|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  Приложение к ОПОП по направлению подготовки 09.03.03 Прикладная информатика (высшее образование - бакалавриат), Направленность (профиль) программы «Проектирование, разработка, внедрение и эксплуатация информационных систем», утв. приказом ректора ОмГА от 25.03.2024 №34. |
|  |  |  |  |  |  |  |  |  |  |
|  Частное учреждение образовательная организация высшего образования «Омская гуманитарная академия» |
|  Кафедра "Информатики, математики и естественнонаучных дисциплин" |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  УТВЕРЖДАЮ |
|  |  |  |  |  |  |  |  |  Ректор, д.фил.н., профессор  \_\_\_\_\_\_\_\_\_\_\_\_\_\_А.Э. Еремеев |
|  |  |  |  |  |  |  |  |  25.03.2024 г. |
|  |  |  |  |  |  |  |  |  |  |
|  РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ |
|  |  |  |  |  Системы классификации и кодирования информации К.М.02.ДВ.04.02 |  |
|  по программе бакалавриата |
|  |  |  Направление подготовки: 09.03.03 Прикладная информатика (высшее образование - бакалавриат) Направленность (профиль) программы: «Проектирование, разработка, внедрение и эксплуатация информационных систем» Области профессиональной деятельности и (или) сферы профессиональной деятельности. |
|  Области профессиональной деятельности. 06.СВЯЗЬ, ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ. |
|  *Профессиональные стандарты:* |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  **06** |  СВЯЗЬ, ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ |
|  **06.001** |  ПРОГРАММИСТ |
|  **06.015** |  СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННЫМ СИСТЕМАМ |
|  **06.017** |  РУКОВОДИТЕЛЬ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ |
|  **06.022** |  СИСТЕМНЫЙ АНАЛИТИК |
|  |  |  |  |  |  |  |  |  |  |
|  *Типы задач профессиональной деятельности:* |  производственно-технологический, проектный |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  **Для обучающихся:** |
|  |
|  |  очной формы обучения 2024 года набора  на 2024-2025 учебный год  Омск, 2024 |

|  |
| --- |
|  Составитель:  к.т.н., доцент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Червенчук И.В./  Рабочая программа дисциплины одобрена на заседании кафедры «Информатики, математики и естественнонаучных дисциплин» Протокол от 22.03.2024 г. №8 |
|  Зав. кафедрой, профессор, к.п.н. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Лучко О.Н./ |

|  |
| --- |
|  **СОДЕРЖАНИЕ** |
|  |
|  1 Наименование дисциплины  2 Формируемые у обучающегося компетенции и запланированные результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций  3 Указание места дисциплины в структуре образовательной программы  4 Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся  5 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий  6 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине  7 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины  8 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины  9 Методические указания для обучающихся по освоению дисциплины  10 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем  11 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине  12 Фонд оценочных средств (Приложения 1-5)  |

|  |
| --- |
|  ***Рабочая программа дисциплины составлена в соответствии с:*** |
|  - Федеральным законом Российской Федерации от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»; - Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.03 Прикладная информатика, утвержденного Приказом Министерства образования и науки РФ от 19.09.2017 г. № 922 «Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика» (далее - ФГОС ВО, Федеральный государственный образовательный стандарт высшего образования);  - Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры, утвержденным приказом Минобрнауки России от 05.04.2017 № 301 (зарегистрирован Минюстом России 14.07.2017, регистрационный № 47415, (далее - Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования). Рабочая программа дисциплины составлена в соответствии с локальными нормативными актами ЧУОО ВО «Омская гуманитарная академия» (далее – Академия; ОмГА): - «Положением о порядке организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам магистратуры», одобренным на заседании Ученого совета от 28.08.2017 (протокол заседания № 1), Студенческого совета ОмГА от 28.08.2017 (протокол заседания № 1), утвержденным приказом ректора от 28.08.2017 №37; - «Положением о порядке разработки и утверждения образовательных программ», одобренным на заседании Ученого совета от 28.08.2017 (протокол заседания № 1), Студенческого совета ОмГА от 28.08.2017 (протокол заседания № 1), утвержденным приказом ректора от 28.08.2017 №37; - «Положением о практической подготовке обучающихся», одобренным на заседании Ученого совета от 28.09.2020 (протокол заседания №2), Студенческого совета ОмГА от 28.09.2020 (протокол заседания №2); - «Положением об обучении по индивидуальному учебному плану, в том числе, ускоренном обучении, студентов, осваивающих основные профессиональные образовательные программы высшего образования - программы бакалавриата, магистратуры», одобренным на заседании Ученого совета от 28.08. 2017 (протокол заседания № 1), Студенческого совета ОмГА от 28.08.2017 (протокол заседания № 1), утвержденным приказом ректора от 28.08.2017 №37; - «Положением о порядке разработки и утверждения адаптированных образовательных программ высшего образования – программ бакалавриата, программам магистратуры для лиц с ограниченными возможностями здоровья и инвалидов», одобренным на заседании Ученого совета от 28.08.2017 (протокол заседания № 1), Студенческого совета ОмГА от 28.08.2017 (протокол заседания № 1), утвержденным приказом ректора от 28.08.2017 №37; - учебным планом по основной профессиональной образовательной программе высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика направленность (профиль) программы: «Проектирование, разработка, внедрение и эксплуатация информационных систем»; форма обучения – очная на 2024-2025 учебный год, утвержденным приказом ректора от 25.03.2024 № 34; Возможность внесения изменений и дополнений в разработанную Академией образовательную программу в части рабочей программы дисциплины «Системы классификации и кодирования информации» в течение 2024-2025 учебного года: при реализации образовательной организацией основной профессиональной образовательной программы высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика; очная форма обучения в соответствии с требованиями законодательства Российской Федерации в сфере образования, Уставом Академии, локальными нормативными актами образовательной организации при |

|  |
| --- |
|  согласовании со всеми участниками образовательного процесса. |
|  |
|  **1. Наименование дисциплины: К.М.02.ДВ.04.02 «Системы классификации и кодирования информации».** **2. Формируемые у обучающегося компетенции и запланированные результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций:** |
|  |
|  В соответствии с требованиями Федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика, утвержденного Приказом Министерства образования и науки РФ от 19.09.2017 г. № 922 «Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика» при разработке основной профессиональной образовательной программы (далее - ОПОП) бакалавриата определены возможности Академии в формировании компетенций выпускников соотнесенные с индикаторами достижения компетенций. Процесс изучения дисциплины «Системы классификации и кодирования информации» направлен на формирование у обучающегося компетенций и запланированных результатов обучения, соотнесенных с индикаторами достижения компетенций: |
|  **Код компетенции: ПК-11** **Способность принимать участие во внедрении информационных систем** |
|  **Индикаторы достижения компетенции:** |
|  ИПК-11.1 знать основные возможности ИС, особенности предметной области автоматизации, устройство и функционирование современных ИС |
|  ИПК-11.2 знать архитектуру, устройство и функционирование вычислительных систем, основы современных систем управления базами данных |
|  ИПК-11.3 знать современные стандарты информационного взаимодействия систем, функциональные возможности программных средств и платформ инфраструктуры информационных технологий организаций |
|  ИПК-11.4 уметь применять современные методики тестирования разрабатываемых ИС: инструменты и методы модульного тестирования, инструменты и методы тестирования нефункциональных и функциональных характеристик ИС |
|  ИПК-11.5 уметь применять современный отечественный и зарубежный опыт в профессиональной деятельности |
|  ИПК-11.6 уметь проектировать архитектуру ИС, проверять (верифицировать) архитектуру ИС |
|  ИПК-11.7 владеть инструментами и методами проектирования архитектуры ИС, навыками работы с инструментами и методами верификации архитектуры ИС |
|  ИПК-11.8 владеть методами проверки результатов исправления дефектов и несоответствий в коде ИС и документации к ИС, навыками работы с источники информации, необходимой для профессиональной деятельности |
|  ИПК-11.9 владеть современными инструментами и методами управления организацией, в том числе методами планирования деятельности, распределения поручений, контроля исполнения, принятия решений |
|  ИПК-11.10 владеть методами ведения документооборота в организациях, инструментами и методами определения финансовых и производственных показателей деятельности организаций |
|  |
|  **Код компетенции: ПК-9** **Способность проводить тестирование компонентов программного обеспечения ИС** |
|  **Индикаторы достижения компетенции:** |

|  |
| --- |
|  ИПК-9.1 знать предметную область автоматизации |
|  ИПК-9.2 знать инструменты и методы тестирования, возможности ИС |
|  ИПК-9.3 знать источники информации, необходимой для профессиональной деятельности |
|  ИПК-9.4 уметь разрабатывать регламенты тестирования |
|  ИПК-9.5 уметь применять диаграмму Ганта, метод «набегающей волны», типы зависимостей между работами |
|  ИПК-9.6 уметь применять современный отечественный и зарубежный опыт в профессиональной деятельности |
|  ИПК-9.7 владеть навыками оценки (прогнозирование) бюджетов и графиков: метод аналогов, экспертные оценки |
|  ИПК-9.8 владеть методами управления содержанием проекта: документирование требований, анализ продукта, модерируемые совещания |
|  ИПК-9.9 владеть методами управления качеством: контрольные списки, верификация, валидация (приемо-сдаточные испытания) |
|  ИПК-9.10 владеть методами управления коммуникациями в проекте: базовые навыки управления (в том числе проведение презентаций, проведение переговоров, публичные выступления) |
|  |  |  |  |
|  **3. Указание места дисциплины в структуре образовательной программы** |
|   Дисциплина К.М.02.ДВ.04.02 «Системы классификации и кодирования информации» относится к обязательной части, является дисциплиной Блока Б1. «Дисциплины (модули)». Модуль "Разработка информационных систем" основной профессиональной образовательной программы высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика. |
|  |  |  |  |
|  Содержательно-логические связи |  Коды форми- руемых компе- тенций |
|  Наименование дисциплин, практик |
|  на которые опирается содержание данной учебной дисциплины |  для которых содержание данной учебной дисциплины является опорой |
|  Программная инженерия Проектирование информационных систем Высокоуровневые методы информатики и программирования Алгоритмизация и программирование Базы данных Интернет- программирование |  Интеллектуальные информационные системы Информационные технологии в бизнесе Производственная практика(преддипломная практика Выполнение и защита выпускной квалификационной работы) |  ПК-9, ПК-11 |
|  |  |  |  |
|  **4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся** |
|  Объем учебной дисциплины – 2 зачетных единиц – 72 академических часов Из них: |
|  |  |  |  |
|  Контактная работа |  36 |
|  *Лекций* |  18 |
|  *Лабораторных работ* |  0 |
|  *Практических занятий* |  18 |
|  *Семинарских занятий* |  0 |
|  Самостоятельная работа обучающихся |  36 |
|  Контроль |  0 |

|  |  |
| --- | --- |
|  Формы промежуточной аттестации |  зачеты 7 |
|  |  |  |  |  |
|  **5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий** **5.1. Тематический план** |
|  |  |  |  |  |
|  Наименование раздела дисциплины |  Вид занятия |  Семестр |  Часов |
|  **Системы классификации и кодирования информации** |  |  |  |
|  Сведения из теории чисел и сложность алгоритмов |  Лек |  7 |  2 |
|  Алгебраические структуры |  Лек |  7 |  2 |
|  Элементы теории информации. Информационная энтропия |  Лек |  7 |  2 |
|  Элементы теории кодирования |  Лек |  7 |  4 |
|  Сложные циклические, сверточные и каскадные коды |  Лек |  7 |  4 |
|  Методы шифрования и их применение |  Лек |  7 |  2 |
|  Аспекты безопасности и основные угрозы |  Лек |  7 |  2 |
|  Основы теории чисел |  Пр |  7 |  2 |
|  Анализ сложности алгоритмов |  Пр |  7 |  2 |
|  Меры измерения информации. |  Пр |  7 |  2 |
|  Теория кодирования |  Пр |  7 |  2 |
|  Помехоустойчивые коды Вопросы для обсуждения на занятии |  Пр |  7 |  2 |
|  Сложные циклические, сверточные и каскадные коды |  Пр |  7 |  2 |
|  Введение в криптографические методы защиты информации |  Пр |  7 |  2 |
|  Поточные и блочные и ассиметричные шифры. Вопросы для обсуждения на занятии |  Пр |  7 |  2 |
|  Электронная подпись и управление ключами Вопросы для обсуждения на занятии |  Пр |  7 |  2 |
|  Сведения из теории чисел и сложность алгоритмов |  СР |  7 |  5 |
|  Алгебраические структуры |  СР |  7 |  5 |
|  Элементы теории информации. Информационная энтропия |  СР |  7 |  5 |
|  Элементы теории кодирования |  СР |  7 |  6 |
|  Сложные циклические, сверточные и каскадные коды |  СР |  7 |  5 |
|  Методы шифрования и их применение |  СР |  7 |  5 |
|  Аспекты безопасности и основные угрозы |  СР |  7 |  5 |
|  Всего |  |  |  72 |
|   \* Примечания: а) Для обучающихся по индивидуальному учебному плану - учебному плану, обеспечивающему освоение соответствующей образовательной программы на основе индивидуализации ее содержания с учетом особенностей и образовательных потребностей конкретного обучающегося, в том числе при ускоренном обучении: При разработке образовательной программы высшего образования в части рабочей программы дисциплины Б1.Б.01 «Философия» согласно требованиям частей 3-5 статьи 13, статьи 30, пункта 3 части 1 |

|  |
| --- |
|  статьи 34 Федерального закона Российской Федерации от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»; Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 06.04.2021 № 245, объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся образовательная организация устанавливает в соответствии с утвержденным индивидуальным учебным планом при освоении образовательной программы обучающимся, который имеет среднее профессиональное или высшее образование, и (или) обучается по образовательной программе высшего образования, и (или) имеет способности и (или) уровень развития, позволяющие освоить образовательную программу в более короткий срок по сравнению со сроком получения высшего образования по образовательной программе, установленным Академией в соответствии с Федеральным государственным образовательным стандартом высшего образования (ускоренное обучение такого обучающегося по индивидуальному учебному плану в порядке, установленном соответствующим локальным нормативным актом образовательной организации). б) Для обучающихся с ограниченными возможностями здоровья и инвалидов: При разработке адаптированной образовательной программы высшего образования, а для инвалидов - индивидуальной программы реабилитации инвалида в соответствии с требованиями статьи 79 Федерального закона Российской Федерации от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации, Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 06.04.2021 № 245, Федеральными и локальными нормативными актами, Уставом Академии образовательная организация устанавливает конкретное содержание рабочих программ дисциплин и условия организации и проведения конкретных видов учебных занятий, составляющих контактную работу обучающихся с преподавателем и самостоятельную работу обучающихся с ограниченными возможностями здоровья (инвалидов) (при наличии факта зачисления таких обучающихся с учетом конкретных нозологий). в) Для лиц, зачисленных для продолжения обучения в соответствии с частью 5 статьи 5 Федерального закона от 05.05.2014 № 84-ФЗ «Об особенностях правового регулирования отношений в сфере образования в связи с принятием в Российскую Федерацию Республики Крым и образованием в составе Российской Федерации новых субъектов - Республики Крым и города федерального значения Севастополя и о внесении изменений в Федеральный закон «Об образовании в Российской Федерации»: При разработке образовательной программы высшего образования согласно требованиями частей 3-5 статьи 13, статьи 30, пункта 3 части 1 статьи 34 Федерального закона Российской Федерации от 29.12.2012 № 273- ФЗ «Об образовании в Российской Федерации»; Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 06.04.2021 № 245, объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся образовательная организация устанавливает в соответствии с утвержденным индивидуальным учебным планом при освоении образовательной программы обучающимися, зачисленными для продолжения обучения в соответствии с частью 5 статьи 5 Федерального закона от 05.05.2014 № 84-ФЗ «Об особенностях правового регулирования отношений в сфере образования в связи с принятием в Российскую Федерацию Республики Крым и образованием в составе Российской Федерации новых субъектов - Республики Крым и города федерального значения Севастополя и о внесении изменений в Федеральный закон «Об образовании в Российской Федерации», в течение установленного срока освоения основной профессиональной образовательной программы высшего образования с учетом курса, на который они зачислены (указанный срок может быть увеличен не более чем на один год по решению Академии, принятому на основании заявления обучающегося). г) Для лиц, осваивающих образовательную программу в форме самообразования (если образовательным стандартом допускается получение высшего образования по соответствующей образовательной программе в форме самообразования), а также лиц, обучавшихся по не имеющей государственной аккредитации образовательной программе: При разработке образовательной программы высшего образования согласно требованиям пункта 9 части 1 статьи 33, части 3 статьи 34 Федерального закона Российской Федерации от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»; Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 06.04.2021 № 245, объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся образовательная организация устанавливает в соответствии с утвержденным индивидуальным учебным планом при освоении образовательной программы обучающегося, зачисленного в качестве экстерна для прохождения промежуточной и(или) государственной итоговой аттестации в Академию по соответствующей имеющей государственную аккредитацию образовательной программе в порядке, установленном соответствующим локальным нормативным актом образовательной организации. |

|  |
| --- |
|  **5.2 Содержание дисциплины** |
|  **Темы лекционных занятий** |
|  **Сведения из теории чисел и сложность алгоритмов** |
|
|  Наибольший общий делитель. Алгоритм Евклида. Расширенный алгоритм Евклида. Китайская теорема об остатках. Функция Эйлера. Программная реализация решения системы уравнений по китайской теореме об остатках. Сложность алгоритмов Экспоненциальная сложность. Полиномиальная сложность. О- нотация. Оценка сложности известных алгоритмов. |
|  **Алгебраические структуры** |
|  Группоиды, полугруппы, группы. Делимость в полугруппах и кольцах. Циклические группы и целые числа. Группы и подстановки. Конечные поля. Конечные поля, поля Галуа. Программная реализация вычислений в полях Галуа. Универсальные алгебры |
|  **Элементы теории информации. Информационная энтропия** |
|  Элементы теории кодирования Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга Двоичный код. Расстояние Хэмминга. Кодовое расстояние. Линейный код. Порождающая матрица. Проверочная матрица. Код Хэмминга и его свойства. Построение кода Хэмминга. Циклические коды. Аппаратная реализация кодирования и декодирования. Определение циклического кода, свойства. Архитектура кодера и декодера для циклического кода. Код Боуза-Чоудхури-Хоквингема. Программная реализация построения порождающего полинома циклического кода. |
|  **Элементы теории кодирования** |
|  Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга Двоичный код. Расстояние Хэмминга. Кодовое расстояние. Линейный код. Порождающая матрица. Проверочная матрица. Код Хэмминга и его свойства. Построение кода Хэмминга. Циклические коды. Аппаратная реализация кодирования и декодирования. Определение циклического кода, свойства. Архитектура кодера и декодера для циклического кода. Код Боуза-Чоудхури-Хоквингема. Программная реализация построения порождающего полинома циклического кода. |
|  **Сложные циклические, сверточные и каскадные коды** |
|  Сложные циклические, сверточные и каскадные коды Коды Рида-Соломона Двоичные квадратично-вычетные коды. Границы для кодов. Коды Адамара Коды Гоппы. Сверточные коды. Полиномиальное описание сверточных кодов. Примеры двоичных сверточных кодов. Декодирование сверточных кодов. Каскадные коды Мягкое декодирование блоковых кодов. Мягкое декодирование сверточных кодов. Кодированная модуляция |
|  **Методы шифрования и их применение** |
|  Симметричное шифрование: докомпьютерные шифры. Шифр сдвига. Шифр замены. Шифр Виженера. Перестановочные шифры. Одноразовый шифр-блокнот. Программная реализация шифра замены. Симметричное шифрование: обзор современных шифров. Алгоритм AES. Алгоритм 3DES. Алгоритм RC4. Реализация алгоритма 3DES. Асимметричное шифрование: односторонние функции и новые задачи криптографии. Задача факторизации. Задача вычисления дискретного логарифма. Реализация алгоритма быстрого возведения в степень по модулю. Проблема распределения ключей и протоколы распределения ключей. Протокол широкоротой лягушки. Протокол Нидхейма-Шредера. Протокол Отвэй-Риса. Программная реализация протокола Нидхейма-Шредера. Система шифрования RSA |
|  **Аспекты безопасности и основные угрозы** |
|  Конфиденциальность, целостность, доступность информации. Классификация атак. Классификация угроз. ГОСТ в области информационной безопасности. Анализ современных атак на программное обеспечение. Протоколы проверки аутентичности, |

|  |
| --- |
|  протоколы распределения секрета, протоколы цифровой подписи Разделение секрета. Алгоритм DSA. Подпись Шнорра. Подпись Ниберга-Руппеля. Реализация алгоритма DSA. Системы электронного голосования |
|  **Темы практических занятий** |
|  |
|  **Основы теории чисел** |
|  Вопросы для обсуждения на занятии  1. Что изучает теория чисел? 2. Основы теории делимости 3. НОД и НОК и их свойства 4. Алгоритм Евклида 5. Диофантовы уравнения 6. Важнейшие функции в теории чисел 7. Непрерывные и подходящие дроби |
|  |
|  **Анализ сложности алгоритмов** |
|  Вопросы для обсуждения на занятии 1. Подходы к оценке сложности алгоритмов. Асимптотика 2. Меры и оценки сложности 3. Анализ сложности генерирования перестановок 4. Класс задач, детерминировано решаемых с полиномиальной Сложностью 5. Экспоненциальная сложность. 6. Полиномиальная сложность. 7. О-нотация.. 8. NP-полные и NP-трудные задачи |
|  |
|  **Меры измерения информации.** |
|  Вопросы для обсуждения на занятии 1. Информация в системе управления 2. Синтаксические меры информации 3. Содержательный подход (энтропийный) 4. Энтропия дискретного источника информации 5. Семантическая мера информации 6. Прагматическая мера информации |
|  |
|  **Теория кодирования** |
|  Вопросы для обсуждения на занятии 1. Теорема Шеннона о кодировании источника без памяти 2. Код Хаффмана 3. Код Шеннона-Фано 4. Код Лемпеля-Зива 5. Расширение алфавита 6. Теорема Шеннона о кодировании источника |
|  |
|  **Помехоустойчивые коды** **Вопросы для обсуждения на занятии** |
|  Вопросы для обсуждения на занятии  1. Общая характеристика помехоустойчивых кодов 2. Элементы теории линейных блоковых кодов 3. Коды Хэмминга 4. Декодирование линейных блоковых кодов 5. Простые преобразования линейного кода 6. Коды Рида-Маллера |

|  |
| --- |
|  **Сложные циклические, сверточные и каскадные коды** |
|  Вопросы для обсуждения на занятии 1. Циклические коды 2. Циклические коды Хэмминга 3. Коды Голея 4. Коды Боуза-Чоудхури-Хоквингема (БЧХ) 5. Коды Рида-Соломона 6. Границы для кодов 7. Коды Адамара 8. Коды Гоппы 9. Сверточные коды 10. Декодирование сверточных кодов 11. Каскадные коды |
|  |
|  **Введение в криптографические методы защиты информации** |
|  Вопросы для обсуждения на занятии 1. Основные понятия и задачи криптографии 2. Задачи криптографии и средства их решения 3. Конфиденциальность 4. Целостность 5. Аутентификация 6. Формальные модели шифров 7. Оценки числа смысловых открытых текстов 8. Шифры гаммирования |
|  |
|  **Поточные и блочные и ассиметричные шифры.** **Вопросы для обсуждения на занятии** |
|  Вопросы для обсуждения на занятии 1. Поточные шифры 2. Линейный регистр сдвига 3. Фильтрующий и комбинирующий генераторы 4. Статистические свойства фильтрующей схемы 5. Блочные шифры 6. Структура блочного алгоритма шифрования 7. Сеть Фейстеля 8. SP-сеть 9. Асимметричное шифрование 10. Схема шифрования RSA 11. Схема шифрования Рабина — Вильямса 12. Схема шифрования Эль-Гамаля 13. Схема шифрования Окамото — Учиямы 14. Схема шифрования Мейера — Мюллера |
|  |
|  **Электронная подпись и управление ключами** **Вопросы для обсуждения на занятии** |
|  Вопросы для обсуждения на занятии 1. Электронная подпись 2. Схема Эль-Гамаля 3. Стандарт ECDSA 4. Схема Шнорра 5. Схема Нюберг — Рюппеля 6. Схема KCDSA 7. Характеристики ключевой системы 8. Стойкость к компрометации заданного числа абонентов 9. Протоколы выработки общего ключа 10. Базовый протокол Диффи — Хеллмана 11. Выработка ключа для конференц-связи 12. Протоколы передачи ключей |

|  |
| --- |
|  **6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине** |
|  1. Методические указания для обучающихся по освоению дисциплины «Системы классификации и кодирования информации» / Червенчук И.В.. – Омск: Изд-во Омской гуманитарной академии, 2024. 2. Положение о формах и процедуре проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата и магистратуры, одобренное на заседании Ученого совета от 28.08.2017 (протокол заседания № 1), Студенческого совета ОмГА от 28.08.2017 (протокол заседания № 1), утвержденное приказом ректора от 28.08.2017 №37. 3. Положение о правилах оформления письменных работ и отчётов обучающихся, одобренное на заседании Ученого совета от 29.08.2016 (протокол заседания № 1), Студенческого совета ОмГА от 29.08.2016 (протокол заседания № 1), утвержденное приказом ректора от 01.09.2016 № 43в. 4. Положение об обучении по индивидуальному учебному плану, в том числе ускоренном обучении, студентов, осваивающих основные профессиональные образовательные программы высшего образования - программы бакалавриата, магистратуры, одобренное на заседании Ученого совета от 28.08.2017 (протокол заседания № 1), Студенческого совета ОмГА от 28.08.2017 (протокол заседания № 1), утвержденное приказом ректора от 28.08.2017 №37. |
|  |  |
|  **7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины** **Основная:** |
| 1. Кодирование в системах защиты информации / Соколов В. П., Тарасова Н. П., Шелухин О. И.. - Кодирование в системах защиты информации - Москва: Московский технический университет связи и информатики, 2016. - 94 с. - ISBN: 2227-8397. - URL: http://www.iprbookshop.ru/61485.html  |
| 2. Теория информации и кодирования. Часть 2 / Горячкин О. В.. - Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. - 138 с. - ISBN: 2227-8397. - URL: http://www.iprbookshop.ru/75413.html  |
| 3. Теория информации и кодирования. Часть 1. Теория потенциальной помехоустойчивости / Горячкин О. В.. - Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. - 94 с. - ISBN: 2227-8397. - URL: http://www.iprbookshop.ru/77235.html  |
| 4. Криптографические методы защиты информации / Лось А. Б., Нестеренко А. Ю., Рожков М. И.. - 2-е изд. - Москва: Юрайт, 2018. - 473 с . - ISBN: 978-5-534-01530-0. - URL: https://urait.ru/bcode/413075  |
|  |  *Дополнительная:* |
| 1. Математическая логика и теория алгоритмов / Макоха А. Н., Шапошников А. В., Бережной В. В.. - Ставрополь: Северо-Кавказский федеральный университет, 2017. - 418 с. - ISBN: 2227-8397. - URL: http://www.iprbookshop.ru/69397.html  |
|
| 2. Математика: основные математические структуры / Вечтомов Е. М.. - 2-е изд. - Москва: Юрайт, 2019. - 296 с . - ISBN: 978-5-534-08077-3. - URL: https://urait.ru/bcode/441205  |
| 3. Защита информации: основы теории / Щеглов А. Ю., Щеглов К. А.. - Москва: Юрайт, 2019. - 309 с . - ISBN: 978-5-534-04732-5. - URL: https://urait.ru/bcode/433715  |
| 4. Криптографические методы защиты информации / Запечников С. В., Казарин О. В., Тарасов А. А.. - Москва: Издательство Юрайт, 2018. - 309 . - ISBN: 978-5-534-02574-3. - URL: https://www.biblio-online.ru/bcode/413316  |
|  **8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины** |
|  1. ЭБС IPRBooks Режим доступа: http://www.iprbookshop.ru 2. ЭБС издательства «Юрайт» Режим доступа: http://biblio-online.ru 3. Единое окно доступа к образовательным ресурсам. Режим доступа: |

|  |
| --- |
|  http://window.edu.ru/ 4. Научная электронная библиотека e-library.ru Режим доступа: http://elibrary.ru 5. Ресурсы издательства Elsevier Режим доступа: http://www.sciencedirect.com 6. Федеральный портал «Российское образование» Режим доступа: www.edu.ru 7. Журналы Кембриджского университета Режим доступа: http://journals.cambridge.org 8. Журналы Оксфордского университета Режим доступа: http://www.oxfordjoumals.org 9. Словари и энциклопедии на Академике Режим доступа: http://dic.academic.ru/ 10. Сайт Библиотеки по естественным наукам Российской академии наук. Режим доступа: http://www.benran.ru 11. Сайт Госкомстата РФ. Режим доступа: http://www.gks.ru 12. Сайт Российской государственной библиотеки. Режим доступа: http://diss.rsl.ru 13. Базы данных по законодательству Российской Федерации. Режим доступа: http://ru.spinform.ru Каждый обучающийся Омской гуманитарной академии в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечной системе (электронной библиотеке) и к электронной информационно-образовательной среде Академии. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно- телекоммуникационной сети «Интернет», и отвечает техническим требованиям организации как на территории организации, так и вне ее. Электронная информационно-образовательная среда Академии обеспечивает: доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах; фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы; проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий; формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса; взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет». |
|  **9. Методические указания для обучающихся по освоению дисциплины** |
|  К современному специалисту общество предъявляет достаточно широкий перечень требований, среди которых немаловажное значение имеет наличие у выпускников определенных способностей и умений самостоятельно добывать знания из различных источников, систематизировать полученную информацию, давать оценку конкретной ситуации. Формирование такого умения происходит в течение всего периода обучения через участие в практических занятиях, выполнение контрольных заданий и тестов. При этом самостоятельная работа обучающихся играет решающую роль в ходе всего учебного процесса. Успешное освоение компетенций, формируемых данной учебной дисциплиной, предполагает оптимальное использование времени самостоятельной работы. Целесообразно посвящать до 20 минут изучению конспекта лекции в тот же день после лекции и за день перед лекцией. Теоретический материал изучать в течение недели до 2 часов, а готовиться к практическому занятию по дисциплине до 1.5 часов. Для понимания материала учебной дисциплины и качественного его усвоения рекомендуется такая последовательность действий: ⦁ после прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры; ⦁ при подготовке к лекции следующего дня нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции; ⦁ в течение недели выбрать время для работы с литературой по учебной дисциплине в библиотеке и для решения задач; ⦁ при подготовке к практическим /семинарским/лабораторным занятиям повторить |

|  |
| --- |
|  основные понятия и формулы по теме домашнего задания, изучить примеры; ⦁ решая упражнение или задачу, предварительно понять, какой теоретический материал нужно использовать; наметить план решения, попробовать на его основе решить 1-2 аналогичные задачи. При решении задач всегда необходимо комментировать свои действия и не забывать о содержательной интерпретации. Рекомендуется использовать методические указания и материалы по учебной дисциплине, текст лекций, а также электронные пособия. Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекций изучаются научная литература по данной учебной дисциплине. Полезно использовать несколько учебников, однако легче освоить курс, придерживаясь одного учебника и конспекта. Рекомендуется, кроме «заучивания» материала, добиться понимания изучаемой темы дисциплины. С этой целью после прочтения очередной главы желательно выполнить несколько простых упражнений на соответствующую тему. Кроме того, очень полезно мысленно задать себе и попробовать ответить на следующие вопросы: о чем эта глава, какие новые понятия в ней введены, каков их смысл. При изучении теоретического материала всегда полезно выписывать формулы и графики. При выполнении домашних заданий и подготовке к контрольной работе необходимо сначала прочитать теорию и изучить примеры по каждой теме. Решая конкретную задачу, предварительно следует понять, что требуется в данном случае, какой теоретический материал нужно использовать, наметить общую схему решения. При решении задачи «по образцу» рассмотренного на аудиторном занятии или в методическом пособии примера, то желательно после этого обдумать процесс решения и попробовать решить аналогичную задачу самостоятельно. При подготовке к промежуточной аттестации необходимо освоить теоретические положения данной дисциплины, разобрать определения всех понятий и постановки моделей, описывающих процессы, рассмотреть примеры и самостоятельно решить несколько типовых задач из каждой темы. Дополнительно к изучению конспектов лекций необходимо пользоваться учебниками по учебной дисциплине. |
|  **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем** |
|  Перечень программного обеспечения  • Microsoft Windows 10 Professional • Microsoft Office Professional 2007 Russian • Cвободно распространяемый офисный пакет с открытым исходным кодом LibreOffice 6.0.3.2 Stable • Антивирус Касперского • Cистема управления курсами LMS Русский Moodle 3KL  Современные профессиональные базы данных и информационные справочные системы: |
|  • Сайт Федеральной службы государственной статистики РФ www.gks.ru |
|  • Сайт Правительства РФ www.government.ru |
|  • Сайт Президента РФ http://www.president.kremlin.ru |
|  • Портал «Информационно-коммуникационные технологии в образовании» |
|  • Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru |
|  • Официальный интернет-портал правовой информации http://pravo.gov.ru |
|  **Электронная информационно-образовательная среда** |
|  Электронная информационно-образовательная среда Академии, работающая на платформе LMS Moodle, обеспечивает: • доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем ( ЭБС IPRBooks, ЭБС Юрайт ) и электронным образовательным ресурсам, указанным в рабочих программах; • фиксацию хода образовательного процесса, результатов промежуточной |

|  |
| --- |
|  аттестации и результатов освоения программы бакалавриата; • проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий; • формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса; • взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет». При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии: • сбор, хранение, систематизация и выдача учебной и научной информации; • обработка текстовой, графической и эмпирической информации; • подготовка, конструирование и презентация итогов исследовательской и аналитической деятельности; • самостоятельный поиск дополнительного учебного и научного материала, с использованием поисковых систем и сайтов сети Интернет, электронных энциклопедий и баз данных; • использование электронной почты преподавателями и обучающимися для рассылки информации, переписки и обсуждения учебных вопросов. • компьютерное тестирование; • демонстрация мультимедийных материалов. |
|  |
|  **11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине** |
|  Для осуществления образовательного процесса Академия располагает материально- технической базой, соответствующей противопожарным правилам и нормам, обеспечивающим проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных рабочей программой дисциплины. Специальные помещения представляют собой учебные аудитории учебных корпусов, расположенных по адресу г. Омск, ул. 4 Челюскинцев, 2а, г. Омск, ул. 2 Производственная, д. 41/1 1. Для проведения лекционных занятий: учебные аудитории, материально-техническое оснащение которых составляют: столы аудиторные; стулья аудиторные; стол преподавателя; стул преподавателя; кафедра, ноутбуки; операционная система Microsoft Windows 10, Microsoft Office Professional Plus 2007, LibreOffice Writer, LibreOffice Calc, LibreOffice Impress, LibreOffice Draw, LibreOffice Math, LibreOffice Base; 1С:Предпр.8 - комплект для обучения в высших и средних учебных заведениях; Линко V8.2, Moodle, BigBlueButton, Kaspersky Endpoint Security для бизнеса – Стандартный, система контент фильтрации SkyDNS, справочно-правовые системы «Консультант плюс», «Гарант»; актовый зал, материально-техническое оснащение которого составляют: Кресла, Кафедра, стол, микше, микрофон, аудио-видео усилитель, ноутбук, Операционная система Microsoft Windows 10, Microsoft Office Professional Plus 2007; 2. Для проведения практических занятий: учебные аудитории, лингофонный кабинет материально-техническое оснащение которых составляют: столы аудиторные; стулья аудиторные; стол преподавателя; стул преподавателя; наглядные материалы; кафедра, ноутбуки; операционная система Microsoft Windows 10, Microsoft Office Professional Plus 2007, LibreOffice Writer, LibreOffice Calc, LibreOffice Impress, LibreOffice Draw, LibreOffice Math, LibreOffice Base; 1С: Предпр.8 - комплект для обучения в высших и средних учебных заведениях; Линко V8.2; Moodle, BigBlueButton, Kaspersky Endpoint Security для бизнеса – Стандартный, система контент фильтрации SkyDNS, справочно- правовые системы «Консультант плюс», «Гарант»; электронно-библиотечные системы «IPRbooks» и «ЭБС ЮРАЙТ». 3. Для проведения лабораторных занятий имеется: учебно-исследовательская межкафедральная лаборатория информатики и ИКТ, оснащение которой составляют: |

|  |
| --- |
|  Столы компьютерные, стулья, компьютеры, доска пластиковая, колонки, стенды информационные, экран, мультимедийный проектор, кафедра. Оборудование: операционная система Microsoft Windows 10, MS Visio Standart, Microsoft Office Professional Plus 2007, LibreOffice, Kaspersky Endpoint Security для бизнеса – Стандартный, Система контент фильтрации SkyDNS, справочно-правовая система «Консультант плюс», «Гарант», Электронно библиотечная система IPRbooks, Электронно библиотечная система «ЭБС ЮРАЙТ» www.biblio-online.ru., 1С:Предпр.8.Комплект для обучения в высших и средних учебных заведениях, Moodle. Учебно-исследовательская межкафедральная лаборатория возрастной анатомии, физиологии и гигиены человека и психодиагностики, оснащение которой составляют: столы аудиторные, стулья аудиторные, стол преподавателя, стул преподавателя, кафедра, мультимедийный проектор, экран, стенды информационные. Оборудование: стенды информационные с портретами ученых, Фрустрационный тест Розенцвейга (взрослый) кабинетный Вариант (1 шт.), тестово-диагностические материалы на эл. дисках: Диагностика структуры личности, Методика И.Л.Соломина, факторный личностный опросник Кеттелла, Тест Тулуз-Пьерона, Тест Векслера, Тест Гилфорда, Методика рисуночных метафор, Тест юмористических фраз А.Г.Шмелева, Диагностический альбом Семаго Н.Я., Семаго М.М., раздаточные материалы: диагностика темперамента, диагностика эмоционально-волевой сферы личности, диагностика определения готовности ребенка к школе, диагностика выявления готовности и способности к обучению дошкольников. 4. Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации имеются учебные аудитории материально-техническое оснащение которых составляют: столы компьютерные, стол преподавательский, стулья, учебно-наглядные пособия: наглядно-дидактические материалы, доска пластиковая, видеокамера, компьютер, Операционная система Microsoft Windows 10, Microsoft Office Professional Plus 2007, LibreOffice Writer, LibreOffice Calc, LibreOffice Impress, LibreOffice Draw, LibreOffice Math, LibreOffice Base, Линко V8.2, 1С:Предпр.8.Комплект для обучения в высших и средних учебных заведениях, Moodle, BigBlueButton, Kaspersky Endpoint Security для бизнеса – Стандартный, Система контент фильтрации SkyDNS, справочно-правовая система «Консультант плюс», «Гарант», Электронно библиотечная система IPRbooks, Электронно библиотечная система «ЭБС ЮРАЙТ» www.biblio-online.ru 5. Для самостоятельной работы: аудитории для самостоятельной работы, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, библиотека, читальный зал, материально-техническое оснащение которых составляют: столы, специализированные стулья, столы компьютерные, компьютеры, стенды информационные, комплект наглядных материалов для стендов. Операционная система Microsoft Windows 10, Microsoft Office Professional Plus 2007, LibreOffice Writer, LibreOffice Calc, LibreOffice Impress, LibreOffice Draw, LibreOffice Math, LibreOffice Base, Moodle, BigBlueButton, Kaspersky Endpoint Security для бизнеса – Стандартный, Система контент фильтрации SkyDNS, справочно-правовая система «Консультант плюс», «Гарант», Электронно библиотечная система IPRbooks, Электронно библиотечная система «ЭБС ЮРАЙТ». |