

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Комарова Светлана Юриевна

Должность: Проректор по образовательной деятельности

Дата подписания: 18.05.2023 12:45:40

Уникальный программный ключ:

43ba42f5deae4116bbfcb9ac98e39108031227e81add207cbee4149f2098d7a

**Федеральное государственное бюджетное образовательное учреждение
высшего образования**

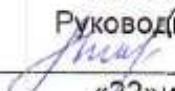
«Омский государственный аграрный университет имени П.А. Столыпина»

Экономический факультет

**ОПОП по направлению подготовки
09.04.02 Информационные системы и технологии**

СОГЛАСОВАНО

Руководитель ОПОП

 Н.В. Манюкова

«22» июня 2022 г.

УТВЕРЖДАЮ

Декан

 И.А. Волкова

«22» июня 2022 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

Б1.В.ДВ.01.01 Криптографические методы защиты информации

Направленность (профиль)

«Информационные системы и технологии»

Обеспечивающая преподавание дисциплины
кафедра –

Экономики, бухгалтерского учета и
финансового контроля

Разработчик РП:

канд. экон. наук, доцент



А.А. Ремизова

Внутренние эксперты:

Председатель МК,

канд. экон. наук



С.А. Нардина

Начальник управления информационных
технологий



П.И. Ревякин

Заведующий методическим отделом УМУ



Г.А. Горелкина

Директор НСХБ



И.М. Демчукова

Омск 2022

1. ОСНОВАНИЯ ДЛЯ ВВЕДЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ, ЕЕ СТАТУС

1.1. Основания для введения дисциплины в учебный план:

- Федеральный государственный образовательный стандарт высшего образования – магистратура по направлению подготовки 09.04.02 Информационные системы и технологии, утверждённый приказом Министерства образования и науки от 19.09.2017 № 917 (с изменениями и дополнениями);
- основная профессиональная образовательная программа подготовки магистров, по направлению подготовки 09.04.02 Информационные системы и технологии, направленность (профиль) Информационные системы и технологии в бизнесе.

1.2. Статус дисциплины в учебном плане:

- относится формируемой участниками образовательных отношений части блока 1 «Дисциплины» ОПОП;
- является дисциплиной обязательной для изучения, если выбрана обучающимся.

1.3. В рабочую программу дисциплины в установленном порядке могут быть внесены изменения и дополнения, осуществляемые в рамках планового ежегодного и ситуативного совершенствования, которые отражаются в п. 9 рабочей программы.

2. ЦЕЛЕВАЯ НАПРАВЛЕННОСТЬ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ. ЛОГИЧЕСКИЕ И СОДЕРЖАТЕЛЬНО-МЕТОДИЧЕСКИЕ ВЗАИМОСВЯЗИ ДИСЦИПЛИНЫ С ДРУГИМИ ДИСЦИПЛИНАМИ И ПРАКТИКАМИ В СОСТАВЕ ОПОП

2.1. Процесс изучения дисциплины в целом направлен на подготовку обучающихся к решению задач профессиональной деятельности следующих типов: научно-исследовательский, предусмотренных федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки, а также ОПОП ВО университета, в рамках которой преподаётся данная дисциплина.

Цель дисциплины: овладение основами теоретических и практических знаний, а также выработка компетенций в области криптографической защиты информации в организациях.

2.2. Перечень компетенций формируемых в результате освоения учебной дисциплины:

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

Компетенции, в формировании которых задействована дисциплина		Код и наименование индикатора достижений компетенции	Компоненты компетенций, формируемые в рамках данной дисциплины (как ожидаемый результат ее освоения)		
код	наименование		знать и понимать	уметь делать (действовать)	владеть навыками (иметь навыки)
Профессиональные компетенции					
ПК-1	Способен разрабатывать и исследовать модели объектов профессиональной деятельности, предлагать и адаптировать методики, определять качество проводимых исследований, составлять отчеты о проделанной работе, обзоры, готовить публикации	ИД-1 _{пк-1.1} Понимает принципы, методы и знает средства анализа и структурирования профессиональной информации; методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации; методы исследований; принципы построения математических моделей процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений	основные принципы, методы и средства криптографической защиты информации в организации; основные понятия и требования криптографической защиты информации; принципы построения математических моделей процессов и объектов; модели шифров и математические методы их исследования	выбирать основные принципы, методы и средства криптографической защиты информации в организации; выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации; выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации;	применения основных принципов, методов и средств криптографической защиты информации в организации; применения принципов построения математических моделей процессов и объектов определения криптографической стойкости шифрсистем; навыками обоснования выбора криптографических средств для защиты информации
		ИД-2 _{пк-2.2} Анализирует профессиональную информацию, выделяет в ней главное, структурирует, оформляет и представляет в виде аналитических обзоров; применяет на практике новые научные принципы и методы исследований; разрабатывает и применяет математические модели процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений	аспекты анализа профессиональной информации; новые научные принципы и методы исследований; математические модели процессов и объектов при решении задач криптографической защиты информации	анализировать профессиональную информацию; применять на практике новые научные принципы и методы исследований; разрабатывать и применять математические модели процессов и объектов при решении задач криптографической защиты информации	всестороннего анализа профессиональной информации; применения на практике новых научных принципов и методов исследований; разработки и применения математического моделирования в криптографии

2.3. Описание показателей, критериев и шкал оценивания в рамках дисциплины

Индекс и название компетенции	Код индикатора достижений компетенции	Индикаторы компетенции	Показатель оценивания – знания, умения, навыки (владения)	Уровни сформированности компетенций				Формы и средства контроля формирования компетенций
				компетенция не сформирована	минимальный	средний	высокий	
				Оценки сформированности компетенций				
				2	3	4	5	
				Оценка «неудовлетворительно»	Оценка «удовлетворительно»	Оценка «хорошо»	Оценка «отлично»	
				Характеристика сформированности компетенции				
				Компетенция в полной мере не сформирована. Имеющихся знаний, умений и навыков недостаточно для решения практических (профессиональных) задач	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач	Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач	
Критерии оценивания								
ПК-1 Способен разрабатывать и исследовать модели объектов профессиональной деятельности, предлагать и адаптировать методики, определять качество проводимых исследований, составлять отчеты о проделанной работе, обзоры, готовить публикации	ИД-1 _{ПК.1} Понимает принципы, методы и средства анализа и структурирования профессиональной информации; методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации; методы исследований; принципы построения математических моделей процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений	Полнота знаний	Основные принципы, методы и средства криптографической защиты информации в организации; основные понятия и требования криптографической защиты информации; принципы построения математических моделей процессов и объектов; модели шифров и математические методы их исследования	Не знает основные принципы, методы и средства криптографической защиты информации в организации; основные понятия и требования криптографической защиты информации; принципы построения математических моделей процессов и объектов; модели шифров и математические методы их исследования	Имеет поверхностное представление о принципах, методах и средствах криптографической защиты информации в организации; об основных понятиях и требованиях криптографической защиты информации; принципах построения математических моделей процессов и объектов; моделях шифров и математических методах их исследования	Знает основные принципы, методы и средства криптографической защиты информации в организации; основные понятия и требования криптографической защиты информации; принципы построения математических моделей процессов и объектов; модели шифров и математические методы их исследования	Знает и понимает ключевые принципы, методы и средства криптографической защиты информации в организации; основные понятия и требования криптографической защиты информации; принципы построения математических моделей процессов и объектов; модели шифров и математические методы их исследования	Оценка ответов на практических занятиях; оценка выполненных заданий на практических занятиях; опрос по самостоятельным темам; проверка выполненной электронной презентации; тестирование
		Наличие умений	Выбирать основные принципы, методы и средства криптографической защиты информации в организации; выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации; выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации	Не умеет выбирать основные принципы, методы и средства криптографической защиты информации в организации; выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации; выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации	Умеет выбирать некоторые принципы, методы и средства криптографической защиты информации в организации; выявлять специфику некоторых криптографических угроз информационной безопасности по ряду категорий информации; с трудом выделяет основания и объекты защиты информации, определяет основания и процедуру осуществления криптографической защиты информации	Умеет выбирать основные принципы, методы и средства криптографической защиты информации в организации; выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации; выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации	В совершенстве умеет выбирать основные принципы, методы и средства криптографической защиты информации в организации; выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации; выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации	
		Наличие навыков	Применения основных принципов, методов и	Отсутствуют навыки применения основных	Поверхностно владеет навыками применения	Владеет основными навыками применения	Свободно владеет навыками применения основных	

		(владение опытом)	средств криптографии-ческой защиты информации в организации; применения принципов построения математических моделей процессов и объектов определения криптографической стойкости шифрсистем; навыками обоснования выбора криптографических средств для защиты информации	принципов, методов и средств криптографии-ческой защиты информации в организации; применения принципов построения математических моделей процессов и объектов определения криптографической стойкости шифрсистем; навыками обоснования выбора криптографических средств для защиты информации	основных принципов, методов и средств криптографии-ческой защиты информации в организации; применения принципов построения математических моделей процессов и объектов определения криптографической стойкости шифрсистем; навыками обоснования выбора криптографических средств для защиты информации	основных принципов, методов и средств криптографии-ческой защиты информации в организации; применения принципов построения математических моделей процессов и объектов определения криптографической стойкости шифрсистем; навыками обоснования выбора криптографических средств для защиты информации	принципов, методов и средств криптографии-ческой защиты информации в организации; применения принципов построения математических моделей процессов и объектов определения криптографической стойкости шифрсистем; навыками обоснования выбора криптографических средств для защиты информации	
	ИД-2пк.2.2. Анализировать профессиональную информацию, выделяет в ней главное, структурирует, оформляет и представляет в виде аналитических обзоров; применяет на практике новые научные принципы и методы исследований; разрабатывает и применяет математические модели процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений	Полнота знаний	Аспекты анализа профессиональной информации; новые научные принципы и методы исследований; математические модели процессов и объектов при решении задач криптографической защиты информации	Не знает аспекты анализа профессиональной информации; новые научные принципы и методы исследований; математические модели процессов и объектов при решении задач криптографической защиты информации	Имеет поверхностное представление об аспектах анализа профессиональной информации; новых научных принципах и методах исследований; математических моделях процессов и объектов при решении задач криптографической защиты информации	Знает основные аспекты анализа профессиональной информации; новые научные принципы и методы исследований; математические модели процессов и объектов при решении задач криптографической защиты информации	Знает и понимает ключевые аспекты анализа профессиональной информации; новые научные принципы и методы исследований; математические модели процессов и объектов при решении задач криптографической защиты информации	Оценка ответов на практических занятиях; оценка выполненных заданий на практических занятиях; опрос по самостоятельному изученным темам; проверка выполненной электронной презентации; тестирование
		Наличие умений	Анализировать профессиональную информацию; применять на практике новые научные принципы и методы исследований; разрабатывать и применять математические модели процессов и объектов при решении задач криптографической защиты информации	Не умеет анализировать профессиональную информацию; применять на практике новые научные принципы и методы исследований; разрабатывать и применять математические модели процессов и объектов при решении задач криптографической защиты информации	Умеет анализировать некоторую профессиональную информацию; применять на практике некоторые научные принципы и методы исследований; разрабатывать и применять некоторые математические модели процессов и объектов при решении задач криптографической защиты информации	Умеет анализировать профессиональную информацию; применять на практике научные принципы и методы исследований; разрабатывать и применять основные математические модели процессов и объектов при решении задач криптографической защиты информации	В совершенстве умеет анализировать профессиональную информацию; применять на практике новые научные принципы и методы исследований; разрабатывать и применять математические модели процессов и объектов при решении задач криптографической защиты информации	
		Наличие навыков (владение опытом)	Всестороннего анализа профессиональной информации; применения на практике новых научных принципов и методов исследований; разработки и применения математического моделирования в криптографии	Отсутствуют навыки всестороннего анализа профессиональной информации; применения на практике новых научных принципов и методов исследований; разработки и применения математического моделирования в криптографии	Поверхностно владеет навыками всестороннего анализа профессиональной информации; применения на практике новых научных принципов и методов исследований; разработки и применения математического моделирования в криптографии	Владеет основными навыками всестороннего анализа профессиональной информации; применения на практике новых научных принципов и методов исследований; разработки и применения математического моделирования в криптографии	Свободно владеет основными навыками всестороннего анализа профессиональной информации; применения на практике новых научных принципов и методов исследований; разработки и применения математического моделирования в криптографии	

2.4. Логические и содержательные взаимосвязи дисциплины с другими дисциплинами и практиками в составе ОПОП

Дисциплины, практики*, на которые опирается содержание данной дисциплины		Индекс и наименование дисциплин, практик, для которых содержание данной дисциплины выступает основой	Индекс и наименование дисциплин, практик, с которыми данная дисциплина осваивается параллельно в ходе одного семестра
Индекс и наименование	Перечень требований, сформированных в ходе изучения предшествующих		
Б1.В.06 Информационная структура современных предприятий Б1.В.01 Надежность информационных систем	Знает: основы теории информационной структуры предприятий, виды информационных процессов и технологий на предприятии;; основные понятия и принципы надежности информационных систем; базовые и прикладные программные средства информационных систем. Умеет: анализировать задачу, выделяя ее базовые составляющие; выбирать и использовать соответствующий программный продукт в информационной системе современного предприятия; использовать современные информационные технологии и программные средства надежности информационных систем. Владеет навыками: приемами работы с информационно-поисковыми системами, сетевыми технологиями, базами данных и пр.; навыками анализа информационных структур современного предприятия; навыками анализа и оценки надежности информационных систем современного предприятия	Б2.О.03(П) Производственная. Технологическая (проектно-технологическая) практика	Б1.О.10 Модели и методы проектирования информационных систем Б1.В.04 Организация работы ИТ-подразделения предприятия Б1.В.07 Реинжиниринг бизнес-процессов

* - для некоторых дисциплин первого года обучения целесообразно указать на взаимосвязь с предшествующей подготовкой обучающихся в старшей школе

2.5 Формы методических взаимосвязей дисциплины с другими дисциплинами и практиками в составе ОПОП

В рамках методической работы применяются следующие формы методических взаимосвязей:

- учёт содержания предшествующих дисциплин при формировании рабочей программы последующей дисциплины;
- согласование рабочей программы предшествующей дисциплины ведущим преподавателем последующей дисциплины;
- совместное обсуждение ведущими преподавателями предшествующей и последующей дисциплин результатов входного тестирования по последующей дисциплине;
- участие ведущего преподавателя последующей дисциплины в процедуре приёма зачета по предыдущей.

2.6 Социально-воспитательный компонент дисциплины

В условиях созданной вузом социокультурной среды в результате изучения дисциплины: формируются мировоззрение и ценностные ориентации обучающихся; интеллектуальные умения, научное мышление; способность использовать полученные ранее знания, умения, навыки, развитие творческих начал.

Воспитательные задачи реализуются в процессе общения преподавателя с обучающимися, в использовании активных методов обучения, побуждающих обучающихся проявить себя в совместной деятельности, принять оценочное решение. Коллективные виды деятельности способствуют приобретению навыков работы в коллективе, умения управления коллективом. Самостоятельная

работа способствует выработке у обучающихся способности принимать решение и навыков самоконтроля.

Через связь с НИРС, осуществляемой во внеучебное время, социально-воспитательный компонент ориентирован на:

1) адаптацию и встраивание обучающихся в общественную жизнь ВУЗа, укрепление межличностных связей и уверенности в правильности выбранной профессии;

2) проведение систематической и целенаправленной профориентационной работы, формирование творческого, сознательного отношения к труду;

3) формирование общекультурных компетенций, укрепление личных и групповых ценностей, общественных ценностей, ценности непрерывного образования;

4) гражданско-правовое воспитание личности;

5) патриотическое воспитание обучающихся, формирование модели профессиональной этики, культуры экономического мышления, делового общения.

Объединение элементов образовательной и воспитательной составляющей дисциплины способствует формированию общекультурных компетенций выпускников, компетенций социального взаимодействия, самоорганизации и самоуправления, системно-деятельностного характера, создает условия, необходимые для всестороннего развития личности.

3. СТРУКТУРА И ТРУДОЕМКОСТЬ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина обучающимися очной формы обучения изучается в четвертом семестре второго курса; обучающимися заочной формы обучения – на втором курсе летняя сессия.

Очная форма обучения: продолжительность четвертого семестра 9 4/6 недель.

Заочная форма обучения: продолжительность обучения, включая зимнюю и летнюю сессии 19 и 13 недель соответственно.

Вид учебной работы	Трудоемкость, час		
	семестр, курс*		
	Очная форма	Заочная форма	
	4 семестр	2 курс (начитка)	2 курс
1. Аудиторные занятия, всего	36	2	12
– лекции	16	2	4
– практические занятия (включая семинары)	20	-	8
– лабораторные работы	-	-	-
2. Внеаудиторная академическая работа	72	34	56
2.1 Фиксированные виды внеаудиторных самостоятельных работ:	10	-	10
Выполнение и сдача/защита индивидуального/группового задания в виде**			
– презентации	10	-	10
2.2 Самостоятельное изучение тем/вопросов программы	30	34	30
2.3 Самоподготовка к аудиторным занятиям	20		10
2.4 Самоподготовка к участию и участие в контрольно-оценочных мероприятиях, проводимых в рамках текущего контроля освоения дисциплины (за исключением учтённых в пп. 2.1 – 2.2):	12		6
3. Получение дифференцированного зачёта по итогам освоения дисциплины	+	-	4
ОБЩАЯ трудоемкость дисциплины:	Часы	108	108
	Зачетные единицы	3	3
Примечание: * – семестр – для очной и очно-заочной формы обучения, курс – для заочной формы обучения; ** – КР/КП, реферата/эссе/презентации, контрольной работы (для обучающихся заочной формы обучения), расчетно-графической (расчетно-аналитической) работы и др.;			

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

4.1 Укрупненная содержательная структура дисциплины и общая схема ее реализации в учебном процессе

Номер и наименование раздела дисциплины. Укрупненные темы раздела		Трудоемкость раздела и ее распределение по видам учебной работы, час.						Формы текущего контроля успеваемости и промежуточной аттестации	№№ компетенций, на формирование которых ориентирован раздел	
		общая	Аудиторная работа				ВАРС			
			всего	лекции	занятия		всего			фиксированные виды
					практические (всех форм)	лабораторные				
Очная форма обучения										
1	Тема 1. Основные понятия.	16	4	2	2	-	12	10	Оценка ответов на практических занятиях; оценка выполненных заданий на практических занятиях; опрос по самостоятельно изученным темам; проверка выполненной электронной презентации; тестирование	ПК-1.1 ПК-1.2
	Тема 2. Основные характеристики шифров	16	4	2	2	-	12			
	Тема 3. Симметричная криптография	20	8	4	4	-	12			
	Тема 4. Криптография с открытым ключом	18	6	2	4	-	12			
	Тема 5. Электронная подпись	18	6	2	4	-	12			
	Тема 6. Применение криптографических методов и средств для обеспечения информационной безопасности	20	8	4	4	-	12			
	Промежуточная аттестация	-	×	×	×	×	×	×	Дифференцированный зачет	
Итого по дисциплине		108	36	16	20	-	72	10		

Номер и наименование раздела дисциплины. Укрупненные темы раздела		Трудоемкость раздела и ее распределение по видам учебной работы, час.						Формы текущего контроля успеваемости и промежуточной аттестации	№№ компетенций, на формирование которых ориентирован раздел	
		общая	Аудиторная работа				ВАРС			
			всего	лекции	занятия		всего			фиксированные виды
					практические (всех форм)	лабораторные				
Заочная форма обучения										
1	Тема 1. Основные понятия.	16	1	1	-	-	15	10	Оценка ответов на практических занятиях; оценка выполненных заданий на практических занятиях; опрос по самостоятельно изученным темам; проверка выполненной электронной презентации; тестирование	ПК-1.1 ПК-1.2
	Тема 2. Основные характеристики шифров	17	2	1	1	-	15			
	Тема 3. Симметричная криптография	18	3	1	2	-	15			
	Тема 4. Криптография с открытым ключом	18	3	1	2	-	15			
	Тема 5. Электронная подпись	18	3	1	2	-	15			
	Тема 6. Применение криптографических методов и средств для обеспечения информационной безопасности	17	2	1	1	-	15			
	Промежуточная аттестация	4	×	×	×	×	×	×	Дифференцированный зачет	
Итого по дисциплине		108	14	6	8	-	90	10	4	

4.2. Лекционный курс.
Примерный тематический план чтения лекций по разделам дисциплины

№		Тема лекции. Основные вопросы темы	Трудоемкость по разделу, час.		Применяемые интерактивные формы обучения
раздела	лекции		очная форма	заочная форма	
1	1	Тема 1. Основные понятия			
		1 Основные понятия.	2	1	Лекция-беседа
		2 Криптографическая система. Классификация шифров			
	2	Тема 2 Основные характеристики шифров			
		1 Алгебраическая модель шифра. Вероятностная модель шифра. Модели открытых текстов.	2	1	Лекция-беседа
		2 Криптографическая стойкость шифров. Атаки на шифры			
		3 Теоретическая и практическая стойкость шифра			
	4 Имитостойкость, помехоустойчивость шифров				
	3	Тема 3 Симметричная криптография			
		1 Блочные и поточные шифры	4	1	Лекция-беседа
		2 Принципы построения блочных шифров			
		3 Сеть Фейстеля. Шифр DES			
		4 Режимы работы блочных шифров.			
		5 Поточные шифры			
	6 Генераторы псевдослучайных последовательностей				
	4	Тема 4 Криптография с открытым ключом			
		1 Односторонние функции, функции с секретом	2	1	Лекция-беседа
		2 Схемы шифрования на основе односторонних функций			
	3 Схемы шифрования RSA и ЭльГамала				
	5	Тема 5 Электронная подпись			
		1 Понятие электронной подписи. Способы построения электронной подписи	2	1	-
		2 Эллиптические кривые.			
		3 Криптографическая хэш-функция			
	4 Конструкция хэш-функций.				
	6	Тема 6 Применение криптографических методов и средств для обеспечения информационной безопасности			
		1 Коды аутентификации сообщений	4	1	-
		2 Криптографические протоколы			
		3 Управление ключами			
		4 Инфраструктура открытых ключей			
		5 Принципы разработки и модернизации СКЗИ			
Общая трудоемкость лекционного курса					
Всего лекций по дисциплине:		час.	Из них в интерактивной форме:		час.
– очная форма обучения		16	– очная форма обучения		10
– заочная форма обучения		6	– заочная форма обучения		4
Примечания:					
– материально-техническое обеспечение лекционного курса – см. Приложение 6;					
– обеспечение лекционного курса учебной, учебно-методической литературой и иными библиотечно-информационными ресурсами и средствами обеспечения образовательного процесса – см. Приложения 1 и 2.					

4.3. Примерный тематический план практических занятий по разделам дисциплины

№		Тема занятия / Примерные вопросы на обсуждение (для семинарских занятий)	Трудоемкость по разделу, час.		Используемые интерактивные формы**	Связь занятия с ВАРС*
раздела (модуля)	занятия		очная форма	заочная форма		
1	1	Тема 1. Основные понятия				
		1 Основные понятия.	2	-	Семинар- беседа	ОСП
		2 Криптографическая система. Классификация шифров				
	2	Тема 2 Основные характеристики шифров				
		1 Алгебраическая модель шифра. Вероятностная модель шифра. Модели открытых текстов.	2	1	-	ОСП
		2 Криптографическая стойкость шифров. Атаки на шифры				
		3 Теоретическая и практическая стойкость шифра				
	4 Имитостойкость, помехоустойчивость шифров					
	3	Тема 3 Симметричная криптография				
		1 Блочные и поточные шифры	4	2	-	ОСП
		2 Принципы построения блочных шифров				
		3 Сеть Фейстеля. Шифр DES				
		4 Режимы работы блочных шифров.				
		5 Поточные шифры				
	6 Генераторы псевдослучайных последовательностей					
	4	Тема 4 Криптография с открытым ключом				
		1 Односторонние функции, функции с секретом	4	2	-	ОСП
		2 Схемы шифрования на основе односторонних функций				
	3 Схемы шифрования RSA и Эль-Гамала					
	5	Тема 5 Электронная подпись				
		1 Понятие электронной подписи. Способы построения электронной подписи	4	2	-	ОСП
		2 Эллиптические кривые.				
		3 Криптографическая хэш-функция				
	4 Конструкция хэш-функций.					
	6	Тема 6 Применение криптографических методов и средств для обеспечения информационной безопасности				
		1 Коды аутентификации сообщений	4	1	-	ОСП
		2 Криптографические протоколы				
		3 Управление ключами				
		4 Инфраструктура открытых ключей				
		5 Принципы разработки и модернизации СКЗИ				
Всего практических занятий по дисциплине:		час.	Из них в интерактивной форме:		час.	
– очная форма обучения		20	– очная форма обучения		2	
– заочная форма обучения		8	– заочная форма обучения		-	
В том числе в форме семинарских занятий						
– очная форма обучения						
– заочная форма обучения						
* Условные обозначения: ОСП – предусмотрена обязательная самоподготовка к занятию; УЗ СРС – на занятии выдается задание на конкретную ВАРС; ПР СРС – занятие содержательно базируется на результатах выполнения обучающимся конкретной ВАРС.						
** в т.ч. при использовании материалов МООК «Название», название ВУЗа-разработчика, название платформы и ссылка на курс (с указанием даты последнего обращения)						
Примечания: - материально-техническое обеспечение практических занятий – см. Приложение 6; - обеспечение практических занятий учебной, учебно-методической литературой и иными библиотечно-информационными ресурсами и средствами обеспечения образовательного процесса – см. Приложения 1 и 2.						

5. ПРОГРАММА ВНЕАУДИТОРНОЙ АКАДЕМИЧЕСКОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

5.1. Фиксированные виды внеаудиторных самостоятельных работ

5.1.1. Выполнение и защита (сдача) курсового проекта (работы) по дисциплине

Не предусмотрено учебным планом

5.1.2. Выполнение и сдача электронной презентации

5.1.2.1 Место электронной презентации в структуре учебной дисциплины

Разделы дисциплины, освоение которых обучающимися сопровождается или завершается выполнением электронной презентации		Компетенции, формирование/развитие которых обеспечивается в ходе выполнения электронной презентации
№	Наименование	
1	Тема 1. Основные понятия.	ПК-1.1 Понимает принципы, методы и знает средства анализа и структурирования профессиональной информации; методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации; методы исследований; принципы построения математических моделей процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений ПК-1.2 Анализирует профессиональную информацию, выделяет в ней главное, структурирует, оформляет и представляет в виде аналитических обзоров; применяет на практике новые научные принципы и методы исследований; разрабатывает и применяет математические модели процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений
	Тема 2 Основные характеристики шифров	
	Тема 3 Симметричная криптография	
	Тема 4 Криптография с открытым ключом	
	Тема 5 Электронная подпись	
	Тема 6 Применение криптографических методов и средств для обеспечения информационной безопасности	

5.1.2.2. Перечень примерных тем электронной презентации

Тема презентации выбирается студентами самостоятельно по согласованию с преподавателем. Материал подготавливается студентами на основе индивидуальной проработки рекомендованной преподавателем и самостоятельно подобранной основной и дополнительной учебной литературы по теме, ее анализа.

Примерные темы презентаций:

1. Определение шифра. Классификация шифров.
2. Понятие криптографической системы. Требования к криптографическим системам.
3. Формальные модели шифров. Алгебраическая и вероятностная модель шифра.
4. Математическая модель открытых текстов.
5. Алгебраическая модель шифра перестановки.
6. Алгебраическая модель шифра замены.
7. Алгебраическая модель шифра гаммирования.
8. Криптографическая стойкость шифра. Виды атак.
9. Практическая стойкость шифра.
10. Имитостойкость шифра.
11. Помехозащищенность шифра.
12. Методы криптоанализа.
13. Блочные шифры. Принципы построения.
14. Блочные шифры. DES. Функция шифрования, S-блоки.

15. Блочные шифры. ГОСТ 34.12-2018 и ГОСТ 34.13-2018.
16. Блочные шифры. AES.
17. Режимы использования блочных шифров. ECB
18. Режимы использования блочных шифров. CBC
19. Режимы использования блочных шифров. OFB
20. Режимы использования блочных шифров. CFB.
21. Комбинирование блочных шифров
22. Поточные шифры. Синхронные и самосинхронизирующиеся шифры
23. Поточные шифры. Принципы построения. Связь с режимами блочных шифров.
24. Поточные шифры. RC4.
25. Датчики истинно случайных последовательностей. Требования. Источники. Свойства.
26. Генераторы псевдослучайной последовательности. Методы усложнения.
27. Методы тестирования случайных последовательностей

5.1.2.3. Информационно-методические и материально-техническое обеспечение процесса выполнения электронной презентации

1. Материально-техническое обеспечение процесса выполнения электронной презентации – см. Приложение 6.

2. Обеспечение процесса выполнения электронной презентации учебной, учебно-методической литературой и иными библиотечно-информационными ресурсами и средствами обеспечения образовательного процесса – см. Приложение 1, 2, 3.

Шкала и критерии оценивания электронной презентации	
Отлично	Оценка «отлично» по презентации присваивается за глубокое раскрытие темы, качественное оформление работы, содержательность презентации, за понимание студентом отражённого в презентации материала.
Хорошо	Оценка «хорошо» по презентации присваивается при соответствии выше перечисленным критериям, но при наличии в содержании работы и ее оформлении небольших недочетов или недостатков в представлении результатов к защите
Удовлетворительно	Оценка «удовлетворительно» по презентации присваивается за неполное раскрытие темы, выводов и предложений, носящих общий характер, плохо подготовленное наглядное представление работы и затруднения при ответах на вопросы
Неудовлетворительно	Оценка «неудовлетворительно» по презентации присваивается за слабое и неполное раскрытие темы, несамостоятельность изложения материала, выводы и предложения, носящие общий характер, отсутствие наглядного представления работы и ответов на вопросы

5.1.3. Перечень заданий для контрольных работ обучающихся заочной формы обучения

не предусмотрено

5.2. Самостоятельное изучение тем

Номер раздела дисциплины	Тема в составе раздела/вопрос в составе темы раздела, вынесенные на самостоятельное изучение	Расчетная трудоемкость, час	Форма текущего контроля по теме
Очная форма обучения			
1	1.1 Основные понятия. 1.2 Классификация шифров	10	Опрос
	3.1 Блочные и поточные шифры 3.2 Принципы построения блочных шифров	10	Опрос
	5.1 Понятие электронной подписи. 5.2 Способы построения электронной подписи	10	Опрос
Заочная форма обучения			
1	1.1 Основные понятия. 1.2 Классификация шифров	10	Опрос
	2.1 Алгебраическая модель шифра. Вероятностная модель шифра. Модели открытых текстов	10	Опрос
	3.1 Блочные и поточные шифры 3.2 Принципы построения блочных шифров	10	Опрос
	4.2 Схемы шифрования на основе односторонних функций	10	Опрос
	5.1 Понятие электронной подписи. 5.2 Способы построения электронной подписи	10	Опрос
	6.1 Коды аутентификации сообщений 6.2 Криптографические протоколы 6.3 Управление ключами	14	Опрос
Примечание: - учебная, учебно-методическая литература и иные библиотечно-информационные ресурсы и средства обеспечения самостоятельного изучения тем – см. Приложения 1-4.			

Общий алгоритм самостоятельного изучения темы

- ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме;
- на этой основе составить развёрнутый план (конспект) изложения темы;
- подготовиться к опросу по теме.

Шкала и критерии оценивания опроса	
Зачтено	Оценка «зачтено» ставится, если обучающийся в процессе опроса использует научную терминологию, стилистическое и логическое изложение ответа на вопросы, умеет делать выводы без существенных ошибок; владеет инструментарием изучаемой дисциплины; умеет ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им оценку.
Не зачтено	Оценка «не зачтено» ставится, если обучающийся: имеет недостаточно полный объем знаний в рамках опрашиваемой темы по дисциплине; использует научную терминологию, но изложение ответа на вопросы осуществляется с существенными логическими ошибками; слабо владеет инструментарием в рамках темы; не умеет ориентироваться в основных теориях, концепциях и направлениях изучаемой темы.

5.3. Самоподготовка к аудиторным занятиям (кроме контрольных занятий)

Занятий, по которым предусмотрена самоподготовка	Характер (содержание) самоподготовки	Организационная основа самоподготовки	Общий алгоритм самоподготовки	Расчетная трудоемкость, час
Очная форма обучения				
Практические (семинарские) занятия	Подготовка по темам занятий	План занятий; Задания преподавателя, выдаваемые в конце предыдущего занятия	1. Рассмотрение вопросов занятия. 2. Изучение литературы по вопросам темы. 3. Выполнение задания	20
Заочная форма обучения				
Практические (семинарские) занятия	Подготовка по темам занятий	План занятий; Задания преподавателя, выдаваемые в конце предыдущего занятия	1. Рассмотрение вопросов занятия. 2. Изучение литературы по вопросам темы. 3. Выполнение задания	10

Шкала и критерии оценивания по результатам самоподготовки

Зачтено	Оценка «зачтено» выставляется студенту, если он в процессе опроса использует научную терминологию, стилистическое и логическое изложение ответа на вопросы, умеет делать выводы без существенных ошибок; владеет инструментарием изучаемой дисциплины; умеет ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им оценку
Не зачтено	Оценка «не зачтено» выставляется студенту, если он имеет недостаточно полный объем знаний в рамках опрашиваемой темы по дисциплине; использует научную терминологию, но изложение ответа на вопросы осуществляется с существенными логическими ошибками; слабо владеет инструментарием в рамках темы; не умеет ориентироваться в основных теориях, концепциях и направлениях изучаемой темы

5.4. Самоподготовка и участие в контрольно-оценочных учебных мероприятиях (работах) проводимых в рамках текущего контроля освоения дисциплины

Наименование оценочного средства	Охват обучающихся	Содержательная характеристика (тематическая направленность)	Расчетная трудоемкость, час
Очная форма обучения			
Входной тест	Фронтальный	Знание базовых понятий по информатике и информационным системам и технологиям	0
Опрос	Фронтальный	По результатам изучения тем № 1-6	6
Итоговый тест	Фронтальный	По результатам тем №1-6	6
Заочная форма обучения			
Опрос	Выборочный	Вопросы на знание базовых понятий по информатике и информационным системам	0
Итоговый тест	Фронтальный	По результатам тем №1-6	6

6. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ОБУЧАЮЩИХСЯ ПО РЕЗУЛЬТАТАМ ИЗУЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

6.1. Нормативная база проведения промежуточной аттестации обучающихся по результатам изучения дисциплины:	
Действующее «Положение о текущем контроле успеваемости, промежуточной аттестации обучающихся по программам высшего образования (бакалавриат, специалитет, магистратура) и среднего профессионального образования в ФГБОУ ВО Омский ГАУ»	
6.2 Основные характеристики промежуточной аттестации обучающихся по итогам изучения дисциплины	
Цель промежуточной аттестации –	Установление уровня достижения каждым обучающимся целей и задач обучения по данной дисциплине, изложенным в п.2.2 настоящей программы
Форма промежуточной аттестации –	Дифференцированный зачет
Место процедуры получения зачёта в графике учебного процесса	1. Участие обучающегося в процедуре получения зачёта осуществляется за счёт учебного времени (трудоемкости), отведённого на изучение дисциплины
	2. Процедура проводится в рамках ВАРО, на последней неделе семестра
Основные условия получения обучающимся зачёта:	1) обучающийся выполнил все виды учебной работы (включая самостоятельную) и отчитался об их выполнении в сроки, установленные графиком учебного процесса по дисциплине; 2) прошёл заключительное тестирование
Процедура получения зачёта –	Представлены в Фонде оценочных средств по данной учебной дисциплине (см. – Приложение 9)
Методические материалы, определяющие процедуры оценивания знаний, умений, навыков:	

7. ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

7.1. Библиотечное, информационное и методическое обеспечение учебного процесса по дисциплине

В соответствии с действующими государственными требованиями для реализации учебного процесса по дисциплине обеспечивающей кафедрой разрабатывается и постоянно совершенствуется учебно-методический комплекс (УМК), соответствующий данной рабочей программе. При разработке УМК кафедра руководствуется установленными университетом требованиями к его структуре, содержанию и оформлению.

Организационно-методическим ядром УМК являются:

- полная версии рабочей программы учебной дисциплины с внутренними приложениями №№ 1-3, 5, 6, 8;
- фонд оценочных средств по ней ФОС (Приложение 9);
- методические рекомендации для обучающихся по изучению дисциплины и прохождению контрольно-оценочных мероприятий (Приложение 4);
- методические рекомендации преподавателям по дисциплине (Приложение 7).

В состав учебно-методического комплекса в обязательном порядке также входят перечисленные в Приложениях 1 и 2 источники учебной и учебно-методической информации, учебные ресурсы и средства наглядности.

Приложения 1 и 2 к настоящему учебно-программному документу в обязательном порядке актуализируется на начало каждого учебного года

Электронная версия актуального УМКД, адаптированная для обучающихся, выставляется в информационно-образовательной среде университета.

7.2. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине; соответствующая им информационно-технологическая и компьютерная база

Применение средств ИКТ в процессе реализации дисциплины:

- использование интернет-браузеров для просмотра, поиска, фильтрации, организации, хранения, извлечения и анализа данных, информации и цифрового контента;
- использование облачных сервисов для просмотра, поиска, фильтрации, организации, хранения, извлечения и анализа данных, информации и цифрового контента (Google диск и т.д.);
- использование офисных приложений Microsoft Office (MS Excel, MS Word, MS Power Point и др.) и Open Office;
- подготовка отчетов в цифровом или бумажном формате, в том числе подготовка презентаций (MS Word, MS Power Point);
- использование digital-инструментов по формированию электронного образовательного контента в ЭИОС университета (<https://do.omgau.ru/>), проверке знаний, общения, совместной (командной) работы и самоподготовки студентов, сохранению цифровых следов результатов обучения и пр.

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине и сведения об информационно-технологической и компьютерной базе, необходимой для преподавания и изучения дисциплины, представлены в Приложении 5. Данное приложение в обязательном порядке актуализируется на начало каждого учебного года.

7.3. Материально-техническое обеспечение учебного процесса по дисциплине

Сведения о материально-технической базе, необходимой для реализации программы дисциплины, представлены в Приложении 6, которое в обязательном порядке актуализируется на начало каждого учебного года.

7.4. Организационное обеспечение учебного процесса и специальные требования к нему с учетом характера учебной работы по дисциплине

Аудиторные учебные занятия по дисциплине ведутся в соответствии с расписанием, внеаудиторная академическая работа организуется в соответствии с семестровым графиком ВАР и графиками сдачи/приёма/защиты выполненных работ. Консультирование обучающихся, изучающих данную дисциплину, осуществляется в соответствии с графиком консультаций.

7.5. Кадровое обеспечение учебного процесса по дисциплине

Сведения о кадровом обеспечении учебного процесса по дисциплине представлены в Приложении 8, которое в обязательном порядке актуализируется на начало каждого учебного года.

7.6. Обеспечение учебного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья

Организационно-педагогическое, психолого-педагогическое сопровождение обучающихся инвалидов и лиц с ограниченными возможностями здоровья осуществляется на основании соответствующей рекомендации в заключении психолого-медико-педагогической комиссии или индивидуальной программе реабилитации инвалида.

Обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов в случае необходимости:

- предоставляются печатные и (или) электронные образовательные ресурсы в формах, адаптированных к ограничениям их здоровья;
- учебно-методические материалы для самостоятельной работы, оценочные средства выбираются с учетом их индивидуальных психофизических особенностей;
- разрешается использование технических средств, необходимых им в связи с их индивидуальными особенностями (эти средства могут быть предоставлены университетом или могут использоваться собственные технические средства).
- проведение процедуры оценивания результатов обучения возможно с учетом особенностей нозологий (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.) при использовании доступной формы предоставления заданий оценочных средств и ответов на задания (в печатной форме увеличенным шрифтом, в форме аудиозаписи, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода) с использованием дополнительного времени для подготовки ответа.

Во время проведения занятий в группах, где обучаются инвалиды и обучающиеся с ОВЗ, возможно применение мультимедийных средств, оргтехники, слайд-проекторов и иных средств для повышения уровня восприятия учебной информации обучающимися с различными нарушениями. Для разъяснения отдельных вопросов изучаемой дисциплины преподавателями дополнительно проводятся индивидуальные консультации, в том числе с использованием сети Интернет.

7.7. Обеспечение образовательных программ с частичным применением электронного обучения и дистанционных образовательных технологий

При реализации программы дисциплины могут применяться электронное обучение и дистанционные образовательные технологии.

В случае применения электронного обучения, дистанционных образовательных технологий, обучающимся обеспечивается доступ к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочей программе. В информационно-образовательной среде университета в рамках дисциплин создается электронный обучающий курс, содержащий учебно-методические, теоретические материалы, информационные материалы для самостоятельной работы.

8. ЛИСТ РАССМОТРЕНИЙ И ОДОБРЕНИЙ

рабочей программы дисциплины Б1.В.ДВ.01.01 Криптографические методы защиты информации
в составе ОПОП 09.04.02 Информационные системы и технологии

1. Рассмотрена и одобрена:

а) На заседании обеспечивающей преподавание кафедры экономики, бухгалтерского учета и финансового контроля;

протокол № 11 от 19.05.2022

Зав. кафедрой, канд. экон. наук, доцент  О.А. Блинов

б) На заседании методической комиссии по направлению 09.04.02 Информационные системы и технологии;

протокол № 9 от 24.05.2022

Председатель МКН 09.04.02, канд. экон. наук  С.А. Нардина

2. Рассмотрение и одобрение представителями профессиональной сферы по профилю ОПОП:

Заместитель генерального директора
ООО ФТО «Центр разработки»



 Д.В. Малыгин

**9. ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ
к рабочей программе дисциплины
представлены в приложении 10.**

ПЕРЕЧЕНЬ литературы, рекомендуемой для изучения дисциплины Б1.В.ДВ.01.01 Криптографические методы защиты информации	
Автор, наименование, выходные данные	Доступ
Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. – 2-е изд., перераб. и доп. – Москва : РИОР : ИНФРА-М, 2021. – 413 с. – (Высшее образование: Бакалавриат). – ISBN 978-5-369-01267-3. – Текст : электронный. – URL: https://znanium.com/catalog/product/1215714 . – Режим доступа: по подписке.	http://znanium.com
Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е. К. Баранова, А. В. Бабаш. – 3-е изд., перераб. и доп. – Москва : РИОР : ИНФРА-М, 2020. – 320 с. – (Высшее образование). – ISBN 978-5-369-01848-4. – Текст : электронный. – URL: https://znanium.com/catalog/product/1052206 . – Режим доступа: по подписке.	http://znanium.com
Балдин, К. В. Информационные системы в экономике : учебное пособие / К.В. Балдин. – Москва : ИНФРА-М, 2022. – 218 с. – ISBN 978-5-16-005009-6. – Текст : электронный. – URL: https://znanium.com/catalog/product/1817522 . – Режим доступа: по подписке.	http://znanium.com
Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. – Москва ; Вологда : Инфра-Инженерия, 2020. – 692 с. – ISBN 978-5-9729-0486-0. – Текст : электронный. – URL: https://znanium.com/catalog/product/1167736 . – Режим доступа: по подписке.	http://znanium.com
Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина. – Москва : ИНФРА-М, 2021. – 216 с. – ISBN 978-5-16-016534-9. – Текст : электронный. – URL: https://znanium.com/catalog/product/1178150 . – Режим доступа: по подписке.	http://znanium.com
Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. – 2-е изд., перераб. и доп. – Москва : Логос, 2020. – 500 с. – ISBN 978-5-98704-711-8. – Текст : электронный. – URL: https://znanium.com/catalog/product/1212394 . – Режим доступа: по подписке.	http://znanium.com
Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере : монография / Н. Н. Куняев. – Москва : Логос, 2020. – 348 с. – ISBN 978-5-98704-513-8. – Текст : электронный. – URL: https://znanium.com/catalog/product/1213114 . – Режим доступа: по подписке.	http://znanium.com
Информационные технологии и вычислительные системы : ежекварт. науч. журн. – Москва : Российская академия наук, 1995 – . – Выходит 4 раза в год. – ISSN 2071-8632. – Текст : непосредственный.	НСХБ

**ПЕРЕЧЕНЬ РЕСУРСОВ
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»
И ЛОКАЛЬНЫХ СЕТЕЙ УНИВЕРСИТЕТА,
необходимых для освоения дисциплины
Б1.В.ДВ.01.01 Криптографические методы защиты информации**

1. Удаленные электронные сетевые учебные ресурсы временного доступа, сформированные на основании прямых договоров с правообладателями (электронные библиотечные системы – ЭБС), информационно-справочные системы		
Наименование		Доступ
Электронно-библиотечная система издательства «Лань»		http://e.lanbook.com
Электронно-библиотечная система «Znaniy.com»		http://znaniy.com
Электронно-библиотечная система «Консультант студента»		http://www.studentlibrary.ru
Универсальная база данных ИВИС		https://eivis.ru/
Справочная правовая система КонсультантПлюс		http://www.consultant.ru
2. Электронные сетевые ресурсы открытого доступа (профессиональные базы данных, массовые открытые онлайн-курсы и пр.):		
Профессиональные базы данных		https://do.omgau.ru
3. Электронные учебные и учебно-методические ресурсы, подготовленные в университете:		
Автор(ы)	Наименование	Доступ
-	-	-

**УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ
САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ
по дисциплине Б1.В.ДВ.01.01 Криптографические методы защиты информации**

1. Учебно-методическая литература			
Автор, наименование, выходные данные			Доступ
2. Учебно-методические разработки на правах рукописи			
Автор(ы)	Наименование		Доступ
3. Учебные ресурсы открытого доступа (МООК)			
Наименование МООК	Платформа	ВУЗ разработчик	Доступ (ссылка на МООК, дата последнего обращения)

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ
по освоению дисциплины
представлены отдельным документом**

**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ,
используемые при осуществлении образовательного процесса
по дисциплине Б1.В.ДВ.01.01 Криптографические методы защиты информации**

1. Программные продукты, необходимые для освоения учебной дисциплины		
Наименование программного продукта (ПП)	Виды учебных занятий и работ, в которых используется данный продукт	
Пакет офисных программ	Лекции, практические занятия, ВАРС	
2. Информационные справочные системы, необходимые для реализации учебного процесса		
Наименование справочной системы	Доступ	
Свободная энциклопедия Википедия	http://ru.wikipedia.org/wiki/	
СПС «КонсультантПлюс»	Учебные аудитории университета http://www.consultant.ru	
3. Специализированные помещения и оборудование, используемые в рамках информатизации учебного процесса		
Наименование помещения	Наименование оборудования	Виды учебных занятий и работ, в которых используется данное помещение
Компьютерные классы с выходом в интернет	ПК, комплект мультимедийного оборудования	Аудиторные занятия, ВАРС
4. Электронные информационно-образовательные системы (ЭИОС)		
Наименование ЭИОС	Доступ	Виды учебных занятий и работ, в которых используется данная система
ЭИОС ОмГАУ-Moodle	http://do.omgau.ru	Самостоятельная работа студента

**МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ
УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ
Б1.В.ДВ.01.01 Криптографические методы защиты информации**

Наименование объекта	Оснащенность объекта
Учебная аудитория для проведения лекционных и практических занятий, групповых и индивидуальных консультаций	Доска ученическая 3х-элементная, мебель аудиторная. Рабочее место преподавателя: монитор, компьютер (клавиатура, мышь, колонки) Рабочие места обучающихся. Демонстрационное оборудование: экран настенный, проектор Список ПО на компьютере: Пакет офисных программ
Учебная аудитория для проведения лекционных и практических (лабораторных) занятий, групповых и индивидуальных консультаций	Компьютерный класс с выходом в «Интернет» Рабочее место преподавателя, рабочие места обучающихся, оснащенные компьютерами с выходом в «Интернет», с программным обеспечением. Программное обеспечение: Пакет офисных программ, Переносное мультимедийное оборудование: проектор, экран.
Помещения для самостоятельной работы и курсового проектирования	Рабочие места обучающихся, оснащенные компьютерами с выходом в «Интернет» (8 шт.), с программным обеспечением. Список ПО на компьютерах: Пакет офисных программ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПРЕПОДАВАТЕЛЯМ по дисциплине

1. ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ К УЧЕБНОЙ РАБОТЕ ПО ДИСЦИПЛИНЕ

Формы организации учебной деятельности по дисциплине: лекция, практические (семинарские) занятия, самостоятельная работа студентов, дифференцированный зачет.

У студентов ведутся лекционные занятия в интерактивной форме в виде лекции-визуализации.

В ходе изучения дисциплины студенту необходимо выполнить внеаудиторную работу, которая состоит из следующих видов работ: подготовка презентации, самостоятельное изучение тем, подготовка к текущему контролю.

Учитывая значимость дисциплины, к ее изучению предъявляются следующие организационные требования:

- обязательное посещение студентом всех видов аудиторных занятий; ведение конспекта в ходе лекционных занятий; качественная самостоятельная подготовка к лабораторным занятиям;
- активная, ритмичная внеаудиторная работа студента; своевременная сдача преподавателю отчетных материалов по аудиторным и внеаудиторным видам работ.

2. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ ЛЕКЦИОННЫХ ЗАНЯТИЙ

Специфика дисциплины состоит в том, что рассмотрение теоретических вопросов на лекциях тесно связано с лабораторными занятиями. В этих условиях на лекциях особенно большое значение имеет реализация следующих задач:

- 1) глубокое осмысливание ряда понятий и положений, введенных в теоретическом курсе;
- 2) раскрытие прикладного значения теоретических сведений;
- 3) развитие творческого подхода к решению практических и некоторых теоретических вопросов;
- 4) закрепление полученных знаний путем практического использования;

Наряду с перечисленными выше образовательными целями, лекционные занятия должны преследовать и важные цели воспитательного характера, а именно:

- а) воспитание настойчивости в достижении конечной цели;
- б) воспитание дисциплины ума, аккуратности, добросовестного отношения к работе;
- в) воспитание критического отношения к своей деятельности, умения анализировать свою работу, искать оптимальный путь решения, находить свои ошибки и устранять их.

При изложении материала учебной дисциплины, преподавателю следует обратить внимание, во-первых, на то, что студенты получили определенное знание об инструментальных средствах информационных систем при изучении других учебных дисциплин, во-вторых, необходимо избегать дублирования материала с другими учебными дисциплинами, которые студенты уже изучили либо которые предстоит им изучить. Для этого необходимо преподавателю ознакомиться с учебно-методическими комплексами дисциплин, взаимосвязанных с дисциплиной.

Преподаватель должен четко дать связанное, последовательное изложение материала в соответствии с новейшими данными науки, представить студентам основное ее содержание в сжатом, систематизированном виде. Преподаватель должен излагать учебный материал с позиций междисциплинарного подхода, давать четкие определения понятийного аппарата, который используется при изучении дисциплины.

В учебном процессе преподаватель должен использовать активные и интерактивные формы обучения студентов, которые должны опираться на творческое мышление студентов, в наибольшей степени активизировать познавательную деятельность, делать их соавторами новых идей, приучать их самостоятельно принимать оптимальные решения и способствовать их реализации.

В аудиторной работе со студентами предполагается проведение лекций-визуализаций.

Лекция-визуализация представляет собой визуальную форму подачи лекционного материала техническими средствами обучения.

3. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ

По дисциплине рабочей программой предусмотрены практические (семинарские) занятия, которые служат для осмысления и более глубокого изучения теоретических проблем, а также отработки навыков использования знаний. Практическое занятие дает студенту возможность:

- проверить, уточнить, систематизировать знания;
- овладеть терминологией и свободно ею оперировать;
- научиться точно и доказательно выражать свои мысли на языке конкретной науки;
- анализировать факты, выполнять определенные задачи.

Практические занятия призваны укреплять интерес студента к науке и научным исследованиям, научить связывать научно-теоретические положения с практической деятельностью. Практические занятия состоят из системы заданий по каждому из вопросов, освещенных заранее.

4. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

4.1. Самостоятельное изучение тем

Преподаватель в начале изучения дисциплины выдает студентам все темы для самостоятельного изучения, определяет сроки ВАРС и предоставления отчетных материалов преподавателю. Студентам необходимо представить выполненные конспекты по темам, изученным самостоятельно, а также пройти опрос.

Преподавателю необходимо пояснить студентам общий алгоритм самостоятельного изучения тем:

Общий алгоритм самостоятельного изучения темы

- ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме;
- на этой основе составить развёрнутый план (конспект) изложения темы;
- подготовиться к опросу по теме.

Шкала и критерии оценивания опроса	
Зачтено	Оценка «зачтено» ставится, если обучающийся в процессе опроса использует научную терминологию, стилистическое и логическое изложение ответа на вопросы, умеет делать выводы без существенных ошибок; владеет инструментарием изучаемой дисциплины; умеет ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им оценку.
Не зачтено	Оценка «не зачтено» ставится, если обучающийся: имеет недостаточно полный объем знаний в рамках опрашиваемой темы по дисциплине; использует научную терминологию, но изложение ответа на вопросы осуществляется с существенными логическими ошибками; слабо владеет инструментарием в рамках темы; не умеет ориентироваться в основных теориях, концепциях и направлениях изучаемой темы.

4.2. Самоподготовка студентов к занятиям по дисциплине

Самоподготовка студентов к занятиям осуществляется в виде изучения литературы по заранее известным темам и вопросам.

Шкала и критерии оценивания по результатам выполнения домашней работы	
Зачтено	Оценка «зачтено» выставляется студенту, если он в процессе опроса использует научную терминологию, стилистическое и логическое изложение ответа на вопросы, умеет делать выводы без существенных ошибок; владеет инструментарием изучаемой дисциплины; умеет ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им оценку
Не зачтено	Оценка «не зачтено» выставляется студенту, если он имеет недостаточно полный объем знаний в рамках опрашиваемой темы по дисциплине; использует научную терминологию, но изложение ответа на вопросы осуществляется с существенными логическими ошибками; слабо владеет инструментарием в рамках темы; не умеет ориентироваться в основных теориях, концепциях и направлениях изучаемой темы

5. КОНТРОЛЬНЫЕ МЕРОПРИЯТИЯ ПО РЕЗУЛЬТАТАМ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

В течение семестра по итогам изучения разделов дисциплины студент должен пройти контроль успеваемости в виде выполнения заданий на практических занятиях, а также опроса по темам дисциплины.

Шкала и критерии оценивания опроса	
Зачтено	<i>Оценка «зачтено»</i> ставится, если обучающийся в процессе опроса использует научную терминологию, стилистическое и логическое изложение ответа на вопросы, умеет делать выводы без существенных ошибок; владеет инструментарием изучаемой дисциплины; умеет ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им оценку.
Не зачтено	<i>Оценка «не зачтено»</i> ставится, если обучающийся: имеет недостаточно полный объем знаний в рамках опрашиваемой темы по дисциплине; использует научную терминологию, но изложение ответа на вопросы осуществляется с существенными логическими ошибками; слабо владеет инструментарием в рамках темы; не умеет ориентироваться в основных теориях, концепциях и направлениях изучаемой темы.

Форма промежуточной аттестации студентов – **дифференцированный зачет**.

Критерии оценки ответов на тестовые задания зачета (итоговый тест):

- оценка «отлично» выставляется обучающемуся, если получено более 81% правильных ответов.
- оценка «хорошо» - получено от 71 до 80% правильных ответов.
- оценка «удовлетворительно» - получено от 61 до 70% правильных ответов.
- оценка «неудовлетворительно» - получено менее 61% правильных ответов.

КАДРОВОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ**Требования ФГОС**

Реализация программы магистратуры обеспечивается педагогическими работниками университета, а также лицами, привлекаемыми университетом к реализации программы магистратуры на иных условиях.

Квалификация педагогических работников должна отвечать квалификационным требованиям, указанным в квалификационных справочниках и (или) профессиональных стандартах (при наличии).

Не менее 70 процентов численности педагогических работников, участвующих в реализации программы магистратуры, и лиц, привлекаемых к реализации программы магистратуры на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), должны вести научную, учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля).

Не менее 5 процентов численности педагогических работников участвующих в реализации программы магистратуры, и лиц, привлекаемых к реализации программы магистратуры на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), должны являться руководителями и (или) работниками иных организаций, осуществляющими трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники (иметь стаж работы в данной профессиональной сфере не менее 3 лет).

Не менее 60 процентов численности педагогических работников и лиц, привлекаемых к образовательной деятельности на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), должны иметь ученую степень (в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации) и (или) ученое звание (в том числе ученое звание, полученное в иностранном государстве и признаваемое в Российской Федерации).

**Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Омский государственный аграрный университет имени П.А. Столыпина»
Экономический факультет**

**ОПОП по направлению подготовки
09.04.02 Информационные системы и технологии**

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине**

Б1.В.ДВ.01.01 Криптографические методы защиты информации

Направленность (профиль) «Информационные системы и технологии»

Обеспечивающая преподавание дисциплины кафедра	Кафедра экономики, бухгалтерского учета и финансового контроля
Разработчик, канд. экон. наук, доцент	А.А. Ремизова

ВВЕДЕНИЕ

1. Фонд оценочных средств по дисциплине является обязательным обособленным приложением к Рабочей программе дисциплины.

2. Фонд оценочных средств является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися указанной дисциплины.

3. При помощи ФОС осуществляется контроль и управление процессом формирования обучающимися компетенций, из числа предусмотренных ФГОС ВО в качестве результатов освоения дисциплины.

4. Фонд оценочных средств по дисциплине включает в себя: оценочные средства, применяемые для входного контроля; оценочные средства, применяемые в рамках индивидуализации выполнения, контроля фиксированных видов ВАРС; оценочные средства, применяемые для текущего контроля и оценочные средства, применяемые при промежуточной аттестации по итогам изучения дисциплины.

5. Разработчиками фонда оценочных средств по дисциплине являются преподаватели кафедры экономики, бухгалтерского учета и финансового контроля, обеспечивающей изучение обучающимися дисциплины в университете. Содержательной основой для разработки ФОС послужила Рабочая программа дисциплины.

1. ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ИЗУЧЕНИЯ
учебной дисциплины, персональный уровень достижения которых проверяется
с использованием представленных в п. 3 оценочных средств

Компетенции, в формировании которых задействована дисциплина		Код и наименование индикатора достижений компетенции	Компоненты компетенций, формируемые в рамках данной дисциплины (как ожидаемый результат ее освоения)		
код	наименование		знать и понимать	уметь делать (действовать)	владеть навыками (иметь навыки)
Профессиональные компетенции					
ПК-1	Способен разрабатывать и исследовать модели объектов профессиональной деятельности, предлагать и адаптировать методики, определять качество проводимых исследований, составлять отчеты о проделанной работе, обзоры, готовить публикации	ИД-1 _{пк-1.1} Понимает принципы, методы и знает средства анализа и структурирования профессиональной информации; методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации; методы исследований; принципы построения математических моделей процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений	основные принципы, методы и средства криптографической защиты информации в организации; основные понятия и требования криптографической защиты информации; принципы построения математических моделей процессов и объектов; модели шифров и математические методы их исследования	выбирать основные принципы, методы и средства криптографической защиты информации в организации; выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации; выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации;	применения основных принципов, методов и средств криптографической защиты информации в организации; применения принципов построения математических моделей процессов и объектов определения криптографической стойкости шифрсистем; навыками обоснования выбора криптографических средств для защиты информации
		ИД-2 _{пк-2.2} Анализирует профессиональную информацию, выделяет в ней главное, структурирует, оформляет и представляет в виде аналитических обзоров; применяет на практике новые научные принципы и методы исследований; разрабатывает и применяет математические модели процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений	аспекты анализа профессиональной информации; новые научные принципы и методы исследований; математические модели процессов и объектов при решении задач криптографической защиты информации	анализировать профессиональную информацию; применять на практике новые научные принципы и методы исследований; разрабатывать и применять математические модели процессов и объектов при решении задач криптографической защиты информации	всестороннего анализа профессиональной информации; применения на практике новых научных принципов и методов исследований; разработки и применения математического моделирования в криптографии

ЧАСТЬ 2. ОБЩАЯ СХЕМА ОЦЕНИВАНИЯ ХОДА И РЕЗУЛЬТАТОВ ИЗУЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общие критерии оценки и реестр применяемых оценочных средств

2.1. Обзорная ведомость-матрица оценивания хода и результатов изучения учебной дисциплины в рамках педагогического контроля

Категория контроля и оценки	Режим контрольно-оценочных мероприятий				
	само- оценка	взаимооценка	Оценка со стороны		Комис- сионная оценка
			препода- вателя	представителя производства	
	1	2	3	4	5
Входной контроль			Тестирование		
Индивидуализация выполнения*, контроль фиксированных видов ВАРС:					
Выполнение и сдача презентации			Проверка отчетных материалов		
Текущий контроль:					
- Самостоятельное изучение тем	Вопросы		Опрос		
- в рамках практических (семинарских) занятий и подготовки к ним	Вопросы и задания		Опрос		
- в рамках обще- университетской системы контроля успеваемости			Фронтальный контроль текущей успеваемости по контрольным неделям, установленным в университете		
По итогам изучения тем 1-6			Опрос		
Промежуточная аттестация* обучающихся по итогам изучения дисциплины	Вопросы для подготовки к дифференцированному зачету		Итоговое тестирование		
* данным знаком помечены индивидуализируемые виды учебной работы					

2.2. Общие критерии оценки хода и результатов изучения учебной дисциплины

1. Формальный критерий получения обучающимися положительной оценки по итогам изучения дисциплины:	
1.1 Предусмотренная программа изучения дисциплины обучающимся выполнена полностью до начала процесса промежуточной аттестации	1.2 По каждой из предусмотренных программой видов работ по дисциплине обучающийся успешно отчитался перед преподавателем, демонстрируя при этом должный (не ниже минимально приемлемого) уровень сформированности элементов компетенций
2. Группы неформальных критериев качественной оценки работы обучающегося в рамках изучения дисциплины:	
2.1 Критерии оценки качества хода процесса изучения обучающимся программы дисциплины (текущей успеваемости)	2.2. Критерии оценки качества выполнения конкретных видов ВАРС
2.3 Критерии оценки качественного уровня итоговых результатов изучения дисциплины	2.4. Критерии аттестационной оценки качественного уровня результатов изучения дисциплины

2.3 РЕЕСТР элементов фонда оценочных средств по учебной дисциплине

Группа оценочных средств	Оценочное средство или его элемент
	Наименование
1. Средства для входного контроля	Тестовые вопросы для проведения входного контроля
	Критерии оценки вопросы тестового задания входного контроля
2. Средства для индивидуализации выполнения, контроля фиксированных видов ВАРС	Перечень тем для подготовки презентации. Процедура выбора темы обучающимся
	Критерии оценки индивидуальных результатов выполнения презентации
3. Средства для текущего контроля	Вопросы для самостоятельного изучения темы
	Общий алгоритм самостоятельного изучения темы
	Критерии оценки самостоятельного изучения темы
	Вопросы для самоподготовки по темам практических занятий
	Критерии оценки самоподготовки по темам практических занятий
	Критерии оценки выполнения практических заданий
	Вопросы для подготовки к опросу
	Критерии оценки ответов на вопросы (опрос)
4. Средства для промежуточной аттестации по итогам изучения дисциплины	Программа для сдачи зачета по учебной дисциплине
	Плановая процедура проведения дифференцированного зачета
	Тестовые вопросы для проведения итогового контроля
	Критерии оценки ответов на тестовые вопросы итогового контроля

2.4. Описание показателей, критериев и шкал оценивания и этапов формирования компетенций в рамках дисциплины

Индекс и название компетенции	Код индикатора достижений компетенции	Индикаторы компетенции	Показатель оценивания – знания, умения, навыки (владения)	Уровни сформированности компетенций				Формы и средства контроля формирования компетенций
				компетенция не сформирована	минимальный	средний	высокий	
				Оценки сформированности компетенций				
				2	3	4	5	
				Оценка «неудовлетворительно»	Оценка «удовлетворительно»	Оценка «хорошо»	Оценка «отлично»	
				Характеристика сформированности компетенции				
				Компетенция в полной мере не сформирована. Имеющихся знаний, умений и навыков недостаточно для решения практических (профессиональных) задач	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач	Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач	
Критерии оценивания								
ПК-1 Способен разрабатывать и исследовать модели объектов профессиональной деятельности, предлагать и адаптировать методики, определять качество проводимых исследований, составлять отчеты о проделанной работе, обзоры, готовить публикации	ИД-1 _{ПК-2.1} Понимает принципы, методы и средства анализа и структурирования профессиональной информации; методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации; методы исследований; принципы построения математических моделей процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений	Полнота знаний	Основные принципы, методы и средства криптографиической защиты информации в организации; основные понятия и требования криптографиической защиты информации; принципы построения математических моделей процессов и объектов; модели шифров и математические методы их исследования	Не знает основные принципы, методы и средства криптографиической защиты информации в организации; основные понятия и требования криптографиической защиты информации; принципы построения математических моделей процессов и объектов; модели шифров и математические методы их исследования	Имеет поверхностное представление о принципах, методах и средствах криптографиической защиты информации в организации; об основных понятиях и требованиях криптографиической защиты информации; принципах построения математических моделей процессов и объектов; моделях шифров и математических методах их исследования	Знает основные принципы, методы и средства криптографиической защиты информации в организации; основные понятия и требования криптографиической защиты информации; принципы построения математических моделей процессов и объектов; модели шифров и математические методы их исследования	Знает и понимает ключевые принципы, методы и средства криптографиической защиты информации в организации; основные понятия и требования криптографиической защиты информации; принципы построения математических моделей процессов и объектов; модели шифров и математические методы их исследования	Оценка ответов на практических занятиях; оценка выполненных заданий на практических занятиях; опрос по самостоятельно изученным темам; проверка выполненной электронной презентации; тестирование
		Наличие умений	Выбирать основные принципы, методы и средства криптографиической защиты информации в организации; выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации; выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации	Не умеет выбирать основные принципы, методы и средства криптографиической защиты информации в организации; выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации; выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации	Умеет выбирать некоторые принципы, методы и средства криптографиической защиты информации в организации; выявлять специфику некоторых криптографических угроз информационной безопасности по ряду категорий информации; с трудом выделяет основания и объекты защиты информации, определяет основания и процедуру осуществления криптографической	Умеет выбирать основные принципы, методы и средства криптографиической защиты информации в организации; выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации; выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации	В совершенстве умеет выбирать основные принципы, методы и средства криптографиической защиты информации в организации; выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации; выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации	

ЧАСТЬ 3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Часть 3.1. Типовые контрольные задания, необходимые для оценки знаний, умений, навыков

**3.1.1. Средства
для индивидуализации выполнения, контроля фиксированных видов ВАРС**

Место электронной презентации в структуре учебной дисциплины

Разделы дисциплины, освоение которых обучающимися сопровождается или завершается выполнением электронной презентации		Компетенции, формирование/развитие которых обеспечивается в ходе выполнения электронной презентации
№	Наименование	
1	Тема 1. Основные понятия.	ПК-1.1 Понимает принципы, методы и знает средства анализа и структурирования профессиональной информации; методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации; методы исследований; принципы построения математических моделей процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений ПК-1.2 Анализирует профессиональную информацию, выделяет в ней главное, структурирует, оформляет и представляет в виде аналитических обзоров; применяет на практике новые научные принципы и методы исследований; разрабатывает и применяет математические модели процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений
	Тема 2 Основные характеристики шифров	
	Тема 3 Симметричная криптография	
	Тема 4 Криптография с открытым ключом	
	Тема 5 Электронная подпись	
	Тема 6 Применение криптографических методов и средств для обеспечения информационной безопасности	

Перечень примерных тем электронной презентации

Тема презентации выбирается студентами самостоятельно по согласованию с преподавателем. Материал подготавливается студентами на основе индивидуальной проработки рекомендованной преподавателем и самостоятельно подобранной основной и дополнительной учебной литературы по теме, ее анализа.

Примерные темы презентаций:

1. Определение шифра. Классификация шифров.
2. Понятие криптографической системы. Требования к криптографическим системам.
3. Формальные модели шифров. Алгебраическая и вероятностная модель шифра.
4. Математическая модель открытых текстов.
5. Алгебраическая модель шифра перестановки.
6. Алгебраическая модель шифра замены.
7. Алгебраическая модель шифра гаммирования.
8. Криптографическая стойкость шифра. Виды атак.
9. Практическая стойкость шифра.
10. Имитостойкость шифра.
11. Помехозащищенность шифра.
12. Методы криптоанализа.
13. Блочные шифры. Принципы построения.
14. Блочные шифры. DES. Функция шифрования, S-блоки.
15. Блочные шифры. ГОСТ 34.12-2018 и ГОСТ 34.13-2018.
16. Блочные шифры. AES.

17. Режимы использования блочных шифров. ECB
18. Режимы использования блочных шифров. CBC
19. Режимы использования блочных шифров. OFB
20. Режимы использования блочных шифров. CFB.
21. Комбинирование блочных шифров
22. Поточные шифры. Синхронные и самосинхронизирующиеся шифры
23. Поточные шифры. Принципы построения. Связь с режимами блочных шифров.
24. Поточные шифры. RC4.
25. Датчики истинно случайных последовательностей. Требования. Источники. Свойства.
26. Генераторы псевдослучайной последовательности. Методы усложнения.
27. Методы тестирования случайных последовательностей

Шкала и критерии оценивания электронной презентации	
Отлично	Оценка «отлично» по презентации присваивается за глубокое раскрытие темы, качественное оформление работы, содержательность презентации, за понимание студентом отражённого в презентации материала.
Хорошо	Оценка «хорошо» по презентации присваивается при соответствии выше перечисленным критериям, но при наличии в содержании работы и ее оформлении небольших недочетов или недостатков в представлении результатов к защите
Удовлетворительно	Оценка «удовлетворительно» по презентации присваивается за неполное раскрытие темы, выводов и предложений, носящих общий характер, плохо подготовленное наглядное представление работы и затруднения при ответах на вопросы
Неудовлетворительно	Оценка «неудовлетворительно» по презентации присваивается за слабое и неполное раскрытие темы, несамостоятельность изложения материала, выводы и предложения, носящие общий характер, отсутствие наглядного представления работы и ответов на вопросы

3.1.2. ТЕСТОВЫЕ ВОПРОСЫ для проведения входного контроля

1. Как информационные технологии влияют на инфраструктуру предприятия?
оптимизируют ее
создают дополнительную финансовую нагрузку
увеличивают объем рутинных работ
никак не влияют
2. Выбор ИТ–инфраструктуры основан на:
современном уровне развития ИТ-технологий
архитектура бизнеса
на техническом задании на создание АИС
финансовых возможностях предприятия
3. ИТ –инфраструктура предприятия –это:
программные, технические и информационные компоненты, входящие в систему управления
комплекс технических средств АИС предприятия
элементы электронного офиса предприятия
система организационных структур, обеспечивающих функционирование и развитие
информационного производства предприятия и средств информационного взаимодействия
4. Объем передаваемой по сети информации называется:
шириной сети
трафиком
коннектом
пропускной способностью
5. Конфиденциальность – это:
обеспечение существования информации в неискажённом виде

обеспечение свободного доступа к информации
обеспечение готовности системы к обслуживанию поступающих к ней запросов
обеспечение доступа к информации только авторизованного круга субъектов

6. По сфере применения различают информационные системы:
внешние и внутренние
региональные и общероссийские
бухгалтерские, банковские, страховые, налоговые

7. Основные проблемы внедрения ИТ в организации включают:
организационные и кадровые
концептуальные
технические
финансовые

8. Информационные технологии это:
система программных средств
комплекс технических средств
система методов сбора, накопления, хранения, поиска и обработки информации

9. Приложение, позволяющие сформировать взаимодействие внутренних подразделений предприятия:
Canva
Trello
Snappable

10. Способы защиты информации в информационных технологиях?
информационные программы
технические, законодательные и программные средства
внесистемные программы

11. Основные этапы обработки в ИТ информации:
устройства ввода, обработка, вывод информации
исходная информация, конечная информация
обработка и выход информации

12. Информационные технологии в деятельности предприятия предназначены для:
для сбора, хранения, выдачи и передачи информации
постоянного хранения информации
производить расчеты и вычисления

13. Руководство компании должно оценивать стратегию в области ИТ-инфраструктуры с точки зрения:
результатов проведения стороннего аудита
эффективности
финансовых вложений

14. Инструментальная система технологии программирования – это...
программное средство, предназначенное для поддержки разработки других программ
устройство компьютера, специально предназначенное для поддержки разработки программного средства
интегрированная совокупность программных и аппаратных инструментов, поддерживающая все процессы разработки и сопровождения больших программных продуктов
логически связанная совокупность программных и аппаратных инструментов, поддерживающих разработку ПП

15. Операционная система – это:
прикладная программа;
система программирования;
системная программа;
текстовый редактор.

ШКАЛА И КРИТЕРИИ ОЦЕНКИ
ответов на тестовые вопросы входного контроля

- оценка «отлично» выставляется обучающемуся, если получено более 81% правильных ответов.
- оценка «хорошо» - получено от 71 до 80% правильных ответов.
- оценка «удовлетворительно» - получено от 61 до 70% правильных ответов.
- оценка «неудовлетворительно» - получено менее 61% правильных ответов.

3.1.3. Средства для текущего контроля

ВОПРОСЫ **для самостоятельного изучения темы** **для очной формы обучения**

Тема 1. Основные понятия

1.1 Криптография. Цели криптографии. История развития криптографии. Классификация криптографических методов. Обеспечение конфиденциальности, целостности, неотказуемости, аутентичности, неотслеживаемости информации. Основные понятия: шифр, открытый текст, шифртекст, электронная подпись, хэш-функция.

1.2 Составные элементы шифра. Классификация шифров.

Тема 3 Симметричная криптография

3.1 Блочные и поточные шифры. Признаки методов шифрования данных.

3.2 Принципы построения блочных шифров

Тема 5 Электронная подпись

5.1 Понятие электронной подписи. Связь с понятием электронной подписи Ф3-63. Процессы формирования и проверки электронной подписи. Алгебраическая модель схемы электронной подписи.

5.2 Способы построения электронной подписи. Схемы электронной подписи.

ВОПРОСЫ **для самостоятельного изучения темы** **для заочной формы обучения**

Тема 1. Основные понятия

1.1 Криптография. Цели криптографии. История развития криптографии. Классификация криптографических методов. Обеспечение конфиденциальности, целостности, неотказуемости, аутентичности, неотслеживаемости информации. Основные понятия: шифр, открытый текст, шифртекст, электронная подпись, хэш-функция.

1.2 Составные элементы шифра. Классификация шифров.

Тема 2 Основные характеристики шифров

2.1 Алгебраическая модель шифра. Вероятностная модель шифра.
Модели открытых текстов

Тема 3 Симметричная криптография

3.1 Блочные и поточные шифры. Признаки методов шифрования данных.

3.2 Принципы построения блочных шифров

Тема 4 Криптография с открытым ключом

4.2 Схемы шифрования на основе односторонних функций

Тема 5 Электронная подпись

5.1 Понятие электронной подписи. Связь с понятием электронной подписи Ф3-63. Процессы формирования и проверки электронной подписи. Алгебраическая модель схемы электронной подписи.

5.2 Способы построения электронной подписи. Схемы электронной подписи.

Тема 6 Применение криптографических методов и средств для обеспечения информационной безопасности

6.1 Коды аутентификации сообщений

6.2 Криптографические протоколы

6.3 Управление ключами

ОБЩИЙ АЛГОРИТМ **самостоятельного изучения темы**

- ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме;
- на этой основе составить развернутый план (конспект) изложения темы;

– подготовиться к опросу по теме.

Шкала и критерии оценивания опроса	
Зачтено	<i>Оценка «зачтено»</i> ставится, если обучающийся в процессе опроса использует научную терминологию, стилистическое и логическое изложение ответа на вопросы, умеет делать выводы без существенных ошибок; владеет инструментарием изучаемой дисциплины; умеет ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им оценку.
Не зачтено	<i>Оценка «не зачтено»</i> ставится, если обучающийся: имеет недостаточно полный объем знаний в рамках опрашиваемой темы по дисциплине; использует научную терминологию, но изложение ответа на вопросы осуществляется с существенными логическими ошибками; слабо владеет инструментарием в рамках темы; не умеет ориентироваться в основных теориях, концепциях и направлениях изучаемой темы.

ВОПРОСЫ для самоподготовки к практическим занятиям

Тема 1. Основные понятия

1. Основные понятия

2 Криптографическая система. Классификация шифров

Криптография. Цели криптографии. История развития криптографии. Классификация криптографических методов. Обеспечение конфиденциальности, целостности, неотказуемости, аутентичности, неотслеживаемости информации. Основные понятия: шифр, открытый текст, шифртекст, электронная подпись, хэш-функция

Математические примитивы. Криптографические алгоритмы. Криптографическая схема. Криптографическая система. Классификация шифров.

Тема 2 Основные характеристики шифров

- 1. Алгебраическая модель шифра. Вероятностная модель шифра. Модели открытых текстов.*
- 2. Криптографическая стойкость шифров. Атаки на шифры*
- 3. Теоретическая и практическая стойкость шифра*
- 4. Имитостойкость, помехоустойчивость шифров*

Алгебраическая модель шифра. Алгебраическая модель шифра замены. Алгебраическая модель шифра перестановки. Алгебраическая модель шифра гаммирования.

Модели открытых текстов. Вероятностная модель шифра. Распределения на множествах открытых текстов, ключей, шифртекстов. Математические модели открытых текстов.

Атаки на шифры. Понятие стойкости шифров. Классификация атак на шифры. Виды атак на схемы шифрования. Цели криптоанализа.

Теоретико-информационная стойкость. Условная вероятность. Энтропия. Понятие абсолютно стойкого шифра. Теоретико-сложностная стойкость шифров.

Понятие практической стойкости шифра. Модель противника.

Основные требования к шифрам. Имитостойкость шифра. Помехоустойчивость шифра. Способы обеспечения имитостойкости и помехоустойчивости.

Тема 3 Симметричная криптография

- 1. Блочные и поточные шифры.*
- 2. Принципы построения блочных шифров.*
- 3. Сеть Фейстеля. Шифр DES.*
- 4. Режимы работы блочных шифров*
- 5. Поточные шифры*
- 6. Генераторы псевдослучайных последовательностей.*

Классификация симметричных криптографических систем. Требования к блочным шифрам. Требования к поточным шифрам.

Криптографические параметры узлов и блоков блочных шифров. Базовые криптографические преобразования блочных шифров. Способы реализации блочных шифров. Процедура развертывания ключа.

Сеть Фейстеля. Шифр DES. Основные преобразования. Алгоритм зашифрования. Алгоритм расшифрования. Процедура развертывания ключа.

Основные параметры. Алгоритм зашифрования. Алгоритм расшифрования. ГОСТ 34.12-15; ГОСТ 34.12-2018 и ГОСТ 34.13-2018.

Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью по выходу. Режим простой замены с зацеплением. Режим гаммирования с обратной связью по шифртексту. Режим выработки имитовставки.

Поточные шифры. Требования к поточным шифрам. Типовые методы построения поточных шифров. Синхронные и самосинхронизирующиеся поточные шифры.

Генератор на основе РЛЗ. Статистические характеристики генераторов псевдослучайных последовательностей. Методы усложнения последовательностей.

Тема 4 Криптография с открытым ключом

1. *Односторонние функции, функции с секретом.*
2. *Схемы шифрования на основе односторонних функций.*
3. *Схемы шифрования RSA и Эль-Гамала*

Элементы теории сложности. Односторонние функции. Односторонние функции с секретом. Примеры односторонних функций с секретом.

Алгебраическая модель асимметричного шифра. Понятие открытого ключа.

Схема шифрования RSA. Процедура генерации ключей. Процедура шифрования. Схема Эль-Гамала. Стойкость схем шифрования RSA и Эль-Гамала.

Тема 5 Электронная подпись

1. *Понятие электронной подписи. Способы построения электронной подписи*
2. *Эллиптические кривые.*
3. *Криптографическая хэш-функция.*
4. *Конструкция хэш-функций*

Понятие электронной подписи. Связь с понятием электронной подписи Ф3-63. Процессы формирования и проверки электронной подписи. Алгебраическая модель схемы электронной подписи.

Конструкция схемы электронной подписи на односторонней функции с секретом. Электронная подпись на основе схемы шифрования с открытым ключом, электронная подпись с извлечением сообщения, электронная подпись с дополнением.

Параметры схемы электронной подписи. Процедуры генерации ключей, формирования и проверки подписи. Стойкость схемы электронной подписи.

Эллиптические кривые. Группа точек эллиптической кривой. Операции с точками эллиптической кривой. Параметры схемы электронной подписи. Процедуры генерации ключей, формирования и проверки подписи. Стойкость схемы электронной подписи.

Криптографическая хэш-функция без ключа. Слабая хэш-функция. Сильная хэш-функция. Стойкость криптографической хэш-функции. Применение хэш-функций. Типовые конструкции криптографических хэш-функций.

Хэш-функция. Конструкция хэш-функции на основе алгоритма шифрования. Шаговая функция хэширования. Процедура вычисления значения хэш-функции. Конструкция хэш-функции на основе специализированной функции. Параметры, преобразования, функция сжатия. Процедура вычисления значения хэш-функции.

Тема 6 Применение криптографических методов и средств для обеспечения информационной безопасности

1. *Коды аутентификации сообщений.*
2. *Криптографические протоколы.*
3. *Управление ключами.*
4. *Инфраструктура открытых ключей.*
5. *Принципы разработки и модернизации СКЗИ*

Коды аутентификации сообщений. Методы построения кодов аутентификации сообщений.

Основные понятия. Цели безопасности криптографических протоколов. Протоколы передачи сообщений. Протоколы передачи ключей. Протоколы аутентификации.

Универсальная модель жизненного цикла ключа. Управление ключами. Службы управления ключами.

Назначение инфраструктуры открытых ключей. Удостоверяющий центр. Функции удостоверяющего центра. Сертификат открытого ключа.

Общие принципы построения СКЗИ. Принципы применения криптографических механизмов защиты. Принципы применения инженерно-криптографических механизмов защиты. Нормативное обеспечение КМЗИ.

Шкала и критерии оценивания по результатам самоподготовки	
Зачтено	Оценка «зачтено» выставляется студенту, если он в процессе опроса использует научную терминологию, стилистическое и логическое изложение ответа на вопросы, умеет делать выводы без существенных ошибок; владеет инструментарием изучаемой дисциплины; умеет ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им оценку
Не зачтено	Оценка «не зачтено» выставляется студенту, если он имеет недостаточно полный объем знаний в рамках опрашиваемой темы по дисциплине; использует научную терминологию, но изложение ответа на вопросы осуществляется с существенными логическими ошибками; слабо владеет инструментарием в рамках темы; не умеет ориентироваться в основных теориях, концепциях и направлениях изучаемой темы

Вопросы для подготовки к опросу

Тема 1. Основные понятия

1. Основные понятия
2. Криптографическая система. Классификация шифров

Тема 2 Основные характеристики шифров

1. Алгебраическая модель шифра. Вероятностная модель шифра. Модели открытых текстов.
2. Криптографическая стойкость шифров. Атаки на шифры
3. Теоретическая и практическая стойкость шифра
4. Имитостойкость, помехоустойчивость шифров

Тема 3 Симметричная криптография

1. Блочные и поточные шифры.
2. Принципы построения блочных шифров.
3. Сеть Фейстеля. Шифр DES.
4. Режимы работы блочных шифров
5. Поточные шифры
6. Генераторы псевдослучайных последовательностей.

Тема 4 Криптография с открытым ключом

1. Односторонние функции, функции с секретом.
2. Схемы шифрования на основе односторонних функций.
3. Схемы шифрования RSA и Эль-Гамала

Тема 5 Электронная подпись

1. Понятие электронной подписи. Способы построения электронной подписи
2. Эллиптические кривые.
3. Криптографическая хэш-функция.
4. Конструкция хэш-функций

Тема 6 Применение криптографических методов и средств для обеспечения информационной безопасности

1. Коды аутентификации сообщений.
2. Криптографические протоколы.
3. Управление ключами.
4. Инфраструктура открытых ключей.
5. Принципы разработки и модернизации СКЗИ

Шкала и критерии оценивания опроса	
Зачтено	Оценка «зачтено» выставляется студенту, если он в процессе опроса использует научную терминологию, стилистическое и логическое изложение ответа на вопросы, умеет делать выводы без существенных ошибок; владеет инструментарием изучаемой дисциплины; умеет ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им оценку
Не зачтено	Оценка «не зачтено» выставляется студенту, если он имеет недостаточно полный объем знаний в рамках опрашиваемой темы по дисциплине; использует научную терминологию, но изложение ответа на вопросы осуществляется с существенными логическими ошибками; слабо владеет инструментарием в рамках темы; не умеет ориентироваться в основных теориях, концепциях и направлениях изучаемой темы

3.1.4. Средства для промежуточной аттестации по итогам изучения дисциплины

Программа для сдачи дифференцированного зачета по учебной дисциплине

Для получения допуска к дифференцированному зачету студент должен прослушать лекции, регулярно посещать лабораторные занятия и выполнять на них задания.

Студенты, пропустившие занятия должны отработать в порядке, согласованном с преподавателем. По всем видам текущего контроля (отчеты по лабораторным заданиям) должны быть получены положительные оценки. Кроме этого, должны быть сданы задание ВАРС (презентация).

По итогам изучения дисциплины, обучающиеся проходят заключительное тестирование. Тестирование является формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин.

Тестирование осуществляется по всем темам и разделам дисциплины, включая темы, выносимые на самостоятельное изучение.

Плановая процедура проведения дифференцированного зачета

Процедура тестирования ограничена во времени и предполагает максимальное сосредоточение обучающегося на выполнении теста, содержащего несколько тестовых заданий.

Тестирование проводится в письменной форме (на бумажном носителе). Тест включает в себя 30 вопросов. Время, отводимое на выполнение теста - 30 минут. В каждый вариант теста включаются вопросы из каждого раздела дисциплины.

Бланк теста

Образец

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Омский государственный аграрный университет имени П.А. Столыпина»

Кафедра экономики, бухгалтерского учета и финансового контроля

Тестирование по итогам освоения дисциплины Б1.В.ДВ.01.01 Криптографические методы защиты информации

Для обучающихся направления подготовки 09.04.02 Информационные системы и технологии
ФИО _____ группа _____

Дата _____

Уважаемые обучающиеся!

Прежде чем приступить к выполнению заданий внимательно ознакомьтесь с инструкцией:

1. Отвечая на вопрос с выбором правильного ответа, правильный, на ваш взгляд, ответ (ответы) обведите в кружок.
2. В заданиях открытой формы впишите ответ в пропуск.
3. В заданиях на соответствие заполните таблицу.
4. В заданиях на правильную последовательность впишите порядковый номер в квадрат.
4. Время на выполнение теста – 30 минут
5. За каждый верный ответ Вы получаете 1 балл, за неверный – 0 баллов. Максимальное количество полученных баллов 30.

Желаем удачи!

Тестовые вопросы для проведения итогового контроля

1. Конфиденциальность защищаемой информации обеспечивается с помощью...
электронной подписи
шифрования
хэш-функции

2. Способность шифра противостоять попыткам противника по имитации или подмене зашифрованной информации называется
имитостойкостью
криптостойкостью
помехозащищенностью
3. Если криптоаналитик может взломать шифр, но не обладает необходимыми вычислительными ресурсами, то считается, что шифр
является практически стойким
шифр является теоретически стойким
шифр является практически имитостойким.
5. Если для шифрования и расшифрования используется один и тот же ключ, то шифр является
симметричным
ассиметричным
блочным
6. Шифры, в которых знание ключа шифрования не позволяет определить ключ расшифрования называются
поточными.
симметричными.
ассиметричными.
7. Шифры, в которых каждый символ открытого текста зашифровывается независимо от других называются
блочными.
имитозащищенными.
поточными.
8. Шифрование информации предназначено для обеспечения
целостности защищаемой информации
конфиденциальности защищаемой
информации доступности защищаемой информации
9. Исходные данные с доступным семантическим содержанием, подлежащие криптографическому преобразованию, называются
открытый текст
шифртекст
имитовставка
10. Параметр шифра, определяющий выбор конкретного варианта преобразования зашифрования или расшифрования из множества преобразований, составляющих шифр, называется...
алгоритм
шифр
ключ
11. Процесс преобразования шифртекста в открытый текст при неизвестном ключе называется...
дешифрование
зашифрование
расшифрование
12. Если за один такт шифрования преобразованию подвергается группа знаков открытого текста, то такой шифр называется
блочным
поточным
ассиметричным
13. Режим использования блочного шифра, при котором блочный шифр может использоваться как поточный называется
режим простой замены со сцеплением.
режим гаммирования с обратной связью
режим простой замены.

14. Режим простой замены заключается в обработке блоков открытого текста независимо от других
обработку блоков открытого текста в зависимости от результата зашифрования предыдущего блока
обработку блоков открытого текста
в режиме наложения гаммы

16. Шифр называется блочным, если...
за один такт шифрования преобразованию подвергается группа знаков открытого текста
за один такт шифрования преобразованию подвергается один знак открытого текста
группа знаков открытого текста преобразуется за несколько тактов шифрования

17. Если управляющая гамма поточного шифра зависит только от ключа и не зависит от
открытого текста и шифротекста, то такой шифр называется
синхронным.
самосинхронизирующимся.
независимым.

18. Достоинством поточных шифров по сравнению с блочными является
наличие открытого ключа
высокая стоимость реализации
высокая скорость работы

19. Недостатком генераторов псевдослучайных последовательностей является
сложность реализации
зависимость от параметров окружающей среды
периодичность последовательности

20. Если управляющая гамма поточного шифра зависит от ключа и от открытого текста и
шифротекста, то такой шифр называется
синхронным.
самосинхронизирующимся.
независимым.

21. Функция, для которой существует простой алгоритм вычисления значения для заданного
аргумента, и не существует простого алгоритма определения аргумента по заданному значению,
называется...
линейной
односторонней
полиномиальной

22. В основе односторонней функции схемы шифрования RSA лежит задача...
факторизации целых чисел;
дискретного логарифмирования.
поиска квадратных корней составного числа.

23. Односторонней функцией называется...
функция, для которой существует простой алгоритм вычисления значения для заданного аргумента, и
не существует простого алгоритма определения аргумента по заданному значению. функция,
сложность вычисления значения которой по заданному аргументу которой является
экспоненциальной.
функция, для которой существует простой алгоритм вычисления значения для заданного аргумента, и
алгоритм полиномиальной сложности для определения аргумента по заданному значению.

24. Функция, для которой существует полиномиальный алгоритм вычисления аргумента по заданному
значению при знании некоторого параметра, является...
односторонней функцией с секретом.
односторонней функцией.
линейной функцией.

25. Основным отличием асимметричной схемы шифрования от симметричной является...
компрометация секретного ключа приводит к нарушению конфиденциальности защищаемой
информации.
возможность зашифрования информации без наличия секретного ключа.
возможность расшифрования только при наличии секретного ключа.

26. В асимметричных схемах шифрования для расшифрования используется...
секретный ключ.
открытый ключ.
симметричный ключ.

27. Результатом процедуры проверки значения электронной подписи является...
логическое значение истина или ложь.
расшифрованное подписываемое сообщение.
секретный ключ подписывающего лица.

28. В асимметричных схемах шифрования открытый ключ используется для...
зашифрования информации.
расшифрования информации.
дешифрования информации.

29. Хэшированием называется...
процесс наложения на входной массив данных произвольной длины маскирующей гаммы фиксированной длины.
процесс преобразования открытых данных в зашифрованные.
преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины

30. Стойкостью к коллизиям первого рода называется...
свойство хэш-функции, означающее вычислительную невозможность нахождения двух произвольных сообщений, имеющих одинаковое значение хэш-кода.
свойство хэш-функции, означающее вычислительную невозможность нахождения сообщения, имеющего такое же значение хэш-кода, что и заданное сообщение.
свойство хэш-функции, означающее вычислительную невозможность нахождения сообщения по значению его хэш-кода.

31. Код аутентификации сообщения обеспечивает...
целостность и аутентификацию источника данных.
только аутентификацию источника данных.
только целостность данных.

32. Недостатком метода нумерации сообщений для защиты от атак повтора, является...
полная предсказуемость порядковых номеров.
необходимость синхронизации часов в сети.
невозможность защиты от повтора ранее переданного сообщения.

33. Криптографический протокол завершается успешно, если...
каждый из участников протокола достигает своих целей безопасности.
противник не может перехватить сообщения протокола.
достигается цель безопасности хотя бы одного из участников протокола.

34. Объект инфраструктуры открытых ключей, который авторизован создавать, подписывать и публиковать сертификаты, называется...
центр сертификации.
центр регистрации.
центр аутентификации.

35. Цифровой документ, который связывает открытый ключ с его владельцем, называется...
сертификат открытого ключа.
сертификат ключа подписи.
сертификат секретного ключа.

36. СКЗИ каких классов должны противостоять нарушителю, способному выполнять их лабораторные исследования
вне контролируемой зоны
КВ и выше
КС1 и выше
КС3 и выше

37. Что из перечисленного не подлежит поэкземплярному учету в качестве компонентов СКЗИ используемые или хранимые криптосредства
эксплуатационная и техническая документация к ним
список лиц, допущенных в помещения, где проводятся работы с использованием СКЗИ

38. В каком из вариантов все перечисленные средства относятся к шифровальным (криптографическим) средствам защиты информации конфиденциального характера:
средства имитозащиты, средства кодирования, ключевые документы
средства шифрования, средства электронной подписи, средства защиты от несанкционированного доступа
средства шифрования, средства электронной подписи, аппаратные средства обеспечения доверенной загрузки

39. Какие требования предъявляются к квалификации руководителя работ в рамках лицензируемой деятельности по обслуживанию шифровальных (криптографических) средств:

высшее профессиональное образование по направлению подготовки «Информационная безопасность» и (или) переподготовка по одной из специальностей этого направления (нормативный срок – свыше 500 аудиторных часов), а также стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 3 лет

высшее профессиональное образование по направлению подготовки «Информационная безопасность» и (или) переподготовка по одной из специальностей этого направления (нормативный срок – свыше 1000 аудиторных часов), а также стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет

высшее или среднее профессиональное образование по направлению подготовки «Информационная безопасность» и (или) переподготовка по одной из специальностей этого направления (нормативный срок – свыше 100 аудиторных часов)

40. Всякий источник сообщений можно моделировать списком допустимых (т.е. встречающихся в каких-либо текстах) k-грамм при $k=1,2,3,\dots$ Какие из приведенных k-грамм не являются допустимыми в русском языке? (несколько верных ответов)

- 1) «ШЕЕ»;
- 2) «ЖФ»;
- 3) «АУ»;
- 4) «ЮЪХ»;
- 5) «ЖЬН»

41. Что означает термин «многократное шифрование» применительно к блочным шифрам?

- 1) повторное применение алгоритма шифрования к шифртексту с теми же ключами;
- 2) шифрование одного и того же блока открытого текста несколько раз с несколькими ключами;
- 3) увеличение числа этапов шифрования открытого текста.

42. Гаммирование чаще всего осуществляется: (несколько верных ответов)

- 1) по модулю 2, если открытый текст представляется в виде бинарной последовательности;
- 2) по модулю 256, если открытый текст представляется в виде последовательности байтов;
- 3) по модулю 16, если открытый текст представлен в цифровом виде;
- 4) по модулю 10, если открытый текст представлен в виде последовательности цифр, что иногда делается в ручных системах шифрования.

43. Основой построения большинства поточных шифров являются:

- 1) генераторы псевдослучайных чисел, в частности, различные комбинации регистров сдвига;
- 2) схемы суммирования по mod 16;
- 3) таблицы подстановок.

44. Зашифрованный методом перестановки открытый текст: «Сертификаты ключей ЭЦП», при ключе длиной 7, и перестановке: {4132756}, имеет вид:

- 1) тСреиифыктал кйюечЦ Э П ;
- 2) юклчТи ЭСЦ еиртфаикт ы ;
- 3) чКилют рСекиафиЭтПы Ц .

45. Зашифровать слово «выборочность» методом перестановки с ключом {3142}:

- 1) бвоычрнотоеьс ;
- 2) ыовбрчоонсьт ;

3) вывброончотсь .

46. Зашифровать открытый текст – «field» методом Виженера, ключ – «moon» (алфавит – латиница):

- 1) rwsup
- 2) rwsyp
- 3) rvsyp

47. Частотный анализ может эффективно применяться для дешифрования шифров:

- 1) перестановки;
- 2) многоалфавитной замены;
- 3) простой замены.

48. Какие меры практической стойкости шифра относительно метода криптоанализа вы можете выделить: (несколько верных ответов)

- 1) вероятность дешифрования за время, не превосходящее T ;
- 2) среднее время, необходимое для дешифрования шифра;
- 3) скорость дешифрования шифра.

49. Какие шифры можно называть имитостойкими?

- 1) шифры, обладающие свойством противостоять разрастанию ошибок при расшифровании текстов;
- 2) шифры, обладающие свойством противостоять попыткам навязывания ложной информации.

50. Какие шифры можно называть помехоустойчивыми?

- 1) шифры, обладающие свойством противостоять разрастанию ошибок при расшифровании текстов;
- 2) шифры, обладающие свойством противостоять попыткам навязывания ложной информации.

51. Разрастание числа ошибок означает что

- 1) ошибка в одной букве, допущенная при шифровании, приводит к большому числу ошибок в расшифрованном тексте;
- 2) ошибка в одной букве, допущенная при расшифровании, приводит к последующим ошибкам.

52. Шифр считается совершенным,

- 1) если он не поддается дешифрованию;
- 2) если положение противника, стремящегося к его дешифрованию, не облегчается в результате перехвата шифртекста;
- 3) если требуются большие затраты или мала вероятность успеха его дешифрования.

54. Шифр считается практически стойким,

- 1) если он не поддается дешифрованию;
- 2) если положение противника, стремящегося к его дешифрованию, не облегчается в результате перехвата шифртекста;
- 3) если требуются большие затраты или мала вероятность успеха его дешифрования.

56. Степень неоднозначности восстановления открытого текста при дешифровании

- 1) возрастает при уменьшении материала;
- 2) снижается при уменьшении материала.

ШКАЛА И КРИТЕРИИ ОЦЕНКИ ответов на тестовые вопросы итогового контроля

- оценка «отлично» выставляется обучающемуся, если получено более 81% правильных ответов.
- оценка «хорошо» - получено от 71 до 80% правильных ответов.
- оценка «удовлетворительно» - получено от 61 до 70% правильных ответов.
- оценка «неудовлетворительно» - получено менее 61% правильных ответов.

Нормативная база проведения промежуточной аттестации обучающихся по результатам изучения дисциплины:	
1) действующее «Положение о текущем контроле успеваемости, промежуточной аттестации обучающихся по программам высшего образования (бакалавриат, специалитет, магистратура) и среднего профессионального образования в ФГБОУ ВО Омский ГАУ»	
Основные характеристики промежуточной аттестации обучающихся по итогам изучения дисциплины	
Цель промежуточной аттестации	установление уровня достижения каждым обучающимся целей и задач обучения по данной дисциплине, изложенным в п.2.2 настоящей программы
Форма промежуточной аттестации	Дифференцированный зачет
Место процедуры получения зачёта в графике учебного процесса	1) участие обучающегося в процедуре получения зачёта осуществляется за счёт учебного времени (трудоемкости), отведённого на изучение дисциплины
	2) процедура проводится в рамках ВАО, на последней неделе семестра
Основные условия получения обучающимся дифференцированного зачёта:	1) обучающийся выполнил все виды учебной работы (включая самостоятельную) и отчитался об их выполнении в сроки, установленные графиком учебного процесса по дисциплине; 2) прошёл заключительное тестирование;
Процедура получения зачёта	Представлены в Фонде оценочных средств по данной учебной дисциплине (см. – Приложение 9)
Методические материалы, определяющие процедуры оценивания знаний, умений, навыков:	

ЛИСТ РАССМОТРЕНИЙ И ОДОБРЕНИЙ

Фонд оценочных средств учебной дисциплины Б1.В.ДВ.01.01 Криптографические методы защиты информации
в составе ОПОП 09.04.02 Информационные системы и технологии

1. Рассмотрен и одобрен в качестве базового варианта:

а) На заседании обеспечивающей кафедры экономики, бухгалтерского учета и финансового контроля
протокол № 11 от 19 . 05 .2022.

Зав. кафедрой, канд. экон. наук, доцент  О.А. Блинов

б) На заседании методической комиссии по направлению 09.04.02 Информационные системы и технологии

протокол № 9 от 24 . 05 .2022.

Председатель МКН – 09.04.02, канд. экон. наук  С.А. Нардина

2. Рассмотрен и одобрен внешним экспертом

Заместитель генерального директора
ООО ФТО «Центр разработки»



 Д.В. Малыгин

ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ
к фонду оценочных средств учебной дисциплины
Б1.В.ДВ.01.01 Криптографические методы защиты информации
в составе ОПОП 09.04.02 Информационные системы и технологии

Ведомость изменений

Срок, с которого вводится изменение	Номер и основное содержание изменения и/или дополнения	Отметка об утверждении/ согласовании изменений	
		инициатор изменения	руководитель ОПОП или председатель МКН

ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ
к рабочей программе дисциплины Б1.В.ДВ.01.01 Криптографические методы защиты
информации
в составе ОПОП 09.04.02 Информационные системы и технологии

Ведомость изменений

№ п/п	Вид обновлений	Содержание изменений, вносимых в ОПОП	Обоснование изменений
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			