Учреждение образования «Полоцкий государственный университет»

УТВЕРЖДАЮ
Проректор по учебной работе
учреждения образования
«Полоцкий государственный
университет»

_____ Ю.П. Голубев
«___» _____ 2021 г.
Регистрационный №УД-304/21/уч

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности
1-98 01 01 Компьютерная безопасность
(по направлениям)
направление специальности
1-98 01 01-01 Компьютерная безопасность
(математические методы и программные системы)

2021 г.

Учебная программа составлена в соответствии с требованиями образовательного стандарта высшего образования Министерства образования Республики Беларусь по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» ОСВО 1-98 01 01-2013 и учебного плана специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)». Регистрационный №13-13/уч. ФИТ от 29.08.2013 г. для дневной формы получения высшего образования.

СОСТАВИТЕЛИ:
КОЗЛОВ АЛЕКСАНДР АЛЕКСАНДРОВИЧ, доцент, кандидат физико-математических наук, доцент кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет»
УСТЮГОВ ВЛАДИСЛАВ ВАЛЕРЬЕВИЧ, ассистент кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет»
(протокол № 12 от «22» 11 2021 г.).

Методической комиссией факультета компьютерных наук и электроники учреждения образования «Полоцкий государственный университет»
(протокол № 4 от «14» 12 2021 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Содержание дисциплины «Математические основы криптологии» охватывает круг вопросов, связанных с базовыми принципами построения и математического обоснования криптографических систем.

Целью изучения дисциплины «Математические основы криптологии» является изложение базовых принципов построения и математического обоснования криптографических систем.

Изучение данной дисциплины является необходимым этапом в профессиональном развитии «специалиста по защите информации, математика».

Задачи изучения дисциплины «Математические основы криптологии». При изучении данной дисциплины требуется разрешить основные задачи:

– формирование представления математического обоснования криптографических методов у студентов;

– изучение основных алгоритмов защиты информации криптографическим методом;

– изучение способов практической реализации алгоритмов путем выполнения лабораторных работ.

В результате изучения дисциплины «Математические основы криптологии» обучаемый должен:

знать:

– основные понятия математической логики и теории алгоритмов;

– основные способы решения рекуррентных уравнений;

– основные подходы при разработке эффективных алгоритмов;

– основные комбинаторные алгоритмы , а также способы их эффективной реализации;

уметь:

– осуществлять программную реализацию алгоритма;

– формализовать поставленную задачу;

– проводить оценку сложности алгоритма.;

владеть:

– основными подходами к разработке эффективных алгоритмов;

– навыками реализации и использования алгоритмов для решения задач криптологии.

Требования к уровню освоения содержания учебной дисциплины. При изучении дисциплины ««Математические основы криптологии» у студентов специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» должен сформироваться набор компетенций, соответствующих присваиваемой по завершению высшего образования квалификации «Специалист по защите информации. Математик», обеспечивающих выпускникам по указанной специальности успешность применения полученных знаний и умений в дальнейшей профессиональной деятельности:

Академические компетенции.

АК-1 Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач;

АК-2 Владеть системным и сравнительным анализом;

АК-3 Владеть исследовательскими навыками;

АК-4 Уметь работать самостоятельно;

АК-5 Быть способным вырабатывать новые идеи (креативность);

АК-6 Владеть междисциплинарным подходом при решении проблем;

АК-7 Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером;

АК-8 Иметь лингвистические навыки (устная и письменная коммуникация);

АК-9 Уметь учиться, повышать свою квалификацию в течение всей жизни.

Социально-личностные компетенции.

СК-2 Быть способным к социальному взаимодействию;

СК-3 Обладать способностью к межличностным коммуникациям.

Профессиональные компетенции.

ПК-8 Взаимодействовать со специалистами смежных профилей;

ПК-12 Пользоваться глобальными информационными ресурсами;

ПК-24 Работать с научной, технической и патентной литературой.

Сформированные компетенции являются базовыми при изучении всех последующих дисциплин, связанных с программированием, а также фундаментальной основой для дальнейшей профессиональной деятельности специалиста в области защиты информации.

Перечень дисциплин, в продолжение и на базе которых изучается дисциплина.
Для изучения учебной дисциплины «Математические основы криптологии» по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» необходимы знания, полученные при изучении базовых дисциплин: «Дискретная математика и математическая логика» государственного компонента и «Программирование» компонента учреждения высшего образования.

Перечень дисциплин, которые изучаются на базе дисциплины.
Знания полученные при изучении дисциплины «Математические основы криптологии» по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» являются основой для дисциплин: «Исследование операций», «Модели данных и системы управления базами данных» государственного компонента, а также при изучении ряда дисциплин специализации. Изучение учебной дисциплины позволяет дать студентам базу, необходимую для успешного усвоения материала перечисленных выше учебных дисциплин, а также получить знания, необходимые им в дальнейшем для успешной работы.

В соответствии с учебным планом по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» на изучение учебной дисциплины отводится:

Форма получения высшего образования первой ступени	дневная
Курс (курсы)	2
Семестр	4
Всего часов по дисциплине	72
Всего аудиторных часов по дисциплине	34
В том числе:	
Лекции, часов	18
Лабораторные занятия, часов	16
Самостоятельная работа, часов	38
Форма текущей аттестации	зачет

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Введение в дисциплину

Цели и задачи изучения дисциплины. Содержание и структура дисциплины. Основные термины и определения, использующиеся в материале.

Тема 1 Целые числа.

Виды и свойства целых чисел. Каноническое разложение Евклида. Факторизация числа. Получение простых чисел. Алгоритмы получения простых чисел. Теоремы алгоритмов получения простых чисел. Решето Эратосфена. Простые числа Эйлера. Простые числа Ферма. Простые числа Мерсенна.

Тема 2 Составные числа.

Каноническая форма. Общий делитель. Наибольший общий делитель. Алгоритм Евклида. Проблема нахождения наибольшего общего делителя. Алгоритм Евклида. Код алгоритма.

Тема 3 Бинарный алгоритм.

Утверждения бинарного алгоритма. Взаимно простые числа. Попарно взаимно простые числа. Сравнения. Сравнимы и не сравнимы по модулю. Вычет.

Тема 4 Свойства сравнений.

Определение свойств сравнений. Лемма. Определения. Пример леммы.

Тема 5 Алгоритм возведения в степень.

Свойства алгоритма. Пример работы алгоритма. Алгоритм быстрого возведения в степень. Пример работы алгоритма. Программная реализация.

Тема 6 Понятие вычета.

Определения. Полная система вычетов. Теорема Ферма. Свойства теоремы. Примеры.

Тема 7 Функция Эйлера.

Свойства функции Эйлера. Примеры. Теорема Эйлера. Примеры работы теоремы.

Тема 8 Линейные сравнения.

Определение. Возможные случаи для линейного сравнения. Примеры. Решение линейных сравнений. Алгоритмы решения линейных сравнений. Примеры работы алгоритма. Основные свойства.

Учебно-методическая карта учебной дисциплины «Математические основы криптологии»

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Литература	Формы контроля знаний
		лекции	Лабораторные занятия	Практические занятия	Управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
1	**Лекция № 1** *Введение в дисциплину.* Цели и задачи изучения дисциплины. Содержание и структура дисциплины. Основные термины и определения, использующиеся в материале.	2				Осн. лит.: [1], [2]. Доп. лит.: [1].	Устный опрос
2	**Лекция № 2** *Тема 1 Целые числа.* Виды и свойства целых чисел. Каноническое разложение Евклида. Факторизация числа. Получение простых чисел. Алгоритмы получения простых чисел. Теоремы алгоритмов получения простых чисел. Решето Эратосфена. Простые числа Эйлера. Простые числа Ферма. Простые числа Мерсенна. *Лабораторная работа №1* Реализация алгоритмов получения простых чисел и их оценка.	2	2			Осн. лит.: [3, Глава 1 стр. 6-20], Доп. лит.: [1], [2].	Защита лабораторной работы
3	**Лекция № 3** *Тема 2 Составные числа.* Каноническая форма. Общий делитель. Наибольший общий делитель. Алгоритм Евклида. Проблема	2				Осн. лит.: [3, Глава 1 стр. 20-22]. Доп. лит.: [1], [2].	Защита лабораторной работы

	нахождения наибольшего общего делителя. Алгоритм Евклида. Код алгоритма. *Лабораторная работа №2* Реализация алгоритма Евклида для нахождения наибольшего общего делителя.		2				
4	**Лекция № 4** *Тема 3 Бинарный алгоритм.* Утверждения бинарного алгоритма. Взаимно простые числа. Попарно взаимно простые числа. Сравнения. Сравнимы и не сравнимы по модулю. Вычет. *Лабораторная работа №3* Реализация бинарного алгоритма.	2	2			Осн. лит.: [3, Глава 1 стр. 20-59]. Доп. лит.: [2].	Защита лабораторной работы
5	**Лекция № 5** *Тема 4 Свойства сравнений.* Определение свойств сравнений. Лемма. Определения. Пример леммы. *Лабораторная работа №4* Реализация алгоритма возведения в степень.	2	2			Осн. лит.: [3, Глава 2 стр. 4-19]. Доп. лит.: [1], [2].	Защита лабораторной работы
6	**Лекция № 6** *Тема 5 Алгоритм возведения в степень.* Свойства алгоритма. Пример работы алгоритма. Алгоритм быстрого возведения в степень. Пример работы алгоритма. Программная реализация. *Лабораторная работа №5* Реализация быстрого алгоритма возведения в степень.	2	2			Осн. лит.: [3, Глава 2 стр. 19-32]. Доп. лит.: [2].	Защита лабораторной работы
7	**Лекция №7** *Тема 6 Понятие вычета.* Определения. Полная система вычетов. Теорема Ферма. Свойства теоремы. Примеры. *Лабораторная работа №6* Реализация теоремы Ферма.	2	2			Осн. лит.: [1], [2], [3, Глава 3 стр. 4-19]. Доп. лит.: [1], [2].	Защита лабораторной работы

8	**Лекция №8** *Тема 7 Функция Эйлера.* Свойства функции Эйлера. Примеры. Теорема Эйлера. Примеры работы теоремы. *Лабораторная работа №7* Реализация функции Эйлера.	2	2			Осн. лит.: [2], [3], [4].	Защита лабораторной работы
9	**Лекция №9** *Тема 8 Линейные сравнения.* Определение. Возможные случаи для линейного сравнения. Примеры. Решение линейных сравнений. Алгоритмы решения линейных сравнений. Примеры работы алгоритма. Основные свойства. *Лабораторная работа №8* Реализация алгоритмов решения линейных сравнений.	2	2			Осн. лит.: [1], [2], [3, Глава 3 стр. 29-69]. Доп. лит.: [1], [2].	Защита лабораторной работы
	Всего (34 часа)	**18**	**16**				

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

ОСНОВНАЯ

1. Панкратова, И. А. Булевы функции в криптографии [Электронный ресурс]: учебное пособие / И. А. Панкратова. — Санкт-Петербург: Лань, 2019. — 92 с. // Лань: электронно-библиотечная система. – Режим доступа: URL: https://e.lanbook.com/book/113402.

2. Введение в теоретико-числовые методы криптографии [Электронный ресурс]: учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург: Лань, 2011. — 400 с.// Лань: электронно-библиотечная система. — Режим доступа: URL: https://e.lanbook.com/book/68466

3. Математические и компьютерные основы криптологии: учебное пособие/ Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич - Минск: Новое знание, 2003. - 381 с. - Допущено М-вом образования РБ в качестве учебного пособия для студ. матем. и инженерно-техн. спец. вузов.

4. Харин, Ю.С. Компьютерный практикум по математическим методам защиты информации: учебное пособие. - Минск: БГУ, 2001. - 190 с. : ил. - Допущено Министерством образования Республики Беларусь в качестве учебного пособия для студентов математических и инженерно-технических специальностей высших учебных заведений.

5. Кирпичников, А. П. Криптографические методы защиты компьютерной информации [Электронный ресурс]: учебное пособие / А. П. Кирпичников, З. М. Хайбуллина. – Казань: Казанский научно-исследовательский технологический университет (КНИТУ), 2016. – 100 с. – Режим доступа: по подписке: URL: https://biblioclub.ru/index.php?page=book&id=560536

6. Ищукова, Е. А. Криптографические протоколы и стандарты [Электронный ресурс]: учебное пособие / Е. А. Ищукова, Е. А. Лобова; Южный федеральный университет, Инженерно-технологическая академия. – Таганрог: Южный федеральный университет, 2016. – 80 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=493059

7. Фомичев, В. М. Дискретная математика и криптология [Электронный ресурс]: курс лекций / В. М. Фомичев; под общ. ред. Н. Д. Подуфалова. – Москва: Диалог-МИФИ, 2003. – 397 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=89387

Бурякова Е.В.

ДОПОЛНИТЕЛЬНАЯ

8. Хорстманн, К.С. Java. Библиотека профессионала = Core Java. - Москва ; Санкт-Петербург : Диалектика, 2020. - ил. - ISBN 978-5-907144-30-9(рус.). - ISBN 978-0-13-516630-7(англ.). Том 2 : Расширенные средства программирования. - 2019. - 968 с.

9. Шилдт, Г. Java. Полное руководство = Java. The Complete Reference. - 10-е издание. - Санкт-Петербург : Диалектика, 2020. - 1488 с. : ил.

10. Оукс, С. Эффективный Java. Тюнинг кода на Java 8,11 и дальше = In-Depth Fdvice for Tuning and Programming Java 8, 11, and Beyond / [перевод с английского Е. Матвеев]. - второе издание. - Санкт-Петербург : Питер, 2021. - 494 с.

11. Лафоре, Р. Структуры данных и алгоритмы Java = Data Struktures & Algorithms in Java / [перевод с английского Е. Матвеев]. - второе издание. - Санкт-Петербург : Питер, 2018. - 701 с. : ил. - (Классика computer science). - Библиогр. : с. 683-685.

ПЕРЕЧЕНЬ ТЕМ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Лабораторная работа №1 Реализация алгоритмов получения простых чисел и их оценка.

Лабораторная работа №2 Реализация алгоритма Евклида для нахождения наибольшего общего делителя.

Лабораторная работа №3 Реализация бинарного алгоритма.

Лабораторная работа №4 Реализация алгоритма возведения в степень.

Лабораторная работа №5 Реализация быстрого алгоритма возведения в степень.

Лабораторная работа №6 Реализация теоремы Ферма.

Лабораторная работа №7 Реализация функции Эйлера.

Лабораторная работа №8 Реализация алгоритмов решения линейных сравнений.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

Вопросы по теоретической части дисциплины

1. Основные понятия теории чисел. Теорема делимости.
2. Наибольший общий делитель и алгоритм Евклида.
3. Цепные дроби и алгоритм Евклида.
4. Наименьшее общее кратное. Простые числа.
5. Теоремы Евклида о простых числах. Решето Эратосфена.
6. Основные свойства простых чисел. Теорема единственности разложения на простые сомножители.
7. Теорема о делителях числа и ее следствия.
8. Асимптотический закон распределения простых чисел.
9. Функция Эйлера и ее свойства.
10. Тест Ферма на простоту. Числа Кармайкла. Теорема Кармайка.
11. Сравнения. Свойства сравнений.
12. Полная система вычетов, приведенная система вычетов. Алгебраические свойства, обратный элемент.
13. Теорема Элера, теорема Ферма. Следствие.
14. Применение теоремы Ферма в криптосистеме.
15. Сравнение с одним неизвестным 1-ой степени.
16. Система сравнений 1-ой степени. Теорема об остатках.
17. Квадратичные сравнения по простому модулю.
18. Решение линейных сравнений.
19. Бинарный алгоритм. Взаимно простые числа.
20. Составные числа. Каноническая форма.
21. Целые числа. Каноническое разложение Евклида.
22. Алгоритмы получения простых чисел.
23. Сравнения и вычет. Сравнимы и не сравнимы по модулю.
24. Число решений квадратичного сравнения по модулю.
25. Простые числа Ферма и Мерсенна. Следствие.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение дисциплине «Математические основы криптологии» предполагает реализацию следующих форм самостоятельной работы студентов:

– проработка конспекта лекций и учебной литературы;

– изучение печатных источников по теме дисциплины;

– изучение профессиональных электронных ресурсов по теме дисциплины;

– изучение вопросов для самоконтроля;

– подготовка к аудиторному выполнению лабораторных работ (предварительное знакомство с методическими указаниями, программным обеспечением, вариантом индивидуального задания по работе);

– решение индивидуальных задач при подготовке к лабораторным занятиям;

– выполнение практических упражнений (работа с тренажерами) для закрепления знаний и навыков;

– подготовка к защите лабораторных работ (оформление отчёта по индивидуальному варианту задания, защита результатов работы и демонстрации степени освоения навыков и умений по конкретной теме);

– решение во внеурочное время контрольных задач, получаемых на лекциях;

– углублённое изучение отдельных тем учебной дисциплины для подготовки к устным опросам;

– изучение основной и дополнительной и научной литературы в процессе подготовки к анализу и решению проблемных задач, реализации элементов исследовательской деятельности;

– подготовка к промежуточной и текущей диагностике компетенции (письменным контрольным работам);

– систематизация полученных знаний при подготовке к зачету.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации образовательного процесса, обеспечиваются:

– наличием и использованием в образовательном процессе открытых систем автоматизированного тестирования при использовании бесплатного сервиса для учебных заведений, некоммерческих организаций и пользователей личных аккаунтов Google – Google Класс, которые доступны пользователям через Интернет в любое удобное для них время;

– использованием бизнес-мессенджера для групповой работы и общения Microsoft Teams;

– использованием «облачных» технологий, в частности облачного хранилища файлового хостинга компании Dropbox для размещения материалов по читаемой дисциплине;

– наличием и полной доступностью электронных вариантов курса лекций и учебно-методических указаний по основным разделам дисциплины.

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Материалы, размещённые на бесплатном сервисе для учебных заведений, некоммерческих организаций и пользователей личных аккаунтов Google Класс Room университета: шифр курса **ZETJSNJ**.
2. Материалы, размещённые в бизнес-мессенджере для групповой работы и общения Microsoft Teams: шифр курса **40F48GC.**
3. Методические указания к выполнению лабораторных работ по дисциплине «Математические основы криптологии» для студентов специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)».

Содержание самостоятельной работы студентов

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Самостоятельное изучение отдельных вопросов по темам дисциплины при подготовке к выполнению и защите лабораторных работ	*Тема 1 Целые числа.* Виды и свойства целых чисел. Каноническое разложение Евклида. Факторизация числа. Получение простых чисел. Алгоритмы получения простых чисел. Теоремы алгоритмов получения простых чисел. Решето Эратосфена. Простые числа Эйлера. Простые числа Ферма. Простые числа Мерсенна.	2
	Лабораторная работа №1 Реализация алгоритмов получения простых чисел и их оценка.	2
	Тема 2 Составные числа. Каноническая форма. Общий делитель. Наибольший общий делитель. Алгоритм Евклида. Проблема нахождения наибольшего общего делителя. Алгоритм Евклида. Код алгоритма.	2
	Лабораторная работа №2 Реализация алгоритма Евклида для нахождения наибольшего общего делителя.	2
	Тема 3 Бинарный алгоритм. Утверждения бинарного алгоритма. Взаимно простые числа. Попарно взаимно простые числа. Сравнения. Определение. Сравнимы и не сравнимы по модулю. Вычет.	2
	Лабораторная работа №3 Реализация бинарного алгоритма.	2
	Тема 4 Свойства сравнений. Определение свойств сравнений. Лемма. Определение. Пример леммы.	2
	Лабораторная работа №4 Реализация алгоритма возведения в степень.	2
	Тема 5 Алгоритм возведения в степень. Свойства алгоритма. Алгоритм быстрого возведения в степень. Пример работы алгоритма. Программная реализация.	2
	Лабораторная работа №5 Реализация быстрого алгоритма возведения в степень.	2
	Тема 6 Понятие вычета. Определение. Полная система вычетов. Теорема Ферма. Свойства теоремы. Примеры.	2
	Лабораторная работа №6 Реализация теоремы Ферма.	2
	Тема 7 Функция Эйлера. Свойства функции Эйлера. Примеры. Теорема Эйлера. Примеры работы теоремы.	2

	Лабораторная работа №7 Реализация функции Эйлера.	2
	Тема 8 Линейные сравнения. Определение. Возможные случаи для линейного сравнения. Примеры. Решение линейных сравнений. Алгоритмы решения линейных сравнений. Примеры работы алгоритма. Основные свойства.	2
.	*Лабораторная работа №8* Реализация алгоритмов решения линейных сравнений.	2
	Всего	**38**

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Контроль качества усвоения знаний проводится в соответствии с Положением о рейтинговой системе оценки знаний и компетенций студентов (приказ ректора УО ПГУ № 294 от 06.06.2014 (в редакции, утверждённой приказом № 605 от 17.11.2014) в форме промежуточного контроля и текущей аттестации.

Для оценивания самостоятельной и аудиторной работы студентов в рамках дисциплины используется накопительная система контроля успеваемости, которая предполагает суммирование бальных оценок, выставляемых в электронный журнал за все виды работ в течение прохождения курса для определения среднеарифметических показателей успеваемости.

Мероприятия промежуточного контроля проводятся в течение семестра и включают в себя следующие формы контроля:

– устная форма (блиц-опрос на лекциях);

– устно-письменная форма (защита лабораторных работ).

Промежуточная (аттестационная) диагностика компетенции студентов осуществляется на основании индивидуального рейтинга студента на момент аттестации. Для положительной аттестации (промежуточного контроля успеваемости) необходимо согласно календарному плану выполнить все лабораторные работы и индивидуальные задания, а также иметь положительную оценку по промежуточному контролю освоения теоретической части курса.

Результат *промежуточного контроля за семестр* оценивается отметкой в баллах по десятибалльной шкале и выводится, исходя из отметок, выставленных в ходе проведения мероприятий промежуточного контроля в течение семестра по следующей формуле:

$$П=(ПК_1+ПК_2+...+ПК_n)/n,$$

где $ПК_1$... $ПК_n$–отметки, выставленные в ходе проведения мероприятий промежуточного контроля,

n – количество мероприятий промежуточного контроля.

Результат промежуточного контроля рассчитывается как округлённое среднее значение. Результат может быть увеличен в соответствии с п.п. 6.8 и 6.9 Положения.

Текущая аттестация проводится в форме зачёта.

Зачёт проводится согласно Положению.

Заключение о *зачёте* формируется на основе накопительного принципа по формуле:

$$З = k \cdot П,$$

где k– весовой коэффициент промежуточного контроля;

П – результат промежуточного контроля за семестр.

Весовой коэффициент k принимается равным 1.

Если полученная отметка $З < 4$ баллов, то проводится устный зачёт отдельно по представленным в программе вопросам.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основные методы (технологии) обучения, отвечающие целям и задачам учебной дисциплины:

– проблемное обучение (проблемное изложение, вариативное изложение), реализуемое на лекционных занятиях;

– учебно-исследовательская деятельность, реализация творческого подхода, реализуемые на лабораторных занятиях.

Используемые технологии обучения и диагностики компетенций в преподавании дисциплины «Математические основы криптологии» реализуют подход, основанный на максимально возможном использовании внутренней и учебной мотивации студента, проявляющейся в чётком понимании им значимости всех видов выполняемых работ, как с точки зрения важности для профессиональной подготовки, так и с точки зрения оценивания. Подход предполагает использование элементов проблемного обучения и элементов исследовательской деятельности студентов в процессе аудиторной работы, а также при выполнении самостоятельных работ при постоянном рейтинговом контроле.

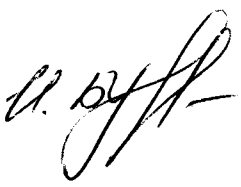
На лекционных занятиях по дисциплине «Математические основы криптологии» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Изучение учебной дисциплины осуществляется на лекционных и лабораторных занятиях. На лекционных занятиях студенты овладевают системой теоретических знаний в области построения эффективных алгоритмов для разнообразных задач дискретной и комбинаторной оптимизации с использованием различных структур данных. В ходе лекционного изложения теоретических сведений используются традиционные словесные приёмы и методы, которые активизируются постановкой проблемных вопросов и заданий, организацией учебных дискуссий с опорой на имеющуюся начальную подготовку студентов и их политехнический кругозор, использованием интерактивных методов обучения.

На лабораторных занятиях развиваются и формируются необходимые практические умения и навыки построения и реализации алгоритмов и методов защиты информации. Применяется индивидуальный, творческий подход. Студенты получают от преподавателя индивидуальные задания, в рамках самостоятельной работы разрабатывает свои алгоритмы их решения с последующими реализациями на некотором языке программирования и проверкой их работоспособности на компьютере, а также доказывают эффективность. Также во время проведения лабораторных работ особое внимание уделяется формированию у студентов умения планировать свою работу и определять эффективную последовательность её выполнения.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, по которой требуется согласование	**Название кафедры**	**Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине**	**Решение, принятое кафедрой, разработавшей учебную программу**
«Исследование операций»	Кафедра математики и компьютерной безопасности	нет	
«Методы оптимизации»	Кафедра математики и компьютерной безопасности	нет	

Заведующий кафедрой математики и компьютерной безопасности, к.ф.-м.н., доцент  И.Б. Бураченок