Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе
_____ С.Н. Ходин
(подпись) (И.О.Фамилия)
«05» _____ 2017 г.
(дата утверждения)
Регистрационный № УД-4869/уч.

Криптографические методы защиты информации

Учебная программа учреждения высшего образования
по учебной дисциплине для специальностей:
1-31 03 07 Прикладная информатика (по направлениям)
направления специальности
1-31 03 07-03 Прикладная информатика (веб-программирование и компьютерный дизайн)

2017 г.

Учебная программа составлена на основе образовательного стандарта высшего образования первой ступени специальности 1-31 03 07-2013 «Прикладная информатика» (по направлениям) 1-31 03 07 и учебного плана БГУ по специальности 1-31 03 07-03 «Прикладная информатика» (Веб-программирование и компьютерный дизайн) G31-188/уч. 2013 г.

СОСТАВИТЕЛЬ:
Дубровина О.В., старший преподаватель кафедры информационных технологий факультета социоультурных коммуникаций

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой информационных технологий
(протокол № 7 от 26.04.2017)

Научно-методическим советом Белорусского государственного университета
(протокол № 5 от 27.05.2017)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа «Криптографические методы защиты информации» разработана для специальности 1-31 03 07-03 «Прикладная информатика» направления «Веб-программирование и компьютерный дизайн» высших учебных заведений. Целью изучения дисциплины является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Содержание курса направлено на ознакомление студентов с математическими основами теории шифрования, историей развития криптографии, включая современные тенденции, основными алгоритмами шифрования, хэширования и электронной цифровой подписи, криптографическими протоколами обмена информацией, методами криптоанализа, стеганографическимим методами скрытия передаваемой информации, современными развивающимися тенденциями в криптографии.

В результате освоения курса «Криптографические методы защиты информации» студент должен:

знать:

– основные задачи и понятия криптографии;

– требования к шифрам и основные характеристики шифров;

– методы построения и блочных и поточных криптосистем, функций хэширования, криптосистем с открыты ключом, систем электронной цифровой подписи, стеганографических систем;

– принципы использования современного программного обеспечения для криптографической защиты информации;

уметь:

– применять полученные знания для создания защищенных систем и документации;

– использовать шифросистемы и стегосистемы для безопасной передачи бинарной и текстовой информации;

– проводить простейший анализ стойкости алгоритмов;

– применять хэш-функции и электронную цифровую подпись при обмене коммерческой информацией;

– уметь пользоваться стандартами и прикладным программным обеспечением в области криптографии;

приобрести навыки:

– криптографической защиты собственной и корпоративной информации.

В ходе изучения дисциплины «Криптографические методы защиты информации» студент должен овладеть компетенциями:

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

АК-2. Владеть системным и сравнительным анализом.

АК-3. Обладать исследовательскими навыками в сфере анализа криптографической защиты информации.
АК-4. Уметь работать самостоятельно.
АК-5. Быть способным порождать новые идеи (обладать креативностью).
АК-6. Обладать междисциплинарным подходом для решения проблем.
АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.
ПК-1. Проектировать,разрабатывать и тестировать программное обеспечение различных видов
ПК-2. Разрабатывать техническую документацию на программное обеспечение.
ПК-7. Заниматься научно-исследовательской деятельностью в сфере современной защиты информации.
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 программного обеспечения, в том числе разработанного сторонними организациями.
ПК-21. Анализировать результаты работы установленного программного обеспечения и вырабатывать предложения по улучшению его работы.
ПК-23. Проводить обучение специалистов, занимающихся эксплуатацией программного обеспечения.
ПК-26. Обеспечивать обучение персонала правилам безопасности и осуществлять современную проверку знаний.
ПК-29. Взаимодействовать со специалистами смежных профилей.

Дисциплина относится к циклу специальных дисциплин (компонент учреждения высшего образования) и связан с дисциплинами «Алгебра и теория чисел», «Программирование», «Технологии программирования».

Изучение курса «Криптографические методы защиты информации» рассчитано на 160 часов, в том числе 68 часов аудиторных занятий (34 часа лекций, 30 часов лабораторных работ и 4 часа управляемой самостоятельной работы). Форма текущей аттестации – экзамен (5 семестр).

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. *Введение в криптографию*

Проблемы информационной безопасности. Угрозы и атаки. Введение в криптографию. История развития криптографии. Задачи криптографии и криптоанализа. Классификация криптосистемы. Методы теории информации в криптографии.

Тема 2. *Классические криптосистемы*

Шифры сдвига. Аффинные шифры. Шифры замены. Шифры перестановки. Шифросистема Виженера. Шифры гаммирования. Композиции шифров. Математические модели. Примеры.

Тема 3. *Симметричные блочные криптосистемы*

Общие принципы построения симметричных блочных систем. Сеть Фейстеля. Криптосистемы DES, ГОСТ 28147-89, IDEA, Blowfish. Режимы использования блочных криптосистем.

Блочно-итерационные криптосистемы. SP-криптосистемы. Криптосистема AES.

Криптосистема Belt.

Атаки на блочные криптосистемы. Имитозащита. Подходы к криптоанализу.

Тема 4. *Симметричные поточные криптосистемы*

Псевдослучайные последовательности. Линейные, мультипликативные, и нелинейные конгруэнтные генераторы. Генераторы на основе регистров сдвига с обратной связью. Фильтрующие генераторы. Комбинирование LSFR-генераторов.

Основные понятия и классификация поточных криптосистем. Рекуррентные последовательности и регистры сдвига. Алгоритмы Берлекэмпа-Месси. Комбинирование последовательностей. Статистическое оценивание. Криптоанализ. Шифры A5, RC4.

Методы криптоанализа поточных шифров.

Тема 5. *Асимметричные криптосистемы*

Общие принципы построения. Криптосистема RSA. Возможные атаки, стойкость. Криптосистемы рюкзака, Рабина, Эль-Гамаля, Мак-Элиса.

Тема 6. *Контроль целостности*

Односторонние функции, хэш-функции. Определения, задачи. Блочно-итерационные хэш-функции, шаговые хэш-функции. Примеры. Атака «дней рождения».

Тема 7. *Электронная цифровая подпись.*

Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП. Алгоритмы ЭЦП: RSA, Эль-Гамаля, Фиата-Шамира, Шнорра. Неотрицаемая подпись Шаума-ван-Антверпена. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94, СТБ 1176.2-99. Подходы к криптоанализу ЭЦП.

Тема 8. *Эллиптические кривые в криптографии*

Основные понятия. Сложение точек. Кривые над конечными полями. Кратная точка. Алгоритм шифрования и электронной цифровой подписи Шнорра.

Тема 9. *Протоколы формирования общего ключа.*

Алгоритм Диффи-Хеллмана. Атака «противник посередине». Протоколы разделения ключа. Сертификаты открытых ключей. Аутентификация. Протоколы MQV, TLS. Схема разделения секрета Шамира.

Тема 10. *Новые направления в криптографии*

Стеганографические методы защиты информации. Скрытие информации в неподвижных изображениях, текстовых файлах, файлах мультимедиа.

Квантовая криптография. Активный криптоанализ. Криптовалюта.

Прикладное программное обеспечение для криптографической защиты информации.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

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	Введение в криптографию	**2**						
2	Классические криптосистемы	**2**			**2**		**2**	
2.1	Классификация. Принципы построения, методы анализа	1					2	Письменный отчет
2.2	Примеры простейших шифров	1			2			Письменный отчет
3	Симметричные криптосистемы. Алгоритмы блочного шифрования	**6**			**6**			
3.1.	Принципы построения симметричных блочных криптосистем. Сеть Фейстеля	2			2			Письменный отчет
3.2	Примеры симметричных блочных криптосистем	4			4			Письменный отчет
4	Симметричные криптосистемы. Алгоритмы поточного шифрования	**4**			**6**			
4.1	Принципы построения симметричных поточных криптосистем	1						
4.2	Методы генерации и анализа случайных последовательностей	1			2			Письменный отчет
4.3	Рекуррентные последовательности и регистры сдвига	1			2			Письменный отчет
4.4	Примеры поточных шифров	1			2			Письменный отчет
5	Асимметричные криптосистемы	**4**			**4**			

1	2	3	4	5	6	7	8	9
5.1	Принципы построения асимметричных криптосистем. Методы анализа.	2						Устный опрос
5.2	Примеры асимметричных криптосистем	2			4			Письменный отчет
6	Хэш-функции	**4**			**2**			Отчет с устной защитой
7	Электронная цифровая подпись	**4**			**2**			Отчет с устной защитой
8	Алгоритмы шифрования данных на основе эллиптических кривых.	**2**			**4**			Письменный отчет
9	Криптографические протоколы формирования общего ключа	**2**			**2**			Письменный отчет
10	Новые направления криптографии	**4**			**2**		**2**	
10.1	Стеганографические методы защиты информации	2			2			Отчет с устной защитой
10.2	Квантовая криптография. Криптовалюта.	2					2	Коллоквиум

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

ОСНОВНАЯ

1. Основы криптографии. / А.П. Алферов [и др.] – 2-е изд. – М.: Гелиос АРВ, 2002. – 480 с.
2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер. – М.: Триумф, 2003. – 816 с.
3. Криптология. / Харин Ю.С. [и др.]. Минск: БГУ, 2013. – 511 с.
4. Конахович, Г.Ф. Цифровая стеганография. Теория и практика. / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев: МК-Пресс, 2006. – 288 с.
5. Алгоритмические основы эллиптической криптографии. / А.А. Болотов [и др.] – М.: Изд-во РГСУ, 2004. – 499 с.

ДОПОЛНИТЕЛЬНАЯ

1. Молдовян, А.А. Криптография. / А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов. – СПб.: Лань, 2000. – 218 с.
2. Токарева, Н.Н. Симметричная криптография. Краткий курс: учеб. пособие. / Н.Н. Токарева. – Новосибирск, 2012. – 234 с.
3. Харин, Ю.С. Компьютерный практикум по математическим методам защиты информации. / Ю.С. Харин, С.В. Агиевич. – Минск: БГУ, 2001. – 194 с.
4. Ященко, В.В. Введение в криптографию. / В.В. Ященко. – М.: МЦНМО, 2012. – 348 с.
5. Жельников, В. Криптография от папируса до компьютера. / В. Жельников. – М.: ABF, 1996. – 336 с.
6. Брассар, Ж. Современная криптология. / Ж. Брассар. – М.: Полимед, 1999. – 178 с.
7. Баричев, С. Основы современной криптографии. / С. Баричев, В. Гончаров, Р. Серов. – М.: Горячая линия-Телеком, 2011. – 175 с.
8. Иванов, М.А. Криптография. Криптографические методы защиты информации в компьютерных системах и сетях. / М.А. Иванов. – М: Кудиц-образ, 2001. – 363 с.

ПЕРЕЧЕНЬ ЗАДАНИЙ УСР СТУДЕНТОВ

Тема 2. *Классические криптосистемы*

Задание: На основе комбинации простейших алгоритмов разработать собственную криптосистему.

Тема 10. *Новые направления в криптографии*

Задание: Изучить и описать прикладное программное средство для обеспечения криптографической защиты (по выбору студента).

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

Для оценки достижений студента используется следующий диагностический инструментарий:

– предоставление письменного отчета по выполненным на лабораторных занятиях индивидуальных заданий с последующей его защитой;

– проведение текущих контрольных вопросов по отдельным темам;

– выступление студента на коллоквиуме по подготовленному реферату;

– сдача экзамена.

МЕТОДИКА ФОРМИРОВАНИЯ ИТОГОВОЙ ОЦЕНКИ ПО ДИСЦИПЛИНЕ

Оценка уровня знаний студента при защите курсовой работы производится по десятибалльной шкале в соответствии с критериями, утвержденными Министерством образования Республики Беларусь.

Методика формирования итоговой оценки формируется на основе: Правил проведения аттестации студентов, курсантов, слушателей при освоении содержания образовательных программ высшего образования, утвержденных Постановлением Министерства образования Республики Беларусь от 29.05.2012 № 53; Положения о рейтинговой системе оценки знаний студентов по дисциплине в Белорусском государственном университете № 382-ОД от 18.08.2015 г.

К оцениваемым видам студентов относятся: анализ изученных студентами теоретических материалов и разработанных студентами примеров шифросистем и их элементов. Контроль самостоятельной работы студентов осуществляется во время аудиторных занятий.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

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)[1]
1. Алгебра и теория чисел	Кафедра информационных технологий	Нет	Изменения не требуются протокол № 7 от 27.04.2017 г.
2. Программирование	Кафедра информационных технологий	Нет	Изменения не требуются протокол № 7 от 27.04.2017 г.
3. Технологии программирования	Кафедра информационных технологий	Нет	Изменения не требуются протокол № 7 от 27.04.2017 г.

[1] При наличии предложений об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
на 20__ / 20__ учебный год

№№ пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры информационных технологий (протокол № __ от «__» _____ 20__ г.)

Заведующий кафедрой
Кандидат физ.-мат. наук, доцент _____ В.А. Нифагин

УТВЕРЖДАЮ
Декан факультета
Кандидат ист. наук, доцент _____ И.И. Янушевич