Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Смоленский государственный университет»
Кафедра прикладной математики и информатики

«Утверждаю»
Проректор по учебно-
методической работе
_____ Ю.А. Устименко
«23» июня 2022 г.

Рабочая программа дисциплины
Б1.В.ДВ.07.01 Основы криптографии

Направление подготовки **01.03.02 Прикладная математика и информатика**
Направленность (профиль) **Математическое и информационное моделирование**
Форма обучения очная
Курс – 4
Семестр – 8
Всего зачетных единиц – 2, часов – 72

Форма отчетности: зачет – 8 семестр

Программу разработал
кандидат физико-математических наук, доцент В.Р. Кристалинский

Одобрена на заседании кафедры
«16» июня 2022 г., протокол № 10

Заведующий кафедрой _____ С.В. Козлов

Смоленск
2022

1. Место дисциплины в структуре ОП

Дисциплина «Основы криптографии» относится к дисциплинам по выбору. Она изучается в 8 семестре.

Требования к входным знаниям, умениям и компетенциям студента формируются на основе программы среднего (полного) общего образования по информатике и информационным технологиям (базовый уровень), а также дисциплин «Защита информации», «Языки и методы программирования», «Теория вероятностей и математическая статистика», «Алгебра и геометрия».

Изучение курса основано на традиционных методах высшей школы, тесной взаимосвязи со смежными курсами, а также на использовании современных технологий программирования.

2. Планируемые результаты обучения по дисциплине

Компетенция	Индикаторы достижения
ПК-1. Способен осуществлять поиск, анализ, систематизацию научной информации в области прикладной математики и информатики для реализации научно-исследовательских проектов и решения прикладных задач по проектированию и разработке программного обеспечения.	**Знает**: теоретические основы и технологии организации научно-исследовательской деятельности. **Умеет**: осуществлять поиск, анализ, систематизацию научной информации в области прикладной математики и информатики для реализации научно-исследовательских проектов и решения прикладных задач по проектированию и разработке программного обеспечения. **Владеет**: навыками организации и проведения научно-исследовательской деятельности в ходе выполнения профессиональных функций.
ПК-2. Способен анализировать требования и проектировать программное и информационное обеспечение компьютерных сетей, вычислительные модели и модели данных для реализации элементов новых (или известных) программных продуктов.	**Знает**: возможности существующей программно-технической аппаратуры, современных и перспективных средств разработки программных продуктов, технических средств; методологии разработки программного обеспечения, технологии программирования; методы и средства проектирования программного обеспечения, баз данных, программных интерфейсов; принципы построения архитектуры программного обеспечения и виды архитектуры программного обеспечения, типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения; методики формализации и алгоритмизации поставленных задач. **Умеет**: проводить анализ требований к программному обеспечению, вырабатывать варианты их реализации, проводить оценку и обоснование вырабатываемых решений; использовать существующие типовые решения и шаблоны проектирования программного обеспечения, применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов; использовать методы и приемы

	формализации и алгоритмизации задач, применять стандартные алгоритмы, использовать программные средства для графического отображения алгоритмов. **Владеет**: методами анализа возможностей реализации требований к программному обеспечению, оценки времени и трудоемкости их реализации, навыками по проектированию программного обеспечения, баз данных, программных интерфейсов, информационных ресурсов сети Интернет.
ПК-3. Способен разрабатывать и отлаживать программный код	**Знает**: методологию разработки программного обеспечения, информационно-коммуникационных систем, баз данных, информационных ресурсов в сети Интернет; технологии программирования; особенности выбранной среды программирования и системы управления базами данных, синтаксис выбранного языка программирования, особенности программирования на нем, стандартные библиотеки языка программирования; компоненты программно-технических архитектур; методы повышения читаемости кода, системы кодировки символов, форматы хранения исходных текстов программ; методы и приемы отладки кода, типы и форматы сообщений об ошибках и состоянии аппаратных средств, современные компиляторы, отладчики оптимизаторы программного кода. **Умеет**: применять выбранные языки программирования для написания программного кода, использовать выбранную среду программирования и средства системы управления базами данных, использовать возможности имеющейся технической и программной архитектуры; структурировать, комментировать, размечать, форматировать программный код в соответствии с требованиями; выявлять ошибки в программном коде, применять методы и приемы его отладки, интерпретировать сообщения об ошибках, предупреждениях, применять современные компиляторы, отладчики, оптимизаторы программного кода. **Владеет**: навыками по созданию программного кода в соответствии с техническим заданием, оптимизации программного кода с использованием специализированных программных средств, форматированию программного кода, анализу, проверке, отладке исходного программного

	кода.

3. Содержание дисциплины

1. **Основные задачи и понятия криптографии.** Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы.
2. **Блочные шифры замены.** Блочные шифры простой замены и особенности их анализа. Сети Фейстеля. Алгоритм Lucifer. Современные блочные шифры. Криптоалгоритм DES. Криптоалгоритм ГОСТ-28147-89.
3. **Основные понятия математической теории информации.** Энтропия. Теоремы Шеннона. Модели содержательных сообщений. Расстояние единственности шифра.
4. **Надёжность шифров.** Криптографическая стойкость шифров. Теоретически стойкие шифры. Методы определения ключей шифрсистем. Методы опробования, статистический метод. Аналитические методы криптоанализа.
5. **Методы синтеза шифрсистем.** Принципы построения алгоритмов шифрования. Шифры, близкие к совершенным. Гомоморфизмы и конгруэнции шифров. Математические основы синтеза булевых функций.
6. **Имитостойкость шифров.** Понятие имитостойкости. Имитация в пустом канале. Имитация при передаче сообщения. Навязывание сообщения. Имитовставки.

4. Тематический план

№ п/п	Разделы и темы	Всего часов	Формы занятий			
			лекции	практические занятия	лабораторные занятия	самостоятельная работа
1	Основные задачи и понятия криптографии.	4	2	–	–	2
2	Блочные шифры замены	14	4	–	4	6
3	Основные понятия математической теории информации	14	4	–	4	6
4	Надёжность шифров.	16	4	–	6	6
5	Методы синтеза шифрсистем.	12	2	–	6	4
6	Имитостойкость шифров	12	2	–	6	4
ИТОГО		72	18	–	26	28

5. Виды образовательной деятельности

Лекции

1. Основные задачи и понятия криптографии. Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы.

2-3. Блочные шифры замены. Блочные шифры простой замены и особенности их анализа. Сети Фейстеля. Алгоритм Lucifer. Современные блочные шифры. Криптоалгоритм DES. Криптоалгоритм ГОСТ-28147-89.

4-5. Основные понятия математической теории информации. Энтропия. Теоремы Шеннона. Модели содержательных сообщений. Расстояние единственности шифра.

6-7. Надёжность шифров. Криптографическая стойкость шифров. Теоретически стойкие шифры. Методы определения ключей шифрсистем. Методы опробования, статистический метод. Аналитические методы криптоанализа.

8. Методы синтеза шифрсистем. Принципы построения алгоритмов шифрования. Шифры, близкие к совершенным. Гомоморфизмы и конгруэнции шифров. Математические основы синтеза булевых функций.

9. Имитостойкость шифров. Понятие имитостойкости. Имитация в пустом канале. Имитация при передаче сообщения. Навязывание сообщения. Имитовставки.

Лабораторные работы

Лабораторное занятие №1-2

1. Разработка программы, реализующей сбалансированную сеть Фейстеля

Лабораторное занятие №3-4

1. Разработка программы, реализующей криптосистему Lucifer.

Лабораторное занятие №5-6

1. Разработка программы, реализующей алгоритм DES.

Лабораторное занятие №7-8

1. Разработка программы, реализующей алгоритм AES.

Лабораторное занятие №9-10

1. Разработка программы, реализующей алгоритм криптографического сжатия данных.

Лабораторное занятие №11-13

1. Разработка программы, реализующей алгоритм Якобсена.

Самостоятельная работа

1. **Основные задачи и понятия криптографии.** Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации.

2. **Блочные шифры замены.** Криптоалгоритм ГОСТ-28147-89.

3. **Основные понятия математической теории информации.** Расстояние единственности шифра.

4. **Надёжность шифров.** Методы опробования, статистический метод. Аналитические методы криптоанализа.

5. **Методы синтеза шифрсистем.** Гомоморфизмы и конгруэнции шифров. Математические основы синтеза булевых функций.

9. Имитостойкость шифров. Навязывание сообщения. Имитовставки.

6. Критерии оценивания результатов освоения дисциплины (модуля)

6.1. Оценочные средства и критерии оценивания для текущей аттестации

Вопросы к лекциям 1-3

1. Каковы функции защиты информации?
2. Как определяется детерминированная система шифрования?
3. Чем различаются блочные и поточные шифры?
4. Что такое симметричные шифры?
5. Какие виды криптоатак вы знаете?

6. Что такое априорная мера неопределенности открытого текста?
7. Что такое апостериорная мера неопределенности открытого текста?
8. Что такое мера неопределенности секретного ключа?
9. Какой шифр называется абсолютно стойким?
10. Что такое рассеивание?
11. Что такое перемешивание?
12. Что такое сеть Файстеля?
13. Что такое s и p- блоки?

Вопросы к лекциям 2-3

1. Что такое произведение шифров?
2. Какой шифр называют транзитивным?
3. Что такое эндоморфный шифр?
4. Какие ключи называют эквивалентными?
5. Что такое матрица переходных вероятностей шифра?
6. Каким условиям равносильно условие совершенности шифра?
7. Опишите модель стационарного источника независимых символов алфавита. В чем ее недостатки?
8. Опишите марковскую модель источника сообщений.
9. Как вычисляется избыточность языка и в чем ее смысл?
10. Что такое запретная m-грамма?

Вопросы к лекциям 4-5

1. Что такое конечная вероятностная схема?
2. Какими свойствами должна обладать энтропия?
3. Как определяется количество информации в сообщении?
4. Что такое энтропия конечной вероятностной схемы?
5. Как определяется объединенная вероятностная схема AB?
6. Как определяется энтропия объединенной схемы?
7. Как вычисляется условная энтропия схемы A при условии схемы B?
8. Как вычисляется количество информации о сообщении a, содержащейся в сообщении b?
9. Как вычисляется взаимная информация между A и B?
10. Сформулируйте свойства энтропии.
11. Сформулируйте 1 и 2 теоремы Шеннона.
12. Какая случайная последовательность называется стационарной и эргодической?
13. Какая величина называется избыточностью языка?
14. Как вычисляются ненадежности открытого текста и ключа?
15. Сформулируйте теоремы Шеннона о ненадежности.

Вопросы к лекциям 5-6

1. Как вычисляется среднее число текстов данной длины, которые могут быть зашифрованы в данный шифртекст?
2. Что такое расстояние единственности шифра (первое определение)?
3. Каково второе определение расстояния единственности шифра?
4. Опишите третий подход к вычислению расстояния единственности шифра.
5. Какова верхняя приблизительная оценка расстояния единственности шифра?
6. Что такое трудоемкость алгоритма дешифрования?
7. Что такое надежность алгоритма дешифрования?
8. Какие классы алгоритмов могут использоваться при дешифровании?

9. Что такое методы частичного опробования ключей?
10. Чему равна трудоемкость тотального метода дешифрования?
11. Чему равна надежность тотального метода дешифрования?
12. Какой смысл имеют величины α и β в формулах трудоемкости и надежности?
13. Какие дополнительные данные могут быть при использовании эквивалентности ключей?
14. Чему равна трудоемкость метода тотального опробования при использовании эквивалентности ключей в различных случаях?
15. Чему равна надежность метода тотального опробования при использовании эквивалентности ключей в различных случаях?

Вопросы к лекциям 7-9

1. Что такое конечный автомат?
2. Что такое автономный конечный автомат?
3. Что такое диаметр автомата?
4. Что такое метод опробования с использованием памяти?
5. Что такое метод расшифровки черного ящика?
6. Что такое метод использования гомоморфизмов?
7. Что такое статистические методы криптоанализа?
8. Что такое метод статистических аналогов?
9. В чем заключается идея статистического определения пары входного и выходного слова автомата?
10. Что такое метод разностного анализа?
11. Что такое метод линейного криптоанализа?
12. Как работает метод координатного спуска?
13. Опишите метод Коновальцева решения систем уравнений над конечными полями.
14. Как решается трапецеидальная система уравнений над конечными полями?
15. При каких условиях произведение шифров является совершенным шифром?
16. Какой шифр называется минимальным?
17. Что такое латинский квадрат?
18. Что такое квазигруппа?
19. При каких условиях групповой транзитивный шифр является обратимым?
20. Что такое инвариант шифра?
21. Что такое двоичный аналог функции?
22. Что такое коэффициент статистической структуры?
23. Что такое матрица Адамара?
24. Каковы свойства матрицы Адамара?
25. Что такое кронекеровское произведение?
26. Что такое матрица Сильвестра-Адамара?
27. Как определяется преобразование Фурье для булевой функции?

Вопросы к лекции 10

1. Что такое навязывание в пустом канале?
2. Какой шифр называется лучшим по имитозащите?
3. Что такое имитация путем подмены?
4. Какой шифр называется лучшим по имитозащите путем подмены?
5. Что такое целевая имитация в пустом канале?
6. Что такое имитовставки?

Критерии оценивания вопросов

1. Нормы оценивания ответов на теоретические вопросы

№ п/п	Теоретический вопрос	Количество баллов (*)

1	Дан краткий ответ на поставленный вопрос	1 балл
2	Дан развернутый ответ на вопрос с анализом результатов	2 балла

(*) Возможна градация в 0,25 балла.

2. Шкала оценивания. Оценка «зачтено» за ответы на теоретические вопросы выставляется, если набрано не менее 3 баллов при ответе на три вопроса, в противном случае выставляется «не зачтено».

Задания для лабораторных занятий

Задачи по темам курса предложены к каждому лабораторному занятию.

Задания для лабораторных и самостоятельной работ, образцы решений основных типовых задач практики также размещены в системе дистанционного обучения СмолГУ (www.moodle.smolgu.ru).

Критерии оценивания выполнения лабораторных работ

1. Нормы оценивания каждой лабораторной работы:

№п/п	Структурная часть работы	Количество баллов (*)
1	Ответ на теоретические вопросы по теме лабораторной работы	1 балл
2	Демонстрация выполнения конкретного задания, предложенного для самостоятельного решения к лабораторной работе	2 балла

(*) с возможностью градации до 0,25 балла.

2. Шкала оценивания. Оценка «зачтено» за лабораторную работу выставляется, если набрано не менее 2 баллов, в противном случае за работу выставляется «не зачтено».

6.2. Оценочные средства и критерии оценивания для промежуточной аттестации

Теоретические вопросы

1. Понятия "информационная безопасность" и "защита информации". Основные составляющие информационной безопасности.
2. Объекты защиты. Категории и носители информации.
3. Средства защиты информации.
4. Криптография. Основные термины и определения.
5. Классификация криптографических систем.
6. Шифры замены. Основные методы шифрования.
7. Шифры перестановки. Основные методы шифрования.
8. Шифры гаммирования. Основные методы шифрования.
9. Шифры гаммирования. Способы генерации гаммы. Генераторы гамм.
10. Схема режима шифрования DES-ECB.
11. Схема режима шифрования DES-CBC.
12. Схема режима шифрования DES-CPB и DES-OFB.
13. Тройной DES. Сферы применения различных режимов DES.
14. Схема режима шифрования простой замены ГОСТ 28147-89.
15. Шифрование с открытым ключом. Основные понятия.
16. Алгоритм шифрования RSA.
17. Алгоритм шифрования Эль-Гамаля.

Критерии оценивания теоретических вопросов

1. Нормы оценивания ответов на теоретические вопросы

№ п/п	Теоретический вопрос	Количество баллов (*)
1	Дан краткий ответ на поставленный вопрос	1 балл
2	Дан развернутый ответ на вопрос с анализом результатов	2 балла

(*) Возможна градация в 0,25 балла.

2. Шкала оценивания. Оценка «зачтено» за ответы на теоретические вопросы выставляется, если набрано не менее 3 баллов при ответе на три вопроса, в противном случае выставляется «не зачтено».

Критерий получения зачета

Зачет выставляется по результатам работы студента в течение семестра.

Для получения зачета студент должен:

- уметь отвечать на теоретические вопросы, рассмотренные на лекциях;
- уметь решать задачи, предложенные на лабораторных занятиях.

7. Перечень основной и дополнительной учебной литературы

7.1. Список основной литературы

1. Бабенко Л. К., Ищукова Е. А. Криптографическая защита информации: симметричное шифрование. Пособие для вузов. – М.: Юрайт, 2018. – 220 с.
2. Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для вузов. М.: Юрайт, 2018. – 309 с.
3. Лось А. Б., Нестеренко А. Ю., Рожков М. И. Криптографические методы защиты информации. Учебник для академического бакалавриата. М.: Юрайт, 2018. – 473 с

7.2. Список дополнительной литературы

1. Аграновский А. В., Хади Р. А.. Практическая криптография: алгоритмы и их программирование. М.:Солон-Пресс, 2009. – 256 с.
2. Бабаш А. В., Шанкин Г. П. Криптография. – М.: СОЛОН-Р, 2002.–512 с.
3. Введение в криптографию / Под общ. Ред. В. В. Ященко. – М.:МЦНМО, 2012. – 348 с.
4. Ветров Ю.В. Криптографические методы защиты информации в телеком-муникационных системах: учеб. пособие / Ю.В. Ветров, С.Б. Макаров. – СПб.: Изд-во Политехн. ун-та, 2011. – 174 с.
5. Рябко Б. Я. Криптографические методы защиты информации: учеб. пособие для вузов / Б. Я. Рябко, А. Н. Фионов. – 2-е изд., стереотип. – М.: Горячая линия - Телеком, 2012. – 229 с.
6. Рябко Б. Я. Основы современной криптографии и стеганографии / Б. Я. Рябко, А. Н. Фионов. – М.: Горячая линия - Телеком, 2011. – 232 с.

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Система дистанционного обучения СмолГУ (moodle.smolgu.ru).
2. Национальный открытый университет (intuit.ru).
3. Национальная платформа открытого образования (opened.ru)

8. Материально-техническое обеспечение

Учебная аудитория для проведения занятий лекционного типа, оснащенная стандартной учебной мебелью, интерактивной доской, мультимедиапроектором, ноутбуком и колонками.

Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации - компьютерная аудитория с выходом в Интернет.

Помещение для самостоятельной работы – компьютерный класс с доступом к сети «Интернет» и ЭИОС СмолГУ.

9. Программное обеспечение

Kaspersky Endpoint Security для бизнеса Стандартный АО «Лаборатория Касперского», лицензия 1FB6-161215-133553-1-6231.

Microsoft Open License, лицензия 49463448 в составе: Microsoft Windows Professional 7 Russian; Microsoft Office 2010 Russian.

Среды разработки на C#.

Поисковые системы сети Интернет.