ПРИЛОЖЕНИЕ А
ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
ПО ДИСЦИПЛИНЕ «Методы и средства криптографической защиты информации»

1. Перечень оценочных средств для компетенций, формируемых в результате освоения дисциплины

Код контролируемой компетенции	Способ оценивания	Оценочное средство
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Экзамен	Комплект контролирующих материалов для экзамена

2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Оцениваемые компетенции представлены в разделе «Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций» рабочей программы дисциплины «Методы и средства криптографической защиты информации».

При оценивании сформированности компетенций по дисциплине «Методы и средства криптографической защиты информации» используется 100-балльная шкала.

Критерий	Оценка по 100-балльной шкале	Оценка по традиционной шкале
Студент освоил изучаемый материал (основной и дополнительный), системно и грамотно излагает его, осуществляет полное и правильное выполнение заданий в соответствии с индикаторами достижения компетенций, способен ответить на дополнительные вопросы.	75-100	*Отлично*
Студент освоил изучаемый материал, осуществляет выполнение заданий в соответствии с индикаторами достижения компетенций с непринципиальными ошибками.	50-74	*Хорошо*
Студент демонстрирует освоение только основного материала, при выполнении заданий в соответствии с индикаторами достижения компетенций допускает отдельные ошибки, не способен систематизировать материал и делать выводы.	25-49	*Удовлетворительно*
Студент не освоил основное содержание изучаемого материала, задания в соответствии с индикаторами достижения компетенций не выполнены или выполнены неверно.	<25	*Неудовлетворительно*

3. Типовые контрольные задания или иные материалы, необходимые для оценки уровня достижения компетенций в соответствии с индикаторами

1.Применение классических шифров для обеспечения конфиденциальности информации

Компетенция	Индикатор достижения компетенции
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2 Способен применять средства криптографической защиты при решении профессиональных задач

Практическое задание (ОПК-9.2):

1. Зашифровать фразу, используя шифр Цезаря.
2. Зашифровать фразу, используя шифр перестановки.
3. Зашифровать фразу, используя квадратную таблицу Тритемия.
4. Зашифровать фразу, используя таблицу Вижинера.

2.Применение средств криптографической защиты для блочного шифрования

Компетенция	Индикатор достижения компетенции
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2 Способен применять средства криптографической защиты при решении профессиональных задач

Практическое задание (ОПК-9.2):

1. Выполнить шифрование файла с использование программного обеспечения ViPNet PKI Client (пробная версия) в режиме алгоритма ГОСТ 28147-89.
2. Выполнить шифрование файла с использование программного обеспечения КриптоПро CSP (пробная версия) в режиме алгоритмов ГОСТ Р 34.12-2015, ГОСТ 28147-89, AES (128/192/256), 3DES, RC2, RC4.
3. Выполнить шифрование файла с использование программного обеспечения Folder Lock в режиме алгоритма AES.
4. Выполнить шифрование файла с использование программного обеспечения PGP Desktop в режиме AES.

3.Применение средств криптографической защиты для поточного шифрования данных

Компетенция	Индикатор достижения компетенции
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2 Способен применять средства криптографической защиты при решении профессиональных задач

Практическое задание (ОПК-9.2):

1. С использованием языка программирования высокого уровня реализовать программу поточного шифрования на основе 4-х разрядного регистра сдвига с линейной обратной связью в синхронном режиме. Осуществить шифрование двоичной последовательности.
2. С использованием языка программирования высокого уровня реализовать программу поточного шифрования на основе 4-х разрядного регистра сдвига с линейной обратной связью в самосинхронизирующемся режиме. Осуществить шифрование двоичной последовательности.

4.Применение средств криптографической защиты для обеспечения контроля целостности

Компетенция	Индикатор достижения компетенции
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2 Способен применять средства криптографической защиты при решении профессиональных задач

Практическое задание (ОПК-9.2):

1. Используя программное обеспечение ViPNet HashCalc (пробная версия), осуществить расчет контрольной суммы файла. Убедиться в корректности контроля целостности после внесения изменения в файл.
2. Используя онлайн-калькулятор, осуществить расчет хеш-суммы текстовой строки. Убедиться в корректности контроля целостности после внесения изменения в информацию.

5.Применение средств криптографической защиты для ассиметричного шифрования

Компетенция	Индикатор достижения компетенции
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2 Способен применять средства криптографической защиты при решении профессиональных задач

Практическое задание (ОПК-9.2):

1. Используя программное обеспечение КриптоАРМ (пробная версия), осуществить шифрование файла с применением ассиметричного алгоритма шифрования. Осуществить расшифровку файла.
2. Используя программного обеспечение КриптоПРО (пробная версия), осуществить шифрование файла с применением ассиметричного алгоритма шифрования. Осуществить расшифровку файла.
3. Используя программного обеспечение PGP, осуществить шифрование файла с применением ассиметричного алгоритма шифрования. Осуществить расшифровку файла.

6.Применение средств криптографической защиты для вычисления электронной подписи

Компетенция	Индикатор достижения компетенции
ОПК-9 Способен применять средства криптографической и технической защиты	ОПК-9.2 Способен применять средства криптографической защиты при решении

информации для решения задач профессиональной деятельности	профессиональных задач

Практическое задание (ОПК-9.2):

1. С применением программного обеспечения КриптоАРМ (пробная версия), осуществить подписание электронной подписью документа в режиме присоединенной подписи. Осуществить проверку электронной подписи.
2. С применением программного обеспечения КриптоАРМ (пробная версия), осуществить подписание электронной подписью документа в режиме отсоединенной подписи. Осуществить проверку электронной подписи.
3. Осуществить подписание электронной подписью текстового файла средствами MS Office. Осуществить проверку электронной подписи.
4. Осуществить подписание электронной подписью файла PDF средствами AdobeReader. Осуществить проверку электронной подписи.
5. С применением программного обеспечения PGP осуществить подписание электронной подписью документа. Осуществить проверку электронной подписи.

7.Применение средств криптографической защиты для организации сетевого взаимодействия

Компетенция	Индикатор достижения компетенции
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2 Способен применять средства криптографической защиты при решении профессиональных задач

Практическое задание (ОПК-9.2):

1. Настроить сетевое взаимодействие 2-х рабочих станций. Средствами операционной системы выполнить настройку протокола IPSec. Продемонстрировать результаты.
2. С применением программного обеспечения ViPNet Client и ViPNet coordinator (пробные версии) осуществить настройку безопасного сетевого взаимодействия рабочих станций.

4. Файл и/или БТЗ с полным комплектом оценочных материалов прилагается.