Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и
образовательным инновациям
_____ О.И. Чуприс
«__» _____ 2019 г.

Регистрационный № УД-7840/уч.

ТЕОРЕТИКО-ЧИСЛОВЫЕ АЛГОРИТМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности

1-31 80 03 Математика и компьютерные науки
профилизации
Веб-программирование и интернет технологии
Математическое и программное обеспечение мобильных устройств

2019 г.

Учебная программа составлена на основе образовательного стандарта ОСВО 1-31 80 03-2019 и учебных планов: G31-031/уч., G31з-032/уч., G31з-034/уч., G31-033/уч от 11.04.2019.

СОСТАВИТЕЛИ:
Васильев Д. В. – доцент кафедры высшей алгебры и зашиты информации механико-математического факультета Белорусского государственного университета, кандидат физико-математических наук.

РЕЦЕНЗЕНТ
Берник В.И. – главный научный сотрудник Института математики НАН Беларуси, доктор физико-математических наук, профессор.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой высшей алгебры и защиты информации
Белорусского государственного университета
(протокол № 10 от 23.05.2019);

Научно-методическим советом
Белорусского государственного университета
(протокол № 5 от 28.06.2019).

Зав. кафедрой высшей алгебры
и защиты информации, профессор В.В. Беняш-Кривец

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

За последние десятилетия такие направления научного исследования как криптография и компьютерная безопасность стали особенно актуальны для развития современного общества. Владение знаниями и навыками по этим специальностям, стало насущной необходимостью в работе любого специалиста естественнонаучного профиля. Эти дисциплины находятся на стыке нескольких научных и технических направлений, но особо важную роль в них играют математические методы и алгоритмы обеспечения информационной безопасности. Программа дисциплины «Теоретико-числовые алгоритмы информационной безопасности» охватывает ту часть этих дисциплин, которая непосредственно относится к математическим методам, используемым при построении современных криптосистем. Цель дисциплины «Теоретико-числовые алгоритмы информационной безопасности» – обучить магистрантов математическим методам, лежащим в основе построения и работы современных криптосистем.

Образовательная цель: ознакомить магистрантов с методами обеспечения компьютерной и сетевой безопасности; дать математическое обоснование алгоритмов криптографии с открытым ключом; познакомить студентов с некоторыми методами анализа криптосистем.

Развивающая цель: формирование у магистрантов понимания принципов построения и работы современных систем защиты информации, формирование алгоритмического мышления и общей математической культуры, привитие студентам умения самостоятельно изучать учебную и научную литературу в области математики.

Основные задачи, решаемые в рамках изучения дисциплины «Теоретико-числовые алгоритмы информационной безопасности»:

- знакомить студентов с важнейшими алгоритмами, применяющимися в криптографии;
- ознакомить студентов с криптографическими системами с открытым ключом;
- ознакомить студентов с алгоритмами цифровой подписи на эллиптических кривых ECDSA, ГОСТ Р 34.10-2012, СТБ 34.101.45-2013.
- развить у студентов аналитическое мышление и общую математическую культуру;
- привить студентам умение самостоятельно изучать учебную и научную литературу в области математики.

В результате изучения учебной дисциплины студент должен

знать:

– общие математические основы построения криптосистем с открытым ключом;

– протоколы работы широко используемых криптосистем,

– требования, налагаемые на параметры широко используемых криптосистем таких как шифрование с открытым ключом, цифровая подпись, распределение секретных ключей.

уметь:

– с помощью расширенного алгоритма Евклида решать линейные сравнения по произвольному модулю и находить обратные элементы в кольце вычетов;

- применять китайскую теорему об остатках для ускорения выполнения арифметических операций с большими числами;

– вычислять степени элементов группы с помощью различных версий бинарного алгоритма;

– уметь решать алгебраические уравнения над простым конечным полем;

– находить элементы заданного порядка в циклических группах;

владеть:

– методами оценки сложности алгоритмов

– умножением целых чисел по методу Карацубы;

– умножением в кольце вычетов по методам Монтгомери и Баррета;

– методами тестирования простоты чисел Миллера-Рабина и некоторыми детерминированные тестами, а также алгоритмами для построения больших простых чисел;

– методами выполнения операции в группе точек эллиптической кривой;

– алгоритмами генерации и проверки электронной цифровую подписи по схеме Эль-Гамаля, ECDSA, ГОСТ Р 34.10-2012, СТБ 34.101.45-2013.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием (магистра).

Учебная дисциплина «Теоретико-числовые алгоритмы информационной безопасности» относится: к модулю «Распределенные приложения и криптотехнологии», компонент учреждения высшего образования профилизации «Веб-программирование и интернет технологии»; к модулю «Компьютерная безопасность и защита информации», компонент учреждения высшего образования профилизации «Математическое и программное обеспечение мобильных устройств».

Связи с другими учебными дисциплинами, включая учебные дисциплины компонента учреждения высшего образования, дисциплины специализации и др. Наиболее тесной является связь данной дисциплины с такой дисциплиной как «Криптотехнологии». Данная дисциплина опирается и использует изученные

ранее сведения из дисциплин «Алгебра и теория чисел», «Дополнительные главы алгебры», «Теоретико-числовые методы в криптографии».

Требования к компетенциям специалиста

Освоение учебной дисциплины «Теоретико-числовые алгоритмы информационной безопасности» должно обеспечить формирование следующей **специализированной компетенции:**

профилизация «Веб-программирование и интернет технологии»:

СК-4. Быть способным применять ключевые методы проектирования и защиты информационных систем для реализации устойчивых распределенных и криптоприложений.

профилизации «Математическое и программное обеспечение мобильных устройств»:

СК-4. Бьггь способным применять технологии защиты информации при проектировании мобильных приложений.

Структура учебной дисциплины.

Дисциплина изучается в 1 семестре. Всего на изучение учебной дисциплины «Теоретико-числовые алгоритмы информационной безопасности» профилизаций «Веб-программирование и интернет технологии» и «Математическое и программное обеспечение мобильных устройств» отведено 108 часов, в том числе:

- для очной формы получения высшего образования – 54 аудиторных часа, из них: лекции – 36 часов, лабораторные занятия – 18 часов;

- для заочной формы получения высшего образования – 12 аудиторных часов, из них: лекции – 8 часов, лабораторные занятия – 4 часа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма текущей аттестации по учебной дисциплине – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Теоретико-числовые основы.

Делимость в кольце целых чисел. НОД, НОК, разрешимость линейного диофантового уравнения.

Закон распределения простых чисел, оценки расстояний между соседними простыми числами.

Алгоритм Евклида, расширенный алгоритм Евклида, оценка сложности алгоритма Евклида.

Сравнения, их свойства, решение линейного сравнения, китайская теорема об остатках, мультипликативные функции, функция Эйлера, теорема Эйлера, малая теорема Ферма.

Квадратичные вычеты. Символ Лежандра. Теорема Эйлера для квадратичных вычетов, Квадратичный закон взаимности. Символы Якоби. Вычисление символа Лежандра.

Первообразные корни. Структура мультипликативной группы кольца вычетов.

Тема 2. Базовые алгоритмы.

Сложность алгоритмов: полиномиальные, субэкспоненциальные, экспоненциальные алгоритмы. Примеры.

Бинарные алгоритмы возведения в степень. Метод скользящего окна. Алгоритм решения квадратичных сравнений. Общий алгоритм решения полиномиальных сравнений.

Метод Карацубы для умножения целых чисел. Умножение целых чисел при помощи китайской теоремы об остатках. Операция Монтгомери и редукция Баррета.

Тема 3. Тесты на простоту.

Детерминированный тест на простоту, тест Миллера-Рабина. Алгоритм построения больших простых чисел. Алгоритм нахождения элемента циклической группы с заданным порядком.

Тема 4. Эллиптические кривые

Эллиптические кривые, группа точек эллиптической кривой. Вывод формул сложения. Алгоритм вычисления кратной точки.

Эффективные методы вычисления операции сложения точек эллиптической кривой. Кривые в форме Вейерштрасса, Монтгомери, Эдвардса.

Тема 5. Криптосистемы с открытым ключом

Криптосистема RSA. Алгоритм Диффи-Хеллмана распределения ключей. Схема цифровой подписи Эль-Гамаля. Алгоритмы цифровой подписи на эллиптических кривых ECDSA, ГОСТ Р 34.10-2012, СТБ 34.101.45-2013.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	Теоретико-числовые основы.	12			6			Отчет по лабораторной работе с устной защитой. Тест.
2.	Базовые алгоритмы.	4			2			Отчет по самостоятельной работе с устной защитой
3.	Тесты на простоту.	4			2			Экспресс-опрос
4.	Эллиптические кривые	4			2			Отчет по лабораторной работе с устной защитой.
5.	Криптосистемы с открытым ключом	12			6			Отчет по лабораторной работе с устной защитой. Контрольная работа
	Итого	36			18			

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Заочная форма получения образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	Теоретико-числовые основы.	1						Отчет по лабораторной работе с устной защитой.
2.	Базовые алгоритмы.	1			1			Отчет по самостоятельной работе с устной защитой
3.	Тесты на простоту.	2			1			Экспресс-опрос
4.	Эллиптические кривые	2			1			Отчет по лабораторной работе с устной защитой.
5.	Криптосистемы с открытым ключом	2			1			Отчет по лабораторной работе с устной защитой. Контрольная работа
	Итого	8			4			

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Харин Ю.С., Агиевич СВ., Васильев Д.В., Матвеев Г.В. Криптология. (Учебник с грифом Минобразования). Минск: БГУ, 2014. 512 с
2. Босс В. Лекции по математике:Теория чисел Т.14. URSS, 2019. 214 с.
3. Виноградов И.М. Основы теории чисел. Лань: Спб, 2019. 176 с.
4. Василенко ОН. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003. 328 с.
5. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Книга 1: алгебраические и алгоритмические основы. URSS, 2019. 376 С.
6. Кнут Д. Искусство программирования на ЭВМ, т.2. Москва: Издательский дом «Вильямс», 2001.

Перечень дополнительной литературы

1. Нестеренко Ю.В. Теория чисел. М.: Академия, 2008. 272 с.
2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2012. 815 с.
3. Применко А. Алгебраические основы криптографии. URSS, 2018. 288 с.
4. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации для изучающих компьютерную безопасность. URSS, 2019.473 с.

Перечень рекомендуемых средств диагностики и методика формирования итоговой оценки

Формой текущей аттестации по дисциплине «Теоретико-числовые алгоритмы информационной безопасности» учебным планом предусмотрен экзамен.

Контроль работы магистранта проходит в форме собеседования, выполнения самостоятельных работ и практических упражнений в аудитории, а также самостоятельной работы вне аудитории с предоставлением отчета с его устной защитой. Задания к самостоятельным работам составляются согласно содержанию учебного материала.

Экзамен по дисциплине проходит в устной форме. При формировании итоговой оценки используется рейтинговая оценка знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний и текущей аттестации в рейтинговую оценку:

Формирование оценки за текущую успеваемость:

– ответы на лекциях – 20 %;

– отчеты по лабораторным работам – 40 %;

– выполнение контрольной работы – 40 %.

Рейтинговая оценка по дисциплине рассчитывается на основе оценки текущей успеваемости и экзаменационной оценки с учетом их весовых коэффициентов. Весовой коэффициент текущей успеваемости – 0.4, весовой коэффициент экзаменационной оценки – 0.6.

Итоговая оценка формируется на основе 3-х документов:

1. Правила проведения аттестации студентов, курсантов, слушателей при освоении содержания образовательных программ высшего образования (Постановление Министерства образования Республики Беларусь №53 от 29.05.2012 г.).

2. ПОЛОЖЕНИЕ о рейтинговой системе оценки знаний студентов по дисциплине в Белорусском государственном университете (Приказ ректора БГУ № 382-ОД от 18.08.2015 г. (с изменениями, согласно приказу 491-ОД от 29.08.2018г.)

3. Критерии оценки знаний и компетенций студентов по 10-балльной шкале (Письмо Министерства образования Республики Беларусь от 22.12.2003 г. № 21-04-1/105).

Описание инновационных подходов и методов к преподаванию учебной дисциплины (эвристический, проектный, практико-ориентированный)

При организации образовательного процесса используется ***эвристический подход,*** который предполагает**:**

– осуществление студентами личностно-значимых открытий окружающего мира;

– демонстрацию многообразия решений большинства профессиональных задач и жизненных проблем;

– творческую самореализацию обучающихся в процессе создания образовательных продуктов;

– индивидуализацию обучения через возможность самостоятельно ставить цели, осуществлять рефлексию собственной образовательной деятельности.

При организации образовательного процесса используется ***практико-ориентированный подход,*** который предполагает***:***

– освоение содержание образования через решения практических задач;

– приобретение навыков эффективного выполнения разных видов профессиональной деятельности;

– ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;

– использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

При организации образовательного процесса ***используется метод проектного обучения,*** который предполагает***:***

– способ организации учебной деятельности студентов, развивающий актуальные для учебной и профессиональной деятельности навыки планирования, самоорганизации, сотрудничества и предполагающий создание собственного продукта;

– приобретение навыков для решения исследовательских, творческих, социальных, предпринимательских и коммуникационных задач.

Методические рекомендации по организации и выполнению самостоятельной работы студентов

Самостоятельная работа студентов - это любая деятельность, связанная с воспитанием мышления будущего профессионала. В широком смысле под самостоятельной работой следует понимать совокупность всей самостоятельной деятельности студентов как в учебной аудитории, так и вне её, в контакте с преподавателем и в его отсутствии.

Самостоятельная работа реализуется:

1. Непосредственно в процессе аудиторных занятий - на лекциях.

2. В контакте с преподавателем вне рамок расписания - на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.

3. В библиотеке, дома, в общежитии, на кафедре при выполнении студентом учебных и творческих задач.

При изучении дисциплины организация самостоятельной работы студентов должна представлять единство трех взаимосвязанных форм:

1. Внеаудиторная самостоятельная работа;

2. Аудиторная самостоятельная работа, которая осуществляется под непосредственным руководством преподавателя;

3. Творческая, в том числе научно-исследовательская работа.

Примерный перечень вопросов к экзамену

1. Делимость в кольце целых чисел. НОД, НОК, разрешимость линейного диофантового уравнения.
2. Закон распределения простых чисел, оценки расстояний между соседними простыми числами.
3. Алгоритм Евклида, расширенный алгоритм Евклида, оценка сложности алгоритма Евклида.
4. Сравнения, их свойства, решение линейного сравнения.
5. Китайская теорема об остатках.
6. Мультипликативные функции, функция Эйлера.
7. Теорема Эйлера, малая теорема Ферма.
8. Квадратичные вычеты. Символ Лежандра. Теорема Эйлера для квадратичных вычетов.
9. Квадратичный закон взаимности. Символы Якоби. Вычисление символа Лежандра.
10. Первообразные корни. Структура мультипликативной группы кольца вычетов.
11. Сложность алгоритмов: полиномиальные, субэкспоненциальные, экспоненциальные алгоритмы. Примеры.
12. Бинарные алгоритмы возведения в степень. Метод скользящего окна.
13. Алгоритм решения квадратичных сравнений. Общий алгоритм решения полиномиальных сравнений.
14. Метод Карацубы для умножения целых чисел. Умножение целых чисел при помощи китайской теоремы об остатках.

15. Операция Монтгомери и редукция Баррета.
16. Детерминированный тест на простоту.
17. Тест Миллера-Рабина.
18. Алгоритм построения больших простых чисел.
19. Алгоритм нахождения элемента циклической группы с заданным порядком.
20. Эллиптические кривые, группа точек эллиптической кривой.
21. Вывод формул сложения. Алгоритм вычисления кратной точки.
22. Эффективные методы вычисления операции сложения точек эллиптической кривой.
23. Кривые в форме Вейерштрасса, Монтгомери, Эдвардса.
24. Криптосистема RSA.
25. Алгоритм Диффи-Хеллмана распределения ключей.
26. Схема цифровой подписи Эль-Гамаля.
27. Алгоритм цифровой подписи на эллиптических кривых ECDSA.
28. Алгоритм цифровой подписи на эллиптических кривых ГОСТ Р 34.10-2012.
29. Алгоритм цифровой подписи на эллиптических кривых СТБ 34.101.45-2013.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Криптотехнологии	Высшей алгебры и защиты информации	нет	Изменения не требуются (протокол № 10 от 23.05.2019)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ
на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры Высшей алгебры и защиты информации (протокол № ____ от _____ 20__ г.)

Заведующий кафедрой

_____ _____ _____
(степень, звание) (подпись) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____
(степень, звание) (подпись) (И.О.Фамилия)

РЕЦЕНЗИЯ

на учебную программу дисциплины

«Теоретико-числовые алгоритмы

информационной безопасности»

Программа курса «Теоретико-числовые алгоритмы информационной безопасности» для магистрантов 1 курса очной и заочной формы обучения предполагается изучение базовых математических понятий и алгоритмов, на которых основаны современные криптосистемы, а также методы обеспечения компьютерной безопасности, использующиеся при организации сетевого взаимодействия. В курсе рассматриваются основные понятия теории чисел, необходимые для построения криптосистем с открытым ключом, а также базовые алгоритмы, использующиеся при работе таких криптосистем. В третьей части курса рассмотрены основные криптосистемы для шифрования (RSA), цифровой подписи стандарты ECDSA и СТБ для формирования и проверки электронной цифровой подписи, а также алгоритм распределения секретного ключа Диффи-Хеллмана.

Материалы, включенные в курс, являются необходимым минимумом для понимания работы современных методов защиты информации и обеспечения компьютерной безопасности. Рецензируемая программа рекомендуется в качестве учебной программы учреждения высшего образования второй ступени (магистратуры) по учебной дисциплине специальности 1-31 80 03 «Математика и компьютерные науки», профилизации «Веб-программирование и интернет-технологии», «Математическое и программное обеспечение мобильных устройств».

Рецензент

Доктор физико-математических наук, профессор,

главный научный сотрудник Института математики

НАН Беларуси В.И. Берник

Подпись В.И. Берника заверяю:

Ведущий специалист по кадрам Института математики НАН Беларуси

Г.И. Анисенко

22.05.2019