

Документ подписан простой электронной подписью

Информация о владельце:

ФИС: Комарова Светлана Юриевна

Должность: Проректор по образовательной деятельности

Дата подписания: 18.05.2023 12:51:45

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

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ  
по освоению учебной дисциплины**

**Б1.В.ДВ.01.01 Криптографические методы защиты информации**

**Направленность (профиль) «Информационные системы и технологии»**

|                                                   |                                                                   |
|---------------------------------------------------|-------------------------------------------------------------------|
| Обеспечивающая преподавание дисциплины<br>кафедра | Кафедра экономики, бухгалтерского учета и<br>финансового контроля |
| Разработчик,<br>канд. экон. наук, доцент          | А.А. Ремизова                                                     |
| Омск 2022                                         |                                                                   |

## СОДЕРЖАНИЕ

|                                                                                               |    |
|-----------------------------------------------------------------------------------------------|----|
|                                                                                               | 3  |
| Введение                                                                                      | 4  |
| 1. Место учебной дисциплины в подготовке                                                      | 8  |
| 2. Структура учебной работы, содержание и трудоёмкость основных элементов дисциплины          | 8  |
| 2.1. Организационная структура, трудоемкость и план изучения дисциплины                       | 9  |
| 2.2. Содержание дисциплины по разделам                                                        | 11 |
| 3. Общие организационные требования к учебной работе обучающегося, условия допуска к экзамену | 11 |
| 3.1. Организация занятий и требования к учебной работе обучающегося                           | 11 |
| 3.2. Условия допуска к зачету по дисциплине                                                   | 12 |
| 4. Лекционные занятия                                                                         | 13 |
| 5. Лабораторные занятия по курсу и подготовка обучающегося к ним                              | 15 |
| 6. Общие методические рекомендации по изучению отдельных разделов дисциплины                  | 16 |
| 7. Общие методические рекомендации по оформлению и выполнению отдельных видов ВАРС            | 16 |
| 7.1. Рекомендации по подготовке презентации                                                   | 17 |
| 7.2. Рекомендации по самостоятельному изучению тем                                            | 21 |
| 8. Текущий (внутрисеместровый) контроль хода и результатов учебной работы обучающегося        | 21 |
| 8.1. Вопросы для входного контроля                                                            | 22 |
| 8.2. Текущий контроль успеваемости                                                            | 23 |
| 9. Промежуточная (семестровая) аттестация                                                     | 23 |
| 9.1 Нормативная база проведения промежуточной аттестации по результатам изучения дисциплины   | 23 |
| 9.2. Процедура проведения зачета                                                              | 24 |
| 9.4 Перечень примерных тестовых вопросов к зачету                                             | 26 |
| 10. Учебно-информационные источники для изучения дисциплины                                   | 26 |

## **ВВЕДЕНИЕ**

1. Настоящее издание является основным организационно-методическим документом учебно-методического комплекса по дисциплине в составе основной профессиональной образовательной программы высшего образования (ОПОП ВО). Оно предназначено стать для них методической основой по освоению данной дисциплины.

2. Содержательной основой для разработки настоящих методических указаний послужила Рабочая программа дисциплины, утвержденная в установленном порядке.

3. Методические аспекты развиты в учебно-методической литературе и других разработках, входящих в состав УМК по данной дисциплине.

4. Доступ обучающихся к электронной версии Методических указаний по изучению дисциплины, обеспечен в электронной информационно-образовательной среде университета.

При этом в электронную версию могут быть внесены текущие изменения и дополнения, направленные на повышение качества настоящих методических указаний.

### **Уважаемые обучающиеся!**

Приступая к изучению новой для Вас учебной дисциплины, начните с вдумчивого прочтения разработанных для Вас кафедрой специальных методических указаний. Это поможет Вам вовремя понять и правильно оценить ее роль в Вашем образовании.

Ознакомившись с организационными требованиями кафедры по этой дисциплине и соизмерив с ними свои силы, Вы сможете сделать осознанный выбор собственной тактики и стратегии учебной деятельности, уберечь самих себя от неразумных решений по отношению к ней в начале семестра, а не тогда, когда уже станет поздно. Используя эти указания, Вы без дополнительных осложнений подойдете к промежуточной аттестации по этой дисциплине. Успешность аттестации зависит, прежде всего, от Вас. Ее залог – ритмичная, целенаправленная, вдумчивая учебная работа, в целях обеспечения которой и разработаны эти методические указания.

## 1. Место учебной дисциплины в подготовке выпускника

Учебная дисциплина относится к дисциплинам ОПОП университета, состав которых определяется вузом и требованиями ФГОС.

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

### **В ходе освоения дисциплины обучающийся должен:**

*иметь целостное представление* о методологии и практическом применении криптографической защиты информации в организациях;

*владеть:* навыками определения криптографической стойкости шифрсистем; навыками обоснования выбора криптографических средств для защиты информации;

*знать:* основания криптографической защиты информации в организации; основные понятия и требования криптографической защиты информации;

*уметь:* выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации; выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации.

### 1.1. Перечень компетенций с указанием этапов их формирования в результате освоения учебной дисциплины:

| 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 <sup>пк-1.1</sup> 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 |
|                                                              |                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                 |

|  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                    |                                                                                                                                                                                                                                                  |                                                                                                                                                                                                       |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p><b>ИД-2<sub>ПК-2.2</sub></b><br/> 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</p> | <p>аспекты анализа профессиональной информации; новые научные принципы и методы исследований; математические модели процессов и объектов при решении задач криптографической защиты информации</p> | <p>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</p> | <p>всестороннего анализа профессиональной информации; применения на практике новых научных принципов и методов исследований; разработки и применения математического моделирования в криптографии</p> |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 1.2. 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 <sub>ПК2.1</sub> . 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 изученным 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 |                                                                                                                                                                                                    |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                     |                                   |                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                    |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | ИД-2 <sub>пк.2.2</sub> 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 | Наличие навыков (владение опытом) | Применения 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 | Отсутствуют навыки применения 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 | Поверхностно владеет навыками применения 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 | Владеет основными навыками применения 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 | Свободно владеет навыками применения 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 |                                                                                                                                                                                                    |
|  |                                                                                                                                                                                                                                                                                                                                                                                                                     | 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 самостоятельным 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 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 информации; применения на практике новых научных принципов и методов исследований; разработки и применения математического моделирования в криптографии                                                                                                                           |                                                                                                                                                                                                    |

## 2. Структура учебной работы, содержание и трудоёмкость основных элементов дисциплины

### 2.1. Организационная структура, трудоёмкость и план изучения 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<br>(начитка) | 2 курс     |
| <b>1. Аудиторные занятия, всего</b>                                                                                                                                                                                                                                                              | <b>36</b>               | <b>2</b>            | <b>12</b>  |
| – лекции                                                                                                                                                                                                                                                                                         | 16                      | 2                   | 4          |
| – практические занятия (включая семинары)                                                                                                                                                                                                                                                        | 20                      | -                   | 8          |
| – лабораторные работы                                                                                                                                                                                                                                                                            | -                       | -                   | -          |
| <b>2. Внеаудиторная академическая работа</b>                                                                                                                                                                                                                                                     | <b>72</b>               | <b>34</b>           | <b>56</b>  |
| <b>2.1 Фиксированные виды внеаудиторных самостоятельных работ:</b>                                                                                                                                                                                                                               | <b>10</b>               | <b>-</b>            | <b>10</b>  |
| Выполнение и сдача/защита индивидуального/группового задания в виде**                                                                                                                                                                                                                            |                         |                     |            |
| – презентации                                                                                                                                                                                                                                                                                    | 10                      | -                   | 10         |
| <b>2.2 Самостоятельное изучение тем/вопросов программы</b>                                                                                                                                                                                                                                       | <b>30</b>               | <b>34</b>           | <b>30</b>  |
| <b>2.3 Самоподготовка к аудиторным занятиям</b>                                                                                                                                                                                                                                                  | <b>20</b>               |                     | <b>10</b>  |
| <b>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):</b>                                                                                                          | <b>12</b>               |                     | <b>6</b>   |
| <b>3. Получение дифференцированного зачёта по итогам освоения дисциплины</b>                                                                                                                                                                                                                     | <b>+</b>                | <b>-</b>            | <b>4</b>   |
| <b>ОБЩАЯ трудоемкость дисциплины:</b>                                                                                                                                                                                                                                                            | <b>Часы</b>             | <b>108</b>          | <b>108</b> |
|                                                                                                                                                                                                                                                                                                  | <b>Зачетные единицы</b> | <b>3</b>            | <b>3</b>   |
| <b>Примечание:</b><br>* – <b>семестр</b> – для очной и очно-заочной формы обучения, <b>курс</b> – для заочной формы обучения;<br>** – КР/КП, реферата/эссе/презентации, контрольной работы (для обучающихся заочной формы обучения), расчетно-графической (расчетно-аналитической) работы и др.; |                         |                     |            |



## 2.2. Укрупнённая содержательная структура учебной дисциплины и общая схема её реализации в учебном процессе

| Номер и наименование<br>раздела дисциплины.<br>Укрупненные темы раздела |                                                                                                    | Трудоемкость раздела и ее распределение<br>по видам учебной работы, час. |                   |        |                             |              |       | Формы текущего<br>контроля успеваемости и<br>промежуточной<br>аттестации | №№ компетенций, на<br>формирование которых<br>ориентирован раздел                                                                                                                                 |                       |
|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|-------------------|--------|-----------------------------|--------------|-------|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                                                                         |                                                                                                    | общая                                                                    | Аудиторная работа |        |                             |              | ВАРС  |                                                                          |                                                                                                                                                                                                   |                       |
|                                                                         |                                                                                                    |                                                                          | всего             | лекции | занятия                     |              | всего |                                                                          |                                                                                                                                                                                                   | фиксированные<br>виды |
|                                                                         |                                                                                                    |                                                                          |                   |        | практические<br>(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<br>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<br>раздела дисциплины.<br>Укрупненные темы раздела |                                                                                                    | Трудоемкость раздела и ее распределение<br>по видам учебной работы, час. |                   |        |                             |              |       | Формы текущего<br>контроля успеваемости и<br>промежуточной<br>аттестации | №№ компетенций, на<br>формирование которых<br>ориентирован раздел                                                                                                                                 |                       |
|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|-------------------|--------|-----------------------------|--------------|-------|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                                                                         |                                                                                                    | общая                                                                    | Аудиторная работа |        |                             |              | ВАРС  |                                                                          |                                                                                                                                                                                                   |                       |
|                                                                         |                                                                                                    |                                                                          | всего             | лекции | занятия                     |              | всего |                                                                          |                                                                                                                                                                                                   | фиксированные<br>виды |
|                                                                         |                                                                                                    |                                                                          |                   |        | практические<br>(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<br>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                                                                                                                                                                                                 |                       |

### **3. Общие организационные требования к учебной работе обучающегося**

#### **3.1. Организация занятий и требования к учебной работе обучающегося**

Организация занятий по дисциплине носит циклический характер. По трем разделам предусмотрена взаимоувязанная цепочка учебных работ: лекция – самостоятельная работа обучающихся (аудиторная и внеаудиторная). На занятиях студенческая группа получает задания и рекомендации.

Для своевременной помощи обучающимся при изучении дисциплины кафедрой организуются индивидуальные и групповые консультации, устанавливается время приема выполненных работ.

Учитывая статус дисциплины к её изучению предъявляются следующие организационные требования;:

- обязательное посещение обучающимся всех видов аудиторных занятий;
- ведение конспекта в ходе лекционных занятий;
- качественная самостоятельная подготовка к практическим занятиям, активная работа на них;
- активная, ритмичная самостоятельная аудиторная и внеаудиторная работа обучающегося в соответствии с планом-графиком, представленным в таблице 2.4; своевременная сдача преподавателю отчетных документов по аудиторным и внеаудиторным видам работ;
- в случае наличия пропущенных обучающимся занятий, необходимо получить консультацию по подготовке и оформлению отдельных видов заданий.

Для успешного освоения дисциплины, обучающемуся предлагаются учебно-информационные источники в виде учебной, учебно-методической литературы по всем разделам.

#### **3.2 Условия допуска к дифференцированному зачету**

Зачет является формой контроля, который выставляется обучающемуся согласно «Положения о текущем контроле успеваемости, промежуточной аттестации обучающихся по программам высшего образования (бакалавриат, специалитет, магистратура) и среднего профессионального образования в ФГБОУ ВО Омский ГАУ», выполнившему в полном объеме все перечисленные в п.2-3 требования к учебной работе, прошедший все виды тестирования, выполнения презентации с положительной оценкой. В случае не полного выполнения указанных условий по уважительной причине, обучающемуся могут быть предложены индивидуальные задания по пропущенному учебному материалу.

#### 4. Лекционные занятия

Для изучающих дисциплину читаются лекции в соответствии с планом, представленным в таблице 3.

Таблица 3 - Лекционный курс

| №                                                                                                                                                                                                 |                                                  | 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                                                                                                                                                              |                                                  |                                                                                                   |                               |               | х                                        |
| 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. |                                                  |                                                                                                   |                               |               |                                          |

## 5. Практические занятия по дисциплине и подготовка к ним

Практические занятия по курсу проводятся в соответствии с планом, представленным в таблице 4.

Таблица 4 - Примерный тематический план практических занятий по разделам учебной дисциплины

| №                                                                                                                                                                                                                                                                              |                                                     | Тема занятия /<br>Примерные вопросы на обсуждение<br>(для семинарских занятий)                                   | Трудоемкость по<br>разделу, час. |                  | Используемые<br>интерактивные<br>формы** | Связь<br>занятия с<br>ВАРС* |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------|------------------------------------------|-----------------------------|
| раздела<br>(модуля)                                                                                                                                                                                                                                                            | занятия                                             |                                                                                                                  | очная<br>форма                   | заочная<br>форма |                                          |                             |
| 1                                                                                                                                                                                                                                                                              | 1                                                   | <b>Тема 1. Основные понятия</b>                                                                                  |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                |                                                     | 1 Основные понятия.                                                                                              | 2                                | -                | Семинар-<br>беседа                       | ОСП                         |
|                                                                                                                                                                                                                                                                                |                                                     | 2 Криптографическая система.<br>Классификация шифров                                                             |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                | 2                                                   | <b>Тема 2 Основные характеристики шифров</b>                                                                     |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                |                                                     | 1 Алгебраическая модель шифра.<br>Вероятностная модель шифра. Модели<br>открытых текстов.                        | 2                                | 1                | -                                        | ОСП                         |
|                                                                                                                                                                                                                                                                                |                                                     | 2 Криптографическая стойкость шифров.<br>Атаки на шифры                                                          |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                |                                                     | 3 Теоретическая и практическая стойкость<br>шифра                                                                |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                | 4 Имитостойкость, помехоустойчивость<br>шифров      |                                                                                                                  |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                | 3                                                   | <b>Тема 3 Симметричная криптография</b>                                                                          |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                |                                                     | 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<br>последовательностей |                                                                                                                  |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                | 4                                                   | <b>Тема 4 Криптография с открытым ключом</b>                                                                     |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                |                                                     | 1 Односторонние функции, функции с<br>секретом                                                                   | 4                                | 2                | -                                        | ОСП                         |
|                                                                                                                                                                                                                                                                                |                                                     | 2 Схемы шифрования на основе<br>односторонних функций                                                            |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                | 3 Схемы шифрования RSA и Эль-Гамала                 |                                                                                                                  |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                | 5                                                   | <b>Тема 5 Электронная подпись</b>                                                                                |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                |                                                     | 1 Понятие электронной подписи. Способы<br>построения электронной подписи                                         | 4                                | 2                | -                                        | ОСП                         |
|                                                                                                                                                                                                                                                                                |                                                     | 2 Эллиптические кривые.                                                                                          |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                |                                                     | 3 Криптографическая хэш-функция                                                                                  |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                | 4 Конструкция хэш-функций.                          |                                                                                                                  |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                | 6                                                   | <b>Тема 6 Применение криптографических<br/>методов и средств для обеспечения<br/>информационной безопасности</b> |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                |                                                     | 1 Коды аутентификации сообщений                                                                                  | 4                                | 1                | -                                        | ОСП                         |
|                                                                                                                                                                                                                                                                                |                                                     | 2 Криптографические протоколы                                                                                    |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                |                                                     | 3 Управление ключами                                                                                             |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                |                                                     | 4 Инфраструктура открытых ключей                                                                                 |                                  |                  |                                          |                             |
|                                                                                                                                                                                                                                                                                |                                                     | 5 Принципы разработки и модернизации<br>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                                                                                                                                                                                                                                                       |                                                     |                                                                                                                  |                                  |                  |                                          |                             |
| <b>* Условные обозначения:</b><br><b>ОСП</b> – предусмотрена обязательная самоподготовка к занятию; <b>УЗ СРС</b> – на занятии выдается задание на конкретную ВАРС;<br><b>ПР СРС</b> – занятие содержательно базируется на результатах выполнения обучающимся конкретной ВАРС. |                                                     |                                                                                                                  |                                  |                  |                                          |                             |
| <b>**</b> 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.

Подготовка обучающихся к практическим занятиям осуществляется с учетом общей структуры учебного процесса. На лабораторных занятиях осуществляется входной и текущий аудиторный контроль в виде опроса по основным понятиям дисциплины.

Подготовка к практическим занятиям подразумевает выполнение домашнего задания к очередному занятию по заданиям преподавателя, выдаваемым в конце предыдущего занятия.

Для осуществления работы по подготовке к занятиям, необходимо ознакомиться с методическими указаниями по дисциплине, внимательно ознакомиться с литературой и электронными ресурсами, с рекомендациями по подготовке, вопросами для самоконтроля.

## **6. Общие методические рекомендации по изучению отдельных разделов дисциплины**

При изучении конкретного раздела дисциплины, из числа вынесенных на лекционные и практические занятия, обучающемуся следует учитывать изложенные ниже рекомендации. Обратите на них особое внимание при подготовке к аттестации.

Работа по теме прежде всего предполагает ее изучение по учебнику или пособию. Следует обратить внимание на то, что в любой теории, есть либо неубедительные, либо чересчур абстрактные, либо сомнительные положения. Поэтому необходимо вырабатывать самостоятельные суждения, дополняя их аргументацией, что и следует демонстрировать на семинарах. Для выработки самостоятельного суждения важным является умение работать с научной литературой. Поэтому работа по теме кроме ее изучения по учебнику, пособию предполагает также поиск по теме научных статей в научных журналах информационным технологиям и системам. Выбор статьи, относящейся к теме, лучше делать по последним в году номерам, где приводится перечень статей, опубликованных за год.

Самостоятельная подготовка предполагает использование ряда методов.

1. Конспектирование. Конспектирование позволяет выделить главное в изучаемом материале и выразить свое отношение к рассматриваемой автором проблеме.

Техника записей в конспекте индивидуальна, но есть ряд правил, которые могут принести пользу его составителю: начиная конспект, следует записать автора изучаемого произведения, его название, источник, где оно опубликовано, год издания. Порядок конспектирования:

- а) внимательное чтение текста;
- б) поиск в тексте ответов на поставленные в изучаемой теме вопросы;
- в) краткое, но четкое и понятное изложение текста;
- г) выделение в записи наиболее значимых мест;
- д) запись на полях возникающих вопросов, понятий, категорий и своих мыслей.

2. Записи в форме тезисов, планов, аннотаций, формулировок определений. Все перечисленные формы помогают быстрой ориентации в подготовленном материале, подборе аргументов в пользу или против какого-либо утверждения.

3. Словарь понятий и категорий. Составление словаря помогает быстрее осваивать новые понятия и категории, увереннее ими оперировать. Подобный словарь следует вести четко, разборчиво, чтобы удобно было им пользоваться. Из приведенного в УМК глоссария нужно к каждому семинару выбирать понятия, относящиеся к изучаемой теме, объединять их логической схемой в соответствии с вопросами семинарского занятия.

## 7. Общие методические рекомендации по оформлению и выполнению отдельных видов ВАРС

### 7.1 Общие рекомендации по подготовке презентации

#### Процедура выбора темы обучающимся

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

| <b>Шкала и критерии оценивания электронной презентации</b> |                                                                                                                                                                                                                                                       |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Отлично</b>                                             | Оценка «отлично» по презентации присваивается за глубокое раскрытие темы, качественное оформление работы, содержательность презентации, за понимание студентом отраженного в презентации материала.                                                   |
| <b>Хорошо</b>                                              | 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                               |
| <b>Удовлетворительно</b>                                   | 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                           |
| <b>Неудовлетворительно</b>                                 | 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 |



## 7.2. Рекомендации по самостоятельному изучению тем

### 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 развёрнутый план (конспект) изложения темы;
- подготовиться к опросу по теме.

| Шкала и критерии оценивания опроса |                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Зачтено</b>                     | 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.                        |
| <b>Не зачтено</b>                  | 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. |

### 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.

| <b>Шкала и критерии оценивания по результатам самоподготовки</b> |                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Зачтено</b>                                                   | 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                       |
| <b>Не зачтено</b>                                                | 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 |

## **8. Входной контроль и текущий (внутрисеместровый) контроль хода и результатов учебной работы**

### **8.1 Вопросы для входного контроля**

#### **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  
Snannable

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.

#### **8.2. Текущий контроль успеваемости**

В течение семестра, проводится текущий контроль успеваемости по дисциплине, к которому обучающийся должен быть подготовлен.

Отсутствие пропусков аудиторных занятий, активная работа на практических занятиях, общее выполнение графика учебной работы являются основанием для получения положительной оценки по текущему контролю.

## 9. Промежуточная (семестровая) аттестация по курсу

| <b>9.1 Основные характеристики промежуточной аттестации обучающихся по итогам изучения дисциплины</b> |                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Цель промежуточной аттестации -</b>                                                                | установление уровня достижения каждым обучающимся целей и задач обучения по данной дисциплине, изложенным в п.2.2 настоящей программы                                                                             |
| <b>Форма промежуточной аттестации -</b>                                                               | Дифференцированный зачет                                                                                                                                                                                          |
| <b>Место процедуры получения зачёта в графике учебного процесса</b>                                   | 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                                                                                                                                                |
| <b>Основные условия получения обучающимся дифференцированного зачёта:</b>                             | 1) обучающийся выполнил все виды учебной работы (включая самостоятельную) и отчитался об их выполнении в сроки, установленные графиком учебного процесса по дисциплине;<br>2) прошёл заключительное тестирование; |
| <b>Процедура получения дифференцированного зачёта -</b>                                               | Представлены в Фонде оценочных средств по данной учебной дисциплине (см. – Приложение 9)                                                                                                                          |
| <b>Методические материалы, определяющие процедуры оценивания знаний, умений, навыков:</b>             |                                                                                                                                                                                                                   |

## 9.2. ПРОЦЕДУРА ПРОВЕДЕНИЯ ДИФФЕРЕНЦИРОВАННОГО ЗАЧЕТА

### Программа для сдачи зачета по учебной дисциплине

Для получения допуска к зачету студент должен прослушать лекции, регулярно посещать практические 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 сдано 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!

### Примерные 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.
1. Если для шифрования и расшифрования используется один и тот же ключ, то шифр является  
симметричным  
асимметричным  
блочным
6. Шифры, в которых знание ключа шифрования не позволяет определить ключ расшифрования называются  
поточными.  
симметричными.  
ссимметричными.



**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.

## 10. 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 (УМКД), соответствующий данной рабочей программе и прилагаемый к ней. При разработке УМКД кафедра руководствуется установленными университетом требованиями к его структуре, содержанию и оформлению. В состав УМКД входят перечисленные ниже и другие источники учебной и учебно-методической информации, средства наглядности.

Предусмотренная рабочей учебной программой учебная и учебно-методическая литература размещена в фондах НСХБ и/или библиотеке обеспечивающей преподавание кафедры.

Учебно-методические материалы для обеспечения самостоятельной работы обучающихся размещены в электронном виде в ИОС ОмГАУ-Moodle (URL: <http://do.omgau.ru>), где:

- обучающийся имеет возможность работать с изданиями ЭБС и электронными образовательными ресурсами, указанными в рабочей программе дисциплины, отправлять из дома выполненные задания и отчёты, задавать на форуме вопросы преподавателю или сокурсникам;
- преподаватель имеет возможность проверять задания и отчёты, оценивать работы, давать рекомендации, отвечать на вопросы (обратная связь), вести мониторинг выполнения заданий (освоения изучаемых разделов) по конкретному студенту и группе в целом, корректировать (в случае необходимости) учебно-методические материалы.

| <b>ПЕРЕЧЕНЬ<br/>литературы, рекомендуемой для изучения дисциплины<br/>Б1.В.ДВ.01.01 Криптографические методы защиты информации</b>                                                                                                                                                                                                                                                                                                               |                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| <b>Автор, наименование, выходные данные</b>                                                                                                                                                                                                                                                                                                                                                                                                      | <b>Доступ</b>                                       |
| 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: <a href="https://znanium.com/catalog/product/1215714">https://znanium.com/catalog/product/1215714</a> . – Режим доступа: по подписке.                             | <a href="http://znanium.com">http://znanium.com</a> |
| 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: <a href="https://znanium.com/catalog/product/1052206">https://znanium.com/catalog/product/1052206</a> . – Режим доступа: по подписке.                                     | <a href="http://znanium.com">http://znanium.com</a> |
| 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: <a href="https://znanium.com/catalog/product/1817522">https://znanium.com/catalog/product/1817522</a> . – Режим доступа: по подписке.                                                                                                                               | <a href="http://znanium.com">http://znanium.com</a> |
| 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: <a href="https://znanium.com/catalog/product/1167736">https://znanium.com/catalog/product/1167736</a> . – Режим доступа: по подписке.                                                                  | <a href="http://znanium.com">http://znanium.com</a> |
| 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: <a href="https://znanium.com/catalog/product/1178150">https://znanium.com/catalog/product/1178150</a> . – Режим доступа: по подписке.                                                                                                                | <a href="http://znanium.com">http://znanium.com</a> |
| 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: <a href="https://znanium.com/catalog/product/1212394">https://znanium.com/catalog/product/1212394</a> . – Режим доступа: по подписке. | <a href="http://znanium.com">http://znanium.com</a> |
| 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: <a href="https://znanium.com/catalog/product/1213114">https://znanium.com/catalog/product/1213114</a> . – Режим доступа: по подписке.                                                                                | <a href="http://znanium.com">http://znanium.com</a> |
| Информационные технологии и вычислительные системы : ежекварт. науч. журн. – Москва : Российская академия наук, 1995 – . – Выходит 4 раза в год. – ISSN 2071-8632. – Текст : непосредственный.                                                                                                                                                                                                                                                   | НСХБ                                                |