Приложение

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущей и промежуточной аттестации

по учебной дисциплине

«Современные методы обеспечения безопасности в информационных системах»

для направления подготовки **09.04.01 -Информатика и вычислительная техника**

Магистерская программа "Информационные системы в экономике и управлении"

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

	1 семестр	2 семестр	3 семестр	4 семестр
ОК-1 способностью совершенствовать и развивать свой интеллектуальный и общекультурный уровень				
Б1.Б.1 Иностранный язык			+	
Б1.В.ОД.6 Современные методы обеспечения безопасности в информационных системах			+	
Б2.У Учебная практика	+			
Б3. Государственная итоговая аттестация				+
Этапы формирования компетенций	1		2	3
ОК-8 способностью к профессиональной эксплуатации современного оборудования и приборов (в соответствии с целями магистерской программы)				
Б1.Б.4 Распределенные информационные системы			+	
Б1.В.ОД.6 Современные методы обеспечения безопасности в информационных системах			+	
Б1.В.ДВ.3.2 Управление проектами внедрения информационных систем		+		
Б3. Государственная итоговая аттестация				+
Этапы формирования компетенций		1	2	3
ОПК-3 способностью анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности				
Б1.В.ОД.1 Специальные главы экономики	+			
Б1.В.ОД.6 Современные методы обеспечения безопасности в информационных системах			+	
Б2.У Учебная практика	+			
Б2.П Производственная практика		+	+	
Б3. Государственная итоговая аттестация				+
Этапы формирования компетенций	1	2	3	4
ОПК-6 способностью анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями				
Б1.Б.3 Технология разработки программного обеспечения	+			
Б1.В.ОД.5 Разработка приложений для мобильных устройств			+	
Б1.В.ОД.6 Современные методы обеспечения безопасности в информационных системах			+	
Б1.В.ДВ.3.1 Информационно-аналитические системы управления		+		
Б1.В.ДВ.4.1 Бизнес-моделирование		+		
Б2.У Учебная практика	+			
Б2.П Производственная практика		+	+	
Б2.Н Научно-исследовательская работа		+		+
Б2.Пд Преддипломная практика				+
Б3. Государственная итоговая аттестация				+
Этапы формирования компетенций	1	2	3	4

ПК-7 **применением перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий**				
Б1.В.ОД.3 Современные технологии имитационного моделирования и вычислительного эксперимента в исследовании экономических информационных систем		+		
Б1.В.ОД.4 Архитектура современных программных приложений		+		
Б1.В.ОД.6Современные методы обеспечения безопасности в информационных системах			+	
Б1.В.ДВ.2.2 Управление электронным бизнесом	+			
Б2.У Учебная практика	+			
Б2.П Производственная практика		+	+	
Б2.Н Научно-исследовательская работа		+		+
Б3. Государственная итоговая аттестация				+
Этапы формирования компетенций	1	2	3	4
ПК-11 **способностью формировать технические задания и участвовать в разработке аппаратных и (или) программных средств вычислительной техники**				
Б1.Б.3 Технология разработки программного обеспечения	+			
Б1.В.ОД.4 Архитектура современных программных приложений		+		
Б1.В.ОД.6 Современные методы обеспечения безопасности в информационных системах			+	
Б1.В.ДВ.4.1 Бизнес-моделирование		+		
Б2.Пд Преддипломная практика				+
Б3. Государственная итоговая аттестация				+
Этапы формирования компетенций	1	2	3	4

1. Описание показателей и критериев оценивания компетенций-на различных этапах их формирования, описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

2.1 Показатели и критерии оценивания компетенций на различных этапах их формирования (промежуточная аттестация)

Компетенции	Показатели	Критерии в соответствии с уровнем освоения ОП			Оценочное средство (промежуточная аттестация)
		пороговый (удовлетворительно)	стандартный (хорошо)	эталонный (отлично)	
ОК-1	Знать	Базовые нормативные правовые акты в сфере информационной безопасности и использовать их в различных сферах деятельности	Базовые нормативные правовые акты и эволюцию нормативных правовых актов в сфере регулирования информационной безопасности в различных сферах деятельности	Нормативные правовые акты и эволюцию нормативных правовых актов, актуальные проблемы применения нормативных правовых актов в сфере информационной безопасности в различных сферах деятельности	Теоретические вопросы
	Уметь	Применять использовать законодательную базу Российской Федерации для поиска нормативно-правовых актов, регулирующих вопросы информационной безопасности в различных сферах деятельности	Применять при защите информации расширенный перечень нормативных правовых актов, регулирующих вопросы информационной безопасности в различных сферах деятельности	Применять при защите информации современные правила и принципы постановки стандартных задач профессиональной деятельности, применять расширенный перечень нормативных правовых актов, регулирующих вопросы информационной безопасности в различных сферах деятельности	Практическое задание
	Владеть	Навыками применения по инструкции преподавателя базовых нормативных правовых актов в сфере информационной безопасности	Навыками самостоятельного применения расширенного перечня нормативных правовых актов в сфере информационной безопасности»	Опытом самостоятельного применения расширенного перечня нормативных правовых актов в сфере информационной безопасности и проверки на соответствие национальным и международным стандартам	Практическое задание

ОК-8	Знать	назначение к профессиональной эксплуатации современного оборудования и приборов	Состав, структуру и назначение профессиональной эксплуатации современного оборудования и приборов	Архитектуру, состав, структуру, тенденции развития и назначение профессиональной эксплуатации современного оборудования и приборов	Теоретические вопросы
	Уметь	Использовать современные средства вычислительной техники по инструкции преподавателя	Самостоятельно современные средства вычислительной техники	Уверенно применять современные средства вычислительной техники и информационно - телекоммуникационных сетей	Практическое задание
	Владеть	Основными приемами работы с современными средства вычислительной техники, затрудняясь их применять без инструкции преподавателя	Основными методами работы с современными средства вычислительной техники	Различными методами работы с современными средства вычислительной техники, реализуя навык саморазвития	Практическое задание
ОПК-3	Знать	Основные критерии для оценки уровня своих компетенций для обеспечения информационной безопасности	Основные и дополнительные критерии для оценки уровня своих компетенций для обеспечения информационной безопасности	Современные критерии для оценки уровня своих компетенций для обеспечения информационной безопасности, а также современные методы выполнения анализа и оценки	Теоретические вопросы
	Уметь	Применять методы анализа и оценки уровня своих компетенций для обеспечения информационной безопасности по инструкции преподавателя	Самостоятельно применять методы анализа и оценки уровня своих компетенций для обеспечения информационной безопасности в сочетании с готовностью к саморегулированию дальнейшего образования и профессиональной мобильности	Уверено анализировать и оценивать уровни своих компетенций для обеспечения информационной безопасности в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности	Практическое задание
	Владеть	Основными навыками оценки уровня своих компетенций для обеспечения информационной безопасности	Комплексом навыков для оценки уровня своих компетенций для обеспечения информационной безопасности	Уверенно владеть навыками оценки уровня своих компетенций для обеспечения информационной безопасности современного предприятия	Практическое задание

ОПК-6	Знать	Основные требования информационной безопасности применительно решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	Современные требования национальных и международных стандартов информационной безопасности применительно решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	Современные требования национальных и международных стандартов информационной безопасности применительно решения различных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, а также методы и способы их обеспечения на практике	Теоретические вопросы
	Уметь	решать различные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий соблюдая базовые принципы информационной безопасности	решать различные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий соблюдая требования и принципы информационной безопасности, закрепленные в законодательстве РФ	решать различные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом современных требований национальных и международных стандартов информационной безопасности	Практическое задание
	Владеть	Инструментами решения различных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, соответствующих принципам информационной безопасности	Средствами решения различных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, отвечающих требованиям национальных стандартов информационной безопасности	Методами и средствами решения различных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, отвечающих требованиям национальных и международных стандартов информационной безопасности	Практическое задание

ПК-7	Знать	Основные структурные элементы технического задания отвечающего требованиям информационной безопасности	Методику составления технического задания и способы участия в разработке аппаратных и (или) программных средств вычислительной техники	Регламент и политики информационной безопасности в части положений касающихся разработки технического задания и порядка его выполнения	Теоретические вопросы
	Уметь	По инструкции преподавателя формировать техническое задание отвечающее требованиям информационной безопасности	Самостоятельно формировать техническое задание отвечающее требованиям информационной безопасности	Самостоятельно и уверено формировать техническое задание, отвечающее современным требованиям информационной безопасности, а также разрабатывать аппаратные и (или) программные средства вычислительной техники с обеспечением требований информационной безопасности	Практическое задание
	Владеть	По инструкции преподавателя навыками формирования технические задания для разработки аппаратных и (или) программных средств вычислительной техники с обеспечением требований информационной безопасности	Навыками формирования технические задания для разработки аппаратных и (или) программных средств вычислительной техники с обеспечением требований информационной безопасности	Навыками самостоятельного и уверенного формирования технические задания для разработки аппаратных и (или) программных средств вычислительной техники с обеспечением требований информационной безопасности	Практическое задание
ПК-11	Знать	- понятие информационной безопасности; - способы защиты современных систем обработки данных;	современные технические и программные средства, обеспечивающие информационную безопасность; - концепции, модели безопасности и их применение;- общие алгоритмы построения систем защиты объектовВТ.	- основы унифицированного процесса защиты информации; - методы криптографии; - нормативно-руководящие и нормативно-справочные документы	Теоретические вопросы

	Уметь	- выявлять угрозы безопасности информации; -применять современные методы защиты информации	- применять инструментальные средства для создания и редактирования документов профессионального назначения; - применять методологии и обеспечения информационной безопасности.	- применять инструментальные средства для создания и редактирования документов профессионального назначения; - применять современные информационные технологии для самостоятельного овладения новыми знаниями; - применять методологии и обеспечения информационной безопасности. - создавать собственные компоненты и библиотеки в программной среде для защиты информации.	Практическое задание
	Владеть	- инструментарием для документирования проектных решений; - способами постановки задач по созданию комплекса мер защиты информации; - различными средствами защиты информации.	- методами построения моделей и процессов управления проектом ПИ; - современными информационно-коммуникационными технологиями в сфере информационной безопасности; - методами разработки требований и проектированию программного обеспечения.	- правилами разработки внутренних правил, методик и регламентов проведения работ; - инструментами и методами информационной безопасности	Практическое задание

2.2.Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением семинаров, оцениванием контрольных заданий, проверкой конспектов лекций, выполнением индивидуальных и творческих заданий, периодическим опросом обучающихся на занятиях. Контролируемые разделы (темы) дисциплины, компетенции и оценочные средства представлены в таблице.

№ п/п	Контролируемые разделы	Код контролируемой компетенции	Наименование оценочного средства

1	Комплексная безопасность информационных систем	ОК-1, ОК-8, ОПК-3, ОПК- 6, ПК-7, ПК-11	Конспект, Фронтальный опрос, практическая задача
2	Методы обеспечения безопасности	ОК-1, ОК-8, ОПК-3, ОПК- 6, ПК-7, ПК-11	Конспект, практическая задача

Критерии и шкала оценивания конспекта

Оценка		*Критерий оценки*
«зачтено»	«отлично»	Конспект не превышает 1/8 от исходного текста, материал ясно и четко структурирован, содержательно точен, для облегчения восприятия материала студентом самостоятельно составлены схемы, таблицы.
	«хорошо»	Конспект превышает 1/8, но не превышает 1/4 от исходного текста, материал ясно и четко структурирован, содержательно точен.
	«удовлетворительно»	Конспект превышает 1/4, но не превышает 1/2 от исходного текста, материал слабо структурирован, содержательно точен.
«не зачтено»	«неудовлетворительно»	Вопрос раскрыт не достаточно, нет ясности, четкости в изложении, текст переписан без анализа. Конспект превышает 1/2 от исходного текста или содержательно не точен, или скопирован у третьих лиц.

Критерии и шкала оценивания практических задач

Оценка		*Критерий оценки*
«зачтено»	«отлично»	Студент защищает, выполненное задание, отвечая на вопросы преподавателя. Работа выполнена верно с первого раза на занятии по расписанию или работа выполнена верно с первого раза (если студент отсутствует на занятии по уважительной причине); ответы на вопросы преподавателя четко сформулированы, содержательно точны.
	«хорошо»	Работа выполнена верно с первого раза, но содержит недочеты или работа выполнена верно, но время выполнения превысило отведенное на практическом занятии или работа представлена повторно после исправления ошибок; ответы на вопросы преподавателя четко сформулированы, содержательно точны или содержат не более двух недочетов.

	«удовлетворительно»	Работа выполнена частично или сдается в третий раз и более; ответы на вопросы преподавателя содержат не более трех недочетов.
«не зачтено»	«неудовлетворительно»	Задача не решена или решена со значительными замечаниями. Задание не выполнено или задание выполнено, но студент не может ответить более чем 2/3 вопросов; или скопировано у третьих лиц.

Критерии и шкала оценивания фронтального опроса

Оценка		*Критерий оценки*
«зачтено»	«отлично»	Студент правильно отвечает более чем на 80 % вопросов;
	«хорошо»	Студент правильно отвечает на 70-80 % вопросов;
	«удовлетворительно»	Студент правильно отвечает на 60-70 % вопросов.
«не зачтено»	«неудовлетворительно»	Студент правильно отвечает менее чем на 60 % вопросов;

2.3. Критерии и шкалы оценивания результатов обучения при проведении промежуточной аттестации

Промежуточный контроль в соответствии с учебным планом направления подготовки – экзамен. Основой для определения оценки на зачете и экзамене служит объем и уровень усвоения материала, предусмотренного определенной темой, который должен позволить студенту выполнить практическое задание. Время на выполнение практического задания – 60-90 мин (в зависимости от задания). Форма экзамена – защита выполненного практического задания и ответ на дополнительные вопросы. Количество дополнительных вопросов зависит от правильности и четкости изложения студентом материала, а также работы в течение семестра. Дополнительные вопросы задаются в пределах тем практического задания, если в ходе семестра студент выполнил и защитил все задания, и в рамках курса, в противном случае. Время защиты практического задания, включая ответы на дополнительные вопросы не должно превышать 10 минут.

Порядок проведения экзамена:

а) очередность прибытия студентов на зачет и экзамен определяют преподаватель и староста учебной группы (в случае деления группы на подгруппы);

б) студент, войдя в аудиторию, предъявляет преподавателю зачетную книжку, получает практическое задание и теоретический вопрос согласно последней цифре номера его зачетной книжки и выполняет задание;

в) после подготовки студент докладывает о готовности продемонстрировать выполненное задание, защищает практическое задание и отвечает на поставленные вопросы.

Шкала оценивания		Критерии оценивания	Уровень освоения компетенций
«зачтено»	«отлично»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Ответил на все дополнительные вопросы. Практическое задание сделано правильно, студент уверенно дает ответы на вопросы преподавателя в ходе защиты практического задания.	Эталонный
	«хорошо»	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания, даны ответы на вопросы преподавателя в ходе защиты практического задания. Ответил на большинство дополнительных вопросов.	Стандартный
	«удовлетворительно»	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Допустил много неточностей при ответе на дополнительные вопросы.	Пороговый
«не зачтено»	«неудовлетворительно»	Выполнено менее 2/3 практического задания. Студент испытывает затруднения при ответе на вопросы преподавателя.	Компетенции не сформированы

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,

характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1. Оценочные средства текущего контроля успеваемости

Раздел 1 Основы информационной безопасности

Темы материалов, подлежащих конспектированию

1. Основы обеспечения комплексной защиты конфиденциальной информации
2. Актуальность проблем информационной безопасности

Фронтальный опрос №1

1. Дайте определение риска, опасности, безопасности.
2. В чем состоит механизм обеспечения безопасности
3. Приведите определение информационной безопасности
4. Прокомментируйте классификационную схема понятий в области «Защиты информации»
5. Какие виды защиты информации Вам известны
6. Как увязано применение отдельных видов защиты с комплексным обеспечением информационной безопасности

Фронтальный опрос №2

1. В чем состоит актуальность проблем информационной безопасности
2. Прокомментируйте динамика числа зарегистрированных утечек информации в мире
3. Каково распределение утечек по странам и по виновнику
4. Каково распределение утечек по типам данных и по каналам
5. В чем состоят основные нарушения и тенденции в сфере ИБ
6. Угрозы информационной безопасности
7. Приведите примеры реализации угрозы нарушения конфиденциальности
8. Приведите примеры реализации угрозы нарушения целостности данных
9. Вредоносное программное обеспечение
10. Приведите примеры реализации угрозы отказа в доступе

Практическая задача №1

Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение. Для этого:

- просмотреть предварительно созданный с помощью редактора свой текстовый файл;

- выполнить для этого файла шифрование;

- просмотреть в редакторе зашифрованный файл; - просмотреть гистограммы исходного и зашифрованного текстов, - описать гистограммы (в чем похожи, чем отличаются) и определить, с каким смещением было выполнено шифрование;

- расшифровать зашифрованный текст:

1) с помощью программы, после чего проверить в редакторе правильность расшифрования;

2) вручную с помощью гистограмм;

описать и объяснить процесс дешифрования.

Для одноалфавитного метода с задаваемым смещением (шифр Цезаря):

- для своего исходного текста выполнить шифрование с произвольным смещением;

- просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;

- расшифровать текст с помощью программы;

- имеется зашифрованный шифром Цезаря текст; дешифровать его с помощью программы методом подбора смещения;

-указать, с каким смещением был зашифрован файл.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, описываются полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования. Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы.

Практическая задача №2

Для метода перестановки символов дешифровать зашифрованный файл.

Для этого необходимо определить закон перестановки символов открытого текста. Создайте небольшой файл длиной в несколько слов с известным вам текстом, зашифруйте его, просмотрите гистограммы (опишите их; ответьте, можно ли извлечь из них полезную для дешифрации информацию). Сравните (с помощью редактора) ваш исходный и зашифрованный тексты и определите закон перестановки символов.

Дешифруйте файл:

1) вручную (объясните ваши действия);

2) с помощью программы.

Для инверсного кодирования (по дополнению до 255): - для своего произвольного файла выполните шифрование; - просмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов; - дешифруйте зашифрованный текст,

проверьте в редакторе правильность дешифрования.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, описываются полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования. Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы

Раздел 2 Нормативно-правовое поле информационной безопасности

Темы материалов, подлежащих конспектированию

1. Классические криптоалгоритмы подстановки и перестановки
2. Стандарт симметричного шифрования AES RIJNDAEL
3. Изучение программных продуктов защиты информации. Программа PGP
4. Защита программного обеспечения методами стеганографии

Практическая задача №3

Для многоалфавитного шифрования с фиксированным ключом определите, сколько одноалфавитных методов и с каким смещением используется в программе. Для этого нужно создать свой файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещений.

Для многоалфавитного шифрования с ключом фиксированной длины:

- для файла, состоящего из строки одинаковых символов выполнить шифрование и определить по гистограмме, какое смещение получает каждый символ;
- для файла произвольного текста произвести шифрование и расшифрование;
- просмотреть и описать гистограммы исходного и зашифрованного текстов; ответить, какую информацию можно получить из гистограмм.

Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично предыдущему пункту.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, описываются полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования. Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы

Практическая задача №4

1. Выполнить настройку программы: выбрать метод шифрования; ввести ключи для всех методов; ввести вероятное слово; осуществить все остальные системные настройки.

2. Для метода замены (одноалфавитного метода):

- ✓ выбрать данный алгоритм в списке доступных методов шифрования;
- ✓ установить необходимое смещение;
- ✓ открыть произвольный файл;
- ✓ просмотреть содержимое исходного файла;
- ✓ выполнить для этого файла шифрование (при необходимости можнозадать имя зашифрованного файла);
- ✓ просмотреть в редакторе зашифрованный файл;
- ✓ ввести вероятное слово;
- ✓ ввести вероятную длину ключа (кроме метода замены);
- ✓ подобрать ключ;
- ✓ выполнить расшифрование со всеми найденными ключами;
- ✓ найти в каком-либо из расшифрованных файлов правильно
- ✓ расшифрованное ключевое слово;
- ✓ расшифровать файл исходным ключом;
- ✓ проверить результат

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, указываются исходные и найденные ключи, описывается процесс дешифрования. Преподавателю предоставляется отчет о проделанной работе и все использованные файлы.

Практическая задача №5

Для метода перестановки:

- ✓ выбрать метод перестановки;
- ✓ в открывшемся окне ввода ключа перестановки символов указать
- ✓ сначала длину этого ключа, а затем из появившихся кнопок составить необходимую комбинацию для ключа, нажимая на кнопки в заданном порядке;
- ✓ при этом уже использованные кнопки становятся недоступными для предотвращения их повторного ввода; далее действия полностью соответствуют изложенным в предыдущем пункте задания.

Для метода гаммирования:

- ✓ выбрать метод гаммирования;
- ✓ ввести ключ гаммирования
- ✓ полностью повторить п. 3.

. Для таблицы Виженера все действия повторяются из п. 5 (метод гаммирования).

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, указываются исходные и найденные ключи, описывается процесс дешифрования. Преподавателю предоставляется отчет о проделанной работе и все использованные файлы.

Практическая задача №6

Заполнить таблицу «Перечень видов тайн», рассмотрев не менее 30 видов тайн. Дополнить таблицу описанием сфер деятельности, в которых пользователь может столкнуться с тем или другим видом тайны.

Перечень видов тайн (информация ограниченного доступа)

№	Сведения	Ссылка на НПА		Термин / Комментарии
		Основание	Наказание за разглашение	
1.	Государственная тайна	Конституция РФ ст.29 п.4 ФЗ №5485-1 ст.5 УП №1203 149-ФЗ ст.9 п.3	УК РФ ст.275, 276, 283, 283.1, 284 ТК РФ ст.81 6)в) (разглашение охраняемой законом тайны) ТК РФ ст.243 7) (случаи полной материальной ответственности) КоАП ст.13.12 п.7 (нарушение правил защиты информации)	***«Государственная тайна*** *- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.» - ФЗ №5485-1* Общий перечень сведений представлен в «ФЗ о ГТ», детализированный представлен в перечне, утвержденном Указом Президента РФ
2.	Коммерческая тайна	98-ФЗ ГК РФ IV ст.1465	УК РФ ст.183 УК РФ ст.147	98-ФЗ «… режим КТ в отношении информации, составляющей секрет производства (ноу-хау)»

Практическая задача №7

1. Ознакомиться с основными направлениями работ в рамках федеральной целевой программы “Электронная Россия”, а также со сведениями о порядке использования и действующих алгоритмах постановки электронной цифровой. Запустить программу labWork6.exe, предназначенную для демонстрации порядка постановки и проверки электронной цифровой подписи.

2. Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования набирается непосредственно в окне программы.

3. Зашифровать исходное сообщение и подписать его на секретном ключе отправителя.

4. Переслать зашифрованное и подписанное сообщение получателю. Выполнить проверку правильности ЭЦП и восстановить исходный текст сообщения.

5. Сохранить в отчете экранные формы, демонстрирующие процесс генерации и распространения ключей; процесс шифрования исходного документа и постановки ЭЦП.

6. Привести в отчете ответы на контрольные вопросы:

1) В чем состоит назначение хэш-функций и какие требования предъявляются к хэш-функциям, используемым для постановки ЭЦП? Перечислите стандарты хэш-функций, действующие в Российской федерации.

2)Опишите процедуры постановки и проверки ЭЦП. Какая информация содержится в ЭЦП?

3) Перечислите стандарты ЭЦП, действующие в Российской федерации. На каких принципах основанакриптостойкость современных алгоритмов ЭЦП?

4) Приведите пример реализации алгоритма ЭЦП (RSA, El-Gamal, DSA)

Практическая задача №8

Для выполнения лабораторной работы на компьютере необходимо установить программный модуль XY-Mover.

2. Выполнить начальные установки шифратора, согласно примеру.

3. Загрузить файл для шифрования.

4. Произвести шифрование информации с использованием шифра скользящей перестановки, сохранить шифртекст в файле.

5. Описать в отчете процесс шифрования и расшифрования данных с использованием программы-эмулятора XY-Mover. Проанализировать полученные данные.

6. Привести в отчете ответы на контрольные вопросы:

1) Почему шифрование методом гаммирования является наиболее подходящим для высокоскоростных линий телекоммуникационной связи?

2) Какие общие требования, предъявляются к гамме шифра?

3)Приведите пример, поясняющий работу шифрующего автомата скользящей перестановки при n=5, n1=2, n2=3.

4) Кратко опишите работу схемы реализации шифра скользящей перестановки.

Практическая задача №9

Используя положения НМД по вопросам защиты персональных данных, решите следующие задачи и обоснуйте ответ, ссылаясь на норму закона.

1) При проведении проверки первичной документации по учёту труда и его оплаты было обнаружено, что в личном деле одного из референтов федерального агентства отсутствуют сведения из налоговой службы об имущественном положении, а также данные дактилоскопической регистрации. Инспектор труда потребовал предъявить указанные документы.Правомерны ли требования инспектора труда?

2) Семенов обратился в ОАО «Решение» с просьбой принять его на работу в качестве ведущего специалиста отдела продаж. Начальник кадровой службы направил запрос в психоневрологический диспансер по месту жительства Семенова, в котором просил сообщить сведения о состоянии психологического здоровья и о фактах обращения Семенова за психиатрической помо-

щью, поскольку организации необходимо решить вопрос о пригодности Семенова для выполнения работы.Законны ли действия начальника кадровой службы?

3) Начальник отдела кадров Дубовцева распространяла среди своих знакомых сведения об образовании и данные медицинского осмотра заведующего складом Мамонтова, которые, по её мнению, порочили его честь и достоинство. Мамонтов потребовал от директора организации защитить его персональные данные от неправомерного использования и привлечь Дубовцеву к административной ответственности. Директор оштрафовал Дубовцеву на сумму, равную трем минимальным размера оплаты труда.

Законно ли действие работодателя? Какие виды юридической ответственности установлены законодательством России за нарушение норм, регулирующих сбор, обработку, хранение, распространение и защиту персональных данных работника.

4) Работник Падерин, ознакомившись со своими персональными данными, хранящимися в организации, потребовал от директора ООО «Аквамарин» исключить устаревшие и исправить неверные, а также известить всех лиц которым они ранее были сообщены, обо всех исправлениях или дополнениях. Директор не выполнил требования работника.

Правомерен ли отказ директора? Какие права по защите своих персональных данных, хранящихся у работодателя, закон предоставляет работнику?

5)Перевалов обратился в центр занятости по месту жительства в целях поиска подходящей работы. Инспектор центра занятости потребовал от гражданина предоставить сведения о последнем месте работы, о составе его семьи, его религиозных убеждениях и принадлежности к политическим партиям. Считая такие требования незаконными, Перевалов обратился с жалобой к руководителю центра занятости.

Законны ли требования инспектора. Какое решение по жалобе должен принять руководитель центра занятости?

3.2. Оценочные средства промежуточной аттестации

Перечень теоретических вопросов для экзамена:

1. Понятие риска, опасности, безопасности. Механизм обеспечения безопасности
2. Понятие информационной безопасности
3. Классификационная схема понятий в области «Защита информации»
4. Виды защиты информации
5. Актуальность проблем информационной безопасности

6. Статистика информационных утечек
7. Основные нарушения и тенденции в сфере ИБ
8. Угрозы информационной безопасности
9. Примеры реализации угрозы нарушения конфиденциальности
10. Примеры реализации угрозы нарушения целостности данных
11. Вредоносное программное обеспечение
12. Примеры реализации угрозы отказа в доступе
13. Понятие атаки на информационную систему. Виды атак
14. Классификация сетевых атак
15. Пассивная и активная атака
16. Отказ в обслуживании (DoS-атака)
17. Повторное использование (replay-атаки)
18. Модификация потока данных (атака "man in the middle")
19. Подходы к обеспечению информационной безопасности
20. Принципы обеспечения информационной безопасности
21. Средства защиты информационных систем
22. Методы обеспечения ИБ
23. Использование классических криптоалгоритмов подстановки для защиты текстовой информации
24. Использование классических криптоалгоритмов перестановки для защиты текстовой информации
25. Методы защиты текстовой информации
26. Оценка стойкости методов защиты текстовой информации на основе подбора.
27. Стандарт симметричного шифрования AES RIJNDAEL.
28. Программные продукты для защиты информации.
29. Осовной функционал и назначение программы PGP .
30. Защита программного обеспечения методами стеганографии
31. Защита электронных документов с использованием цифровых водяных знаков.
32. Стегокомплексы, допускающие использование аудиоконтейнеров

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

4.1. Описание процедур проведения текущего контроля успеваемости студентов

В таблице представлено описание процедур проведения контрольно-оценочных мероприятий текущего контроля успеваемости студентов, в соответствии с рабочей программой дисциплины, и процедур оценивания результатов обучения с помощью спланированных оценочных средств.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Конспект	Конспект не подменяется планами работ или полностью переписанным текстом. Цель конспекта – студент должен научиться отбирать основное. Конспект может быть выполнен от руки или на компьютере. В конце конспекта обязательно указывается источник. Качество конспекта оценивается с учетом труда, вложенного в подготовку.
Фронтальный опрос	На вопросы преподавателя по сравнительно небольшому объему материала краткие ответы (как правило, с места) дают многие учащиеся. Этот вид опроса учащихся удачно сочетается с задачами повторения и закрепления пройденного материала, при умелом его использовании за сравнительно небольшое время позволяет осуществить проверку знаний у значительной части учащихся.
Практическая задача	Средство контроля, которое включает в себя описание условия задачи без необходимых указаний, что делать. Практическая работа может быть связана с заданием на компьютере, может быть дано задание построения схемы, таблицы, написания программы и т.д. Студент защищает, выполненное задание, отвечая на вопросы преподавателя.

Методика оценки деятельности студента

Номер раздела	Процедура оценивания	Оценка	
		min	max
1	Конспект	Не зачтено	Зачтено
	Практическая задача№ 1,2	Не зачтено	Зачтено
	Фронтальный опрос №1,2,3	Не зачтено	Зачтено
2	Практическая задача№ 3,4,5,6,7,8,9	Не зачтено	Зачтено
	Конспект	Не зачтено	Зачтено

4.2. Описание процедур проведения промежуточной аттестации Экзамен

При определении уровня достижений обучающих на экзамене обращается особое внимание на следующее:

- дан полный, развернутый ответ на поставленный вопрос;
- показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные признаки, причинно-следственные связи;
- знание об объекте демонстрируются на фоне понимания его в системе данной дисциплины и междисциплинарных связей;
- ответ формулируется в терминах дисциплины, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию обучающегося;
- теоретические постулаты подтверждаются примерами из практики.