования методов моделирования и математического анализа</p>	
<p>ПК-4 -Способен управлять проектами в области ИТ малого и среднего уровня сложности в условиях неопределенностей, порождаемых запросами на изменения, с применением формальных инструментов управления рисками и проблемами проекта</p>	<p>З-4 - Изложить принципы и методы управления информационной безопасностью ресурсов проекта в области ИТ.</p> <p>З-5 - Сформулировать принципы обеспечения информационной безопасности ресурсов проекта в области ИТ.</p> <p>П-4 - Иметь практический опыт управления информационной безопасностью ресурсов проекта в области ИТ.</p> <p>У-4 - Анализировать возможные угрозы для безопасности данных проекта в области ИТ.</p>	<p>Лабораторные занятия Экзамен</p>
<p>УК-7 -Способен обрабатывать, анализировать, передавать данные и информацию с использованием цифровых средств для эффективного решения поставленных задач с учетом требований информационной безопасности</p>	<p>З-1 - Сделать обзор угроз информационной безопасности, основных принципов организации безопасной работы в информационных системах и в сети интернет</p> <p>З-2 - Описать способы и средства защиты персональных данных и данных в организации в соответствии с действующим законодательством</p> <p>П-1 - Обосновать выбор технических и программных средств защиты персональных данных и данных организации при работе с информационными системами на основе анализа потенциальных и реальных угроз безопасности информации</p>	<p>Домашняя работа Лекции Экзамен</p>

	У-1 - Определять основные угрозы безопасности при использовании информационных технологий и выбирать оптимальные способы и средства защиты персональных данных и данных организации от мошенников и вредоносного ПО	
--	---	--

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
<i>Контрольная работа</i>	1,10	100
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.60		
Промежуточная аттестация по лекциям – экзамен		
Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.40		
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 – 0.50		
Текущая аттестация на лабораторных занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
<i>домашняя работа</i>	1,15	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 1.00		
Промежуточная аттестация по лабораторным занятиям – нет		

Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – 0.00		
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. Лабораторные занятия

Примерный перечень тем

1. Алгоритмы симметричного шифрования
 2. Криптография с открытым ключом
 3. Хэш-функции и аутентификация сообщений
 4. Электронная цифровая подпись
 5. Криптография с использованием эллиптических кривых
 6. Алгоритмы обмена ключей и протоколы Аутентификации
 7. Инфраструктура открытого ключа (PKI)
- 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. Криптография с открытым ключом
2. Хэш-функции и аутентификация сообщений

Примерные задания

- Основные понятия криптографии с открытым ключом
- Шифрование
- Создание и проверка цифровой подписи
- Алгоритмы RSA и Диффи-Хеллмана
- Основные понятия обеспечения целостности сообщений с помощью MAC и хэш-функций
- Простые хэш-функции
- Сильные хэш-функции MD5, SHA-1, SHA-2, ГОСТ 3411
- Обеспечение целостности сообщений и вычисление MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC

LMS-платформа – не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Простые и сильные хэш-функции

Примерные задания

1. Придумайте некоторую хэш-функцию и вкратце проанализируйте ее, учитывая сложность подсчета и вероятности появления коллизий
2. Используя Вашу хэш-функцию, реализуйте 2 подхода к построению хэш-таблиц с помощью цепочек и с открытой адресацией (к примеру, линейное или квадратичное пробирование из книги Кормена, глава «Хэш-таблицы»)
3. Для каждого из 2-х подходов оцените время (сложность, т.е. количество сравнений элементов) для поиска случайного числа x (предполагайте, что Ваши ключи должны быть большими или используйте строки, так как для малых значений существует прямой метод

индексации). В итоге, в среднем случае сложность занимает $O(1+\epsilon)$ времени, но это зависит от Вашей хэш-функции и наша цель проверить данное утверждение

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 и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; классификация атак
2. Алгоритмы симметричного шифрования. Понятие стойкости алгоритма, типы операций, используемых в алгоритмах симметричного шифрования. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ. Алгоритмы DES и тройной DES
3. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, режимы выполнения алгоритмов симметричного шифрования. Способы создания псевдослучайных чисел
4. Новый стандарт алгоритма симметричного шифрования – AES. Критерии выбора алгоритма и сравнительная характеристика пяти финалистов; атаки на алгоритмы с уменьшенным числом раундов и понятие резерва безопасности. Характеристики алгоритмов, являющихся финалистами конкурса AES
5. Алгоритм Rijndael. Математические понятия, лежащие в основе алгоритма Rijndael. Структура алгоритма Rijndael
6. Основные понятия, относящиеся к криптографии с открытым ключом, способы использования алгоритмов с открытым ключом: шифрование, создание и проверка цифровой подписи, обмен ключа. Алгоритмы RSA и Диффи-Хеллмана
7. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; требования к хэш-функциям; простые и сильные хэш-функции
8. Сильные хэш-функции MD5, SHA-1, SHA-2, ГОСТ 3411. Обеспечение целостности сообщений и вычисление MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC
9. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS
10. Криптография с использованием эллиптических кривых. Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой. Аналоги алгоритма Диффи-Хеллмана на эллиптических кривых, алгоритма цифровой подписи на эллиптических кривых и алгоритма шифрования с открытым ключом получателя на эллиптических кривых
11. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны. Сравнение протоколов аутентификации с использованием временных меток
12. Инфраструктура открытого ключа. Сертификаты X.509 v3, CRL v2, протокол OCSP
13. Назовите преимущества и недостатки однократного гаммирования

- 14. Необходимые и достаточные условия абсолютной стойкости шифра
 - 15. Определение сети Файстеля и лавинообразного эффекта
 - 16. Процесс дешифрования шифра Файстеля
 - 17. Общая схема шифрования DES. Процесс расшифровывания данных в DES
 - 18. Алгоритм шифрования ГОСТ 28147-89
- 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.