ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Методы и средства криптографической защиты информации

Код модуля	Модуль
1157413(1)	Методы и средства криптографической защиты информации

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Домуховский Николай Анатольевич	без ученой степени, без ученого звания	Старший преподаватель	алгебры и фундаментальной информатики
2	Поршнев Сергей Владимирович	доктор технических наук, профессор	Профессор	Учебно-научный центр "Информационная безопасность"

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Методы и средства криптографической защиты информации

1.	**Объем дисциплины в зачетных единицах**	4	
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 Методы и средства криптографической 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**
ПК-7 -Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	З-1 - Различать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в телекоммуникационных системах З-2 - Различать 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	Домашняя работа Контрольная работа Лабораторные занятия Лекции Экзамен

	решении профессиональных задач У-1 - Анализировать программные модели средств криптографической защиты информации	

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 – 0.5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	5,9	*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 – 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 –0.5		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа	5,6	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. Лабораторные занятия

Примерный перечень тем

1. Система защиты конфиденциальной информации StrongDisk
2. Система защиты корпоративной информации Secret Disk

3. Система криптографической защиты информации «Верба-OW»
4. Организация VPN средствами СКЗИ VipNet
5. Организация VPN средствами СКЗИ StrongNet
6. Организация VPN сетевого уровня средствами программного комплекса «Игла-П»
7. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ «КриптоПро CSP»
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
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)
LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем
1. Разработка средства криптографической защиты информации
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 и постулаты криптографии
2. Понятие параметризированной функции зашифрования (расшифрования).
3. Алгоритмы шифрования данных
4. Ключи шифрования данных
5. Функциональные возможности современных криптосредств
6. Методы криптографической защиты информации
7. Носитель ключевой информации
8. Классическая схема криптографической защиты информации. Ее достоинства и недостатки. Примеры симметричных криптоалгоритмов
9. Схема криптографической защиты информации с открытым ключом. Ее достоинства и недостатки. Примеры асимметричных криптоалгоритмов
10. Понятие хэш-функции
11. Основные свойства хеш-функций
12. Цифровой конверт
13. Структура файла-образа виртуального шифрованного диска
14. Понятие электронной подписи, способы формирования электронной подписи
15. Схема использования электронной подписи
16. Требования к средствам электронной подписи
17. Классификация средств электронной подписи в зависимости от способности противостоять атакам нарушителя
18. Способы обеспечения гарантированного удаления информации
19. Контроль целостности информации
20. Аудит безопасности в СКЗИ
21. Классификация аппаратно-программных средств защиты информации
22. Понятие криптосредства. Возможности СКЗИ по криптографическому преобразованию информации
23. Основные возможности СКЗИ «StrongDisk»
24. Основные возможности СКЗИ «Secret Disk»
25. Основные возможности СКЗИ «Верба-OW»
26. Защита сетевого трафика на основе технологии VPN
27. Основные возможности СКЗИ «КриптоПро CSP»
28. Структура криптографического контейнера СКЗИ «КриптоПро CSP». Назначение элементов
29. Лицензирование и сертификация в области проектирования средств защиты информации
30. Порядок обращения с криптосредствами и криптоключами к ним
31. Модели и типы угроз безопасности персональных данных

32. Уровни защищенности информационных систем персональных данных
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 целенаправленная работа с информацией для использования в практических целях	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности Технология самостоятельной работы	ПК-7	П-1	Домашняя работа Контрольная работа Лабораторные занятия Лекции Экзамен