Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и
образовательным инновациям
_____ О. И. Чуприс
«10» 10 2018 г.

Регистрационный № УД-6264 /уч.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

**Учебная программа учреждения высшего образования
по учебной дисциплине для специальности первой ступени высшего образования:**

**1-31 03 07 Прикладная информатика (по направлениям)
направление специальности
1-31 03 07 – 01 Прикладная информатика
(программное обеспечение компьютерных систем)**

2018 г.

Учебная программа составлена на основе образовательного стандарта первой ступени высшего образования ОСВО 1-31 03 07-2013 и учебного плана G31-167/уч. от 30.05.2013, G31и-194/уч. от 30.05.2013.

СОСТАВИТЕЛЬ:

И.А. Бодягин, заведующий кафедрой математического моделирования и анализа данных факультета прикладной математики и информатики Белорусского государственного университета, кандидат физико-математических наук, доцент.

РЕЦЕНЗЕНТЫ:

А.И. Трубей, старший научный сотрудник учреждения Белорусского государственного университета «Научно-исследовательский институт прикладных проблем математики и информатики»;
В.И. Берник, главный научный сотрудник государственного научного учреждения «Институт математики Национальной академии наук Беларуси», доктор физико-математический наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математического моделирования и анализа данных Белорусского государственного университета (протокол № 6 от 6 ноября 2018 г.);

Научно-методическим Советом Белорусского государственного университета (протокол № 1 от 16 ноября 2018 г.).

Бод / Бодягин И.А., зав. кафедрой ММАД/

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Целью дисциплины «Криптографические методы» является изложение основных сведений о построении и анализе криптографических алгоритмов и протоколов, а также создание базы для освоения основных понятий и методов современной криптографии.

В рамках поставленной цели ***задачи*** учебной дисциплины состоят в следующем:

1) формирование представления о месте и роли криптографии в современном информационном обществе;
2) теоретическое освоение студентами основных положений дисциплины;
3) формирование необходимого уровня математической подготовки для понимания основ криптографии;
4) приобретение практических навыков решения типовых задач, способствующих усвоению основных понятий в их взаимной связи.
5) формирование системы основных понятий, используемых для описания криптографических методов, а также раскрытие взаимосвязи этих понятий.

Учебная дисциплина «Криптографические методы» относится к циклу специальных дисциплин государственного компонента.

Учебная программа составлена с учетом межпредметных связей с учебными дисциплинами. Так, основой для изучения дисциплины «Криптографические методы» являются дисциплины «Алгебра и теория чисел» и «Теория вероятностей и математическая статистика». Знания, полученные в результате изучения дисциплины, будут использованы при изучении дисциплины «Компьютерная безопасность распределенных систем», а также способствовать успешному прохождению производственной практики по специальности и подготовки дипломной работы.

В результате освоения учебной дисциплины студент должен:

знать:

- методы построения надежных блочных и поточных криптосистем, функций хэширования, криптосистем с открытым ключом и систем электронной цифровой подписи;
- задачи и основные методы криптоанализа;
- стандартные криптосистемы;

уметь:

- применять полученные знания для создания надежных систем защиты информации;

владеть:

- методами построения надежных криптосистем и функций хэширования;

- методами построения криптосистем с открытым ключом и систем электронной цифровой подписи;
- основными методами криптоанализа.

Освоение учебной дисциплины «Криптографические методы» должно обеспечить формирование следующих академических и профессиональных компетенций:

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 порождать новые идеи (обладать креативностью).

АК-6. Владеть междисциплинарным подходом при решении проблем.

профессиональные компетенции:

ПК-1. Проектировать, разрабатывать и тестировать программное обеспечение различных видов.

ПК-2. Разрабатывать техническую документацию на программное обеспечение.

ПК-7. Применять профессиональные знания и навыки для проведения научных исследований в области прикладной информатики

ПК-9. Работать с научно-технической информацией с использованием современных информационных технологий.

ПК-10. Формулировать выводы и рекомендации по применению результатов научно-исследовательской работы.

ПК-11. Пользоваться глобальными информационными ресурсами.

ПК-18. Оказывать консультации по вопросам работы программного обеспечения, в том числе разработанного сторонними организациями.

ПК-21. Анализировать результаты работы установленного программного обеспечения и вырабатывать предложения по улучшению качества его работы

ПК-23. Проводить обучение специалистов, занимающихся эксплуатацией программного обеспечения.

Структура содержания учебной дисциплины включает такие дидактические единицы, как темы (разделы), в соответствии с которыми разрабатываются и реализуются соответствующие лекционные и семинарские занятия. Примерная тематика занятий приведена в информационно-методической части.

Дисциплина изучается в 4 семестре. Всего на освоение учебной дисциплины «Криптографические методы» отведено 158 часов, в том числе 68 аудиторных часов, из них: лекции – 34 часа, лабораторные занятия – 30 часов, УСР – 4 часа.

Трудоемкость учебной дисциплины составляет 4 зачетные единицы.

Форма текущей аттестации – зачет и экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел I. Введение

Тема 1.1. Введение. История криптографии. Абоненты, коммуникации и угрозы. Задачи криптографии и криптоанализа. Криптосистемы (шифрсистемы).

Раздел II. Симметричная криптография

Тема 2.1. Алгебраические основы криптографии. Подстановки. Симметрические группы. Делимость чисел. Сравнение по модулю и его свойства. Разрешимость сравнений. Функция Эйлера е ее свойства. Теорема Эйлера. Обобщенный алгоритм Евклида. Проверка простоты. Построение простых чисел.

Тема 2.2. Элементы теории Шеннона. Классические криптосистемы. Шифр сдвига. Аффинный шифр. Шифр простой замены. Шифр Хилла. Шифр перестановки. Шифр Виженера. Модель противника. Совершенные криптосистемы. Пессимистическое утверждение Шеннона. Шифр Вернама. Расстояние единственности.

Тема 2.3. Блочные криптосистемы. Блочно-итерационные криптосистемы. Криптосистемы подстановки-перестановки. Использование инволютивных подстановок. Криптосистемы Фейстеля. DES. ГОСТ 2814-89. AES. Режимы шифрования.

Тема 2.4. Криптоанализ. Задачи криптоанализа. Сложность атак. Частотная атака. Атака «грубой силой». Простые соотношения. Баланс «время – память».

Тема 2.5. Поточные криптосистемы. Конечные автоматы. Регистры сдвига с линейной обратной связью. Линейная рекуррентная последовательность. Характеристический многочлен. Периодичность. Постулаты Голомбо. Фильтрующий генератор. Комбинирующий генератор. Генератор с неравномерным движением. Криптосистема A5/1. Сжимающий и самосжимающий генератор. Линейная сложность.

Раздел III. Асимметричная криптография

Тема 3.1. Протокол Диффи-Хэллмана. Протокол Диффи-Хэллмана для двух и более участников. Атака «Человек по-середине». Сертификаты открытых ключей.

Тема 3.2. Криптосистема RSA. Криптосистема RSA. RSA и факторизация. Атаки на RSA.

Тема 3.3. Функции хэширования. Определение и использования. Задачи криптоанализа. Связь между задачами криптоанализа. Блочно-

итерационные функции хэширования. Шаговые функции хэширования. Атака «дней рождения».

Тема 3.4. Электронная цифровая подпись. Определение, использование и принципы построения. Классификация ЭЦП. ЭЦП ЭльГамаля. ЭЦП ЭльГамаля и дискретное логарифмирование. ЭЦП Шнорра. Умножение по Монтгомери.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов			Количество часов УСР	Форма контроля знаний
		Лекции	Семинарские Занятия	Лабораторные занятия		
1	**Введение**	**2**				
1.1	Введение	2				Устный опрос
2	**Симметричная криптография**	**18**		**16**	**2**	
2.1.	Алгебраические основы криптографии.	4		4		Защита лабораторной работы
2.2	Элементы теории Шеннона	4		4		Защита лабораторной работы
2.3	Блочные криптосистемы	4		4		Защита лабораторной работы. Контрольная работа № 1
2.4	Криптоанализ	2			2	Устный опрос
2.5	Поточные криптосистемы	4		4		Защита лабораторной работы. Проведение коллоквиума
3	**Асимметричная криптография**	**14**		**14**	**2**	
3.1	Протокол Диффи-Хэллмана	2		2		Защита лабораторной работы
3.2	Криптосистема RSA	4		4		Защита лабораторной работы
3.3	Функции хэширования	4		4	2	Защита лабораторной работы. Устный опрос

3.4	Электронная цифровая подпись	4		4		Защита лабораторной работы. Контрольная работа № 2
ИТОГО		**34**		**30**	**4**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Харин Ю.С., Агиевич С.В., Васильев Д.В., Матвеев Г.В. Криптология. — Минск: БГУ, 2013.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. — Москва: Гелиос АРВ, 2001.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. – М.: Вильямс, 2016.

Перечень дополнительной литературы

1. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. — CRC Press, 1996.
2. Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим ме-тодам защиты информации. — Минск, БГУ, 2001.

Рекомендуемая тематика контрольных работ

1) Контрольная работа №1. *Модель Шеннона и блочно-итерационные криптосистемы*.

2) Контрольная работа №2. *Криптосистема RSA, функция хэширования и электронная цифровая подпись*.

Методические рекомендации по организации самостоятельной работы обучающихся

Для организации самостоятельной работы студентов магистратуры по учебной дисциплине следует использовать современные информационные технологии: разместить в сетевом доступе комплекс учебных и учебно-методических материалов (учебно-программные материалы, ссылки на учебные издания для теоретического изучения дисциплины, методические указания к лабораторным занятиям, материалы текущего контроля и текущей аттестации, позволяющие определить соответствие учебной деятельности обучающихся требованиям образовательных стандартов высшего образования и учебно-программной документации, в т.ч. вопросы для подготовки к зачету, задания, тесты, вопросы для самоконтроля, тематика рефератов и др., список рекомендуемой литературы, информационных ресурсов и др.). Эффективность самостоятельной работы студентов магистратуры проверяется в ходе текущего и итогового контроля знаний. Для общей оценки качества усвоения студентами магистратуры учебного материала рекомендуется использование рейтинговой системы.

Перечень рекомендуемых средств диагностики

Для текущего контроля качества усвоения знаний студентами магистратуры используется следующий диагностический инструментарий:

1. Устная форма: устные опросы, защиты отчетов по домашним заданиям защиты отчетов лабораторных работ; проведение коллоквиума.
2. Письменная форма: письменные контрольные работы по отдельным темам учебной дисциплины.

Методика формирования итоговой оценки

Формами текущей аттестации по учебной дисциплине «Криптографические методы» учебным планом предусмотрены зачет и экзамен.

Рекомендуется использовать рейтинговую оценку знаний студента магистратуры, дающую 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 в рейтинговую оценку:

- работа на лабораторных занятиях – 45 %;
- контрольные работы – 30 %;
- коллоквиум – 25 %.

Итоговая оценка формируется на основе:

1) Правил проведения аттестации студентов (Постановление Министерства образования Республики Беларусь № 53 от 29 мая 2012г.);
2) Положение о рейтинговой системе оценки знаний по дисциплине в БГУ (Приказ ректора БГУ от 18.08.2015 № 382-ОД);
3) Критериев оценки знаний студентов (письмо Министерства образования от 22.12.2003).

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Компьютерная безопасность распределенных систем	Информационных систем управления	нет	Оставить содержание учебной дисциплины без изменения, протокол № 6 от 06.11.2018 г.

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 _____ (протокол № ____ от _____ 201_ г.)

Заведующий кафедрой

_____ _____ _____

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____