Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ В.А.Прытков
29.05.2019 г.
Регистрационный № УД-6-1154/уч.

«ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В ОТКРЫТЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ»

Учебная программа учреждения высшего образования по учебной дисциплине
для специальности:
1-98 80 01 «Информационная безопасность»

2019 г.

Учебная программа учреждения высшего образования составлена на основе образовательного стандарта ОСВО 1-98 80 01-2019 и учебных планов специальности 1-98 80 01 «Информационная безопасность».

Составители:
Т.В. Борботько, заведующий кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор технических наук, профессор;
А.М. Тимофеев, доцент кафедры защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент.

Рецензенты:
Кафедра телекоммуникационных систем учреждения образования «Белорусская государственная академия связи» (протокол № 10 от 02.05.2019г.);
В.Ю. Цветков, заведующий кафедрой инфокоммуникационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор технических наук, профессор.

Рассмотрена и рекомендована к утверждению:
Кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 13 от 15.05.2019г.);
Научно-методическим советом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 8 от 24.05.2019г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа рассчитана на 90 учебных часов (3 з.е.).

План учебной дисциплины в дневной форме обучения:

Код специальности	Название специальности	Курс	Семестр	Аудиторных часов (в соответствии с учебным планом уво)				Форма текущей аттестации
				Всего	Лекции	Лабораторные занятия	Практические занятия, семинары	
1-98 80 01	Информационная безопасность	1	1	30	18	12	-	экзамен

План учебной дисциплины в заочной форме обучения:

Код специальности	Название специальности	Курс	Семестр	Аудиторных часов (в соответствии с учебным планом уво)				Контрольная работа	Форма текущей аттестации
				Всего	Лекции	Лабораторные занятия	Практические занятия, семинары		
1-98 80 01	Информационная безопасность	1	1	8	4	4	-	1	экзамен

Место учебной дисциплины.

Актуальность изучения учебной дисциплины «Обеспечение конфиденциальности информации в открытых сетях передачи данных» состоит в том, что при построении современных открытых сетей передачи данных необходимо обеспечивать конфиденциальность передаваемой информации. Поэтому при подготовке специалистов в области информационной безопасности представляется весьма важным изучение алгоритмов и стандартов шифрования данных, обеспечивающих конфиденциальность информации при ее передаче в открытых сетях связи. Дисциплина «Обеспечение конфиденциальности информации в открытых сетях пере-

дачи данных» является одной из дисциплин, составляющих основу общей подготовки специалистов по защите информации.

Цель преподавания учебной дисциплины: получение магистрантами базовых знаний в области построения и функционирования систем и сетей связи, обеспечивающих скрытность и конфиденциальность передаваемой информации.

Задачи учебной дисциплины:
- изучение математического аппарата, используемого для обеспечения конфиденциальности информации;
- изучение принципов построения криптосистем;
- получение знаний об особенностях реализации стандартов и алгоритмов шифрования информации.

В результате изучения учебной дисциплины «Обеспечение конфиденциальности информации в открытых сетях передачи данных» формируются следующие компетенции:
- применять средства обеспечения конфиденциальности данных в инфокоммуникационных сетях.

В результате изучения учебной дисциплины магистрант должен:

знать:
- основные подходы к классификации средств защиты информации, обеспечивающих конфиденциальность информации;
- нормативно-правовую базу в области построения и реализации систем связи, обеспечивающих конфиденциальность информации;

уметь:
- определять критерии для оценки эффективности и надежности систем, использующих методы и средства обеспечения конфиденциальности информации;
- применять современные алгоритмы и стандарты шифрования данных, позволяющие обеспечивать конфиденциальность информации;

владеть:
- практическими навыками по построению систем защиты, обеспечивающих конфиденциальность информации.

Перечень учебных дисциплин, усвоение которых необходимо для изучения данной учебной дисциплины.

№ п.п.	Название учебной дисциплины	Раздел, темы
	Базируется на знаниях, полученных при освоении содержания образовательных программ по специальностям первой ступени высшего образования	

1. Содержание учебной дисциплины

№ тем	Наименование разделов, тем	Содержание тем
Раздел 1. Обеспечение конфиденциальности информации на основе алгебраических структур и полей		
1	Группы	Свойства и набор элементов групп. Использование свойств групп для повышения безопасности шифра
2	Кольца	Свойства и набор элементов кольца. Коммутативное кольцо <R = *Zn*, +, ×>
3	Поля	Поля Галуа GF (p^n), используемые в криптографии. Сопоставительный анализ алгебраических структур
Раздел 2. Алгоритмы обеспечения конфиденциальной передачи информации		
4	Алгоритм AES	Вспомогательные процедуры и спецификации алгоритма. Схемы шифрования данных, расшифрования шифртекстов и генерации раундовых ключей
5	Алгоритм IDEA	Спецификации алгоритма. Схемы шифрования данных, расшифрования шифртекстов и генерации раундовых подключей
6	Обзор алгоритмов шифрования данных	Отечественные и зарубежные алгоритмы шифрования данных. Сопоставительный анализ алгоритмов

2. Информационно-методический раздел

2.1 Литература

2.1.1 Основная

2.1.1.1 Рябко Б. Я. Криптографические методы защиты информации / Б. Я. Рябко, А. Н. Фионов. – М. : Горячая линия-Телеком, 2017. – 230 с.

2.1.1.2 Введение в теоретико-числовые методы криптографии / М. М. Глухов [и др.]. – Санкт-Петербург : Лань, 2011. – 400 с.

2.1.1.3 Криптографические методы защиты информации. Кн. 4 / под ред. Е. М. Сухарева. – М. : Радиотехника, 2007. – 312 с.

2.1.1.4 Смарт Н. Криптография / Н. Смарт . – М. : Техносфера, 2005. – 528 с.

2.1.1.5 Вельшенбах М. Криптография на Си и С++ в действии / М. Вельшенбах. – М. : Триумф, 2004. – 464 с.

2.1.2 Дополнительная

2.1.2.1 Словарь основных терминов по криптологии / сост. Ю. С. Харин [и др.]. – Мн. : БГУ, 2014. – 92 с.

2.1.2.2 Мао В. Современная криптография : теория и практика / В. Мао. – М. : Вильямс, 2005. – 768 с.

2.1.2.3 Левин М. Криптография / М. Левин. – М. : Познавательная книга плюс, 2001. – 320 с.

2.1.2.4 Основы криптографии : учебное пособие для студентов вузов / А. П. Алферов [и др.]. – М. : Гелиос АРВ, 2001. – 480 с.

2.2 Перечень компьютерных программ, наглядных и других пособий, методических указаний и материалов, технических средств обучения, оборудования для лабораторных работ

2.2.1 Персональный компьютер с операционной системой Windows (XP или более поздней версии).

2.2.2 Тимофеев, А. М. Криптографическая защита информации: пособие / А. М. Тимофеев. – Мн. : БГУИР, 2018. – 44 с.

2.2.3 Методологические основы информационной безопасности: учеб.-метод. пособие / В. Ф. Голиков [и др.]. – Мн.: БГУИР, 2012. – 72 с.

2.3 Перечень тем лабораторных занятий, их название

Основная цель проведения лабораторных занятий состоит в закреплении теоретического материала курса, приобретении навыков выполнения эксперимента, обработки экспериментальных данных, анализа результатов, грамотного оформления отчетов.

№ темы по п.1	Наименование лабораторной работы	Содержание	Обеспеченность по пункту 2.2
4	Процедура Key Expansion() стандарта AES-128	Изучение схемы процедуры Key Expansion() стандарта AES-128	2.2.1 - 2.2.3
4	Стандарт AES-128 в режиме шифрования	Изучение схемы шифрования данных стандарта AES-128	2.2.1 - 2.2.3
4	Стандарт AES-128 в режиме расшифрования	Изучение схемы расшифрования шифртекстов стандарта AES-128	2.2.1 - 2.2.3

2.4 Перечень рекомендуемых средств диагностики результатов учебной деятельности

Для диагностики результатов учебной деятельности могут использоваться следующие формы:

1. Отчет по лабораторным работам.
2. Текущий опрос.
3. Доклад.
4. Контрольный опрос.
5. Контрольная работа

2.5 Контрольная работа

№ темы по п.1	Наименование контрольной работы	Содержание	Обеспеченность по пункту 2.2
1 - 3	Группы. Кольца. Поля	Абелевы группы $< Zn, +>$ и $< Zn^*, \times>$. Абелевы кольца $<R = Zn, +, \times>$. Поля Галуа GF (p) и GF (2^n)	2.2.1 - 2.2.3

3. 1 Учебно-методическая карта учебной дисциплины в дневной форме обучения

Номер раздела, темы по п.1	Название раздела, темы	Количество аудиторных часов			Самостоятельная работа, часы	Форма контроля знаний
		ЛК	Лаб. зан.	ПЗ		
Раздел 1. Обеспечение конфиденциальности информации на основе алгебраических структур и полей		**8**	**-**	**-**	**24**	
1	Группы	2	-	-	8	доклад
2	Кольца	2	-	-	8	доклад
3	Поля	4	-	-	8	текущий опрос, доклад
Раздел 2. Алгоритмы обеспечения конфиденциальной передачи информации		**10**	**12**	**-**	**36**	
4	Алгоритм AES	6	12	-	10	отчет по лаб. раб.
5	Алгоритм IDEA	2	-	-	10	доклад
6	Обзор алгоритмов шифрования данных	2	-	-	16	контрольный опрос
	Текущая аттестация					**экзамен**
	Итого	**18**	**12**	**-**	**60**	

3. 2 Учебно-методическая карта учебной дисциплины в заочной форме обучения

Номер раздела, темы по п.1	Название раздела, темы	Количество аудиторных часов			Самостоятельная работа, часы	Форма контроля знаний
		ЛК	Лаб. зан.	ПЗ		
Раздел 1. Обеспечение конфиденциальности информации на основе алгебраических структур и полей		**2**	**-**	**-**	**30**	
1	Группы	0,5	-	-	10	контрольная работа
2	Кольца	0,5	-	-	10	контрольная работа
3	Поля	1,0	-	-	10	контрольная работа
Раздел 2. Алгоритмы обеспечения конфиденциальной передачи информации		**2**	**4**	**-**	**52**	
4	Алгоритм AES	1,0	4	-	22	отчет по лаб. раб.
5	Алгоритм IDEA	0,5	-	-	15	доклад
6	Обзор алгоритмов шифрования данных	0,5	-	-	15	контрольный опрос
	Текущая аттестация					**экзамен**
	Итого	**4**	**4**	**-**	**82**	

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Перечень учебных дисциплин	Кафедра, обеспечивающая учебную дисциплину по п.1	Предложения об изменениях в содержании по изучаемой учебной дисциплине	Подпись заведующего кафедрой, обеспечивающей учебную дисциплину по п.1
1	2	3	4
Системы противодействия утечке данных Защита веб-ресурсов от несанкционированного доступа Стандартизация и сертификация средств защиты информации Проектирование систем защиты объектов информатизации	кафедра защиты информации	изменения не требуются	_____ Т. В.Борботько протокол № 13 от 15.05.2019 г.

Заведующий кафедрой
защиты информации _____ Т.В. Борботько