Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе
_____ А.Л. Толстик
_____
Регистрационный № УД-3678 /уч.

ИНФОРМАЦИОННЫЕ АСПЕКТЫ НЕЛИНЕЙНОЙ ДИНАМИКИ

Учебная программа учреждения высшего образования по учебной дисциплине для специальностей:

1-98 01 01 Компьютерная безопасность (по направлениям)
направление 1-98 01 01-02 Компьютерная безопасность (радиофизические методы и программно-технические средства)

2016 г.

Учебная программа учреждения высшего образования «Информационные аспекты нелинейной динамики на основании:

Образовательного стандарта высшего образования ОСВО 1-98 01 01-2013 Высшее образование. Первая ступень. Специальность 1-98 01 01 « Компьютерная безопасность» (по направлениям) направление 1 – 98 01 01-02 Компьютерная безопасность (радиофизические методы и программно-технические средства) и учебного плана Р 98 – 139/уч.2013.

СОСТАВИТЕЛЬ:

А.В.Сидоренко, профессор кафедры физики и аэрокосмических технологий Белорусского государственного университета, доктор технических наук, профессор

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой телекоммуникаций и информационных технологий Белорусского государственного университета (протокол № 5 от 13 декабря 2016 г.);

Учебно-методической комиссией факультета радиофизики и компьютерных технологий (протокол № 4 от 20 декабря 2016 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Целью изучения данной дисциплины является освоение основных методов построения и анализа систем и средств обеспечения защиты информации, основанных на теории нелинейных динамических систем, использующих детерминированный хаос.

Основные задачи дисциплины:

- усвоить методы теории динамического хаоса и закономерностей поведения динамической системы для разработки средств защиты информации на уровне аппаратного и программного обеспечения;
- получить информацию по устойчивости динамических систем и появлению в них бифуркаций с иллюстрацией на моделях Лоренца, Рёсслера и Чуа для практической синхронизации сигналов динамического хаоса в телекоммуникационных системах,
- обучить использованию методов информационного анализа сложных сигналов для разработки средств защиты в телекоммуникационных системах ;
- ознакомить с принципами построения, структурным составом и схемными решениями аппаратуры для технической реализации телекоммуникационных систем при использовании динамического хаоса в области передачи и криптографической защиты информации.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием, связи с другими учебными дисциплинами

Дисциплина входит в цикл спецкурсов и посвящена изучению основ нелинейной динамики и их приложению к проблемам телекоммуникаций и информационных приложений. Она знакомит студентов с элементами динамической теории информации, методами и алгоритмами решения задач нелинейного анализа систем при использовании динамического хаоса для генерации, передачи и шифрования информации. Определяется ряд задач в области информационно-телекоммуникационных технологий, решаемых методами дисциплины. Это способствует формированию у студентов навыков формализации, элементов информационного подхода на основе моделей динамических систем и практической реализации методов нелинейного анализа при решении типовых задач конфиденциальной передачи и шифрования информации.

Лабораторный практикум проводится в компьютерном классе и предполагает решение конкретных задач в области передачи и защиты информации с использованием динамического хаоса. Он предполагает самостоятельное изучение алгебраических манипуляций и программирования в программной среде Mathematica 5.2., исследование вычислительных алгоритмов.

Для успешного усвоения дисциплины «Информационные аспекты нелинейной динамики» необходимо комплексное использование знаний, полученных при изучении базовых дисциплин информатики, теории информации.

Требования к освоению учебной дисциплины в соответствии с образовательным стандартом

В результате изучения учебной дисциплины студент должен:

знать:

- основные элементы теории информации, ее ценности и эволюции для конфиденциальной передачи данных;
- принципы моделирования генерации ценной информации для необходимого временного и пространственного обеспечения ее целостности;
- методологию теории динамического хаоса для разработки средств защиты информации на уровне аппаратного и программного обеспечения;

уметь применять:

- полученные знания в области разработки средств защиты информации в телекоммуникационных системах при использовании динамического хаоса для передачи и криптографической защиты информации.

Состав компетенций специалиста

Требования к академическим компетенциям специалиста

Специалист должен:

– уметь применять базовые научно-теоретические знания для решения теоретических и практических задач;

– владеть системным и сравнительным анализом;

– уметь работать самостоятельно;

– иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

Требования к социально-личностным компетенциям специалиста

Специалист должен:

– быть способным к социальному взаимодействию;

– обладать способностью к межличностным коммуникациям.

Требования к профессиональным компетенциям специалиста

Специалист должен быть способен:

– взаимодействовать со специалистами смежных профилей;

– разрабатывать программные, аппаратно-программные и технические средства и системы защиты информации; разрабатывать необходимую документацию.

Общее количество часов и количество аудиторных часов, отводимое на изучение учебной дисциплины в соответствии с учебным планом

Программа рассчитана на объем: Компьютерная безопасность – 116, аудиторных часов (примерное распределение по видам занятий: лекции – 34 ч., лабораторный практикум – 28 ч.) Число зачетных единиц – 3,5.

Форма текущей аттестации – зачет в 8 семестре.

Форма получения образования – очная.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

1 **ВВЕДЕНИЕ. ПРЕДМЕТ И МЕТОД ДИСЦИПЛИНЫ**.

Информационные аспекты нелинейной динамики как научная дисциплина, изучающая принципы построения сложных динамических систем и особенности использования динамического хаоса для передачи и шифрования информации. Основные этапы реализации методов исследования динамических систем: формализация исходной проблемы, построение математической модели, реконструкция системы по экспериментальным данным. Защита информации.

*. Всего часов: 1. В том числе аудиторных – 1.

2 **ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИИ**

Определение понятия “информация”. Количество и ценность информации. Генерация информации. Иерархия информационных уровней. Условная и безусловная информация. Макро- и микроинформация. Генерация, передача и прием конфиденциальной информации.

*. Всего часов: 1. В том числе аудиторных – 1.

3 **ДИНАМИЧЕСКИЕ СИСТЕМЫ**

Динамическая система и ее математическая модель. Динамические уравнения и фазовые портреты динамических систем.

Устойчивость. Линейный анализ устойчивости. Устойчивость состояний равновесия. Устойчивость открытых систем. Устойчивость периодических и квазипериодических решений.

Бифуркации динамических систем. Бифуркации предельных циклов.

Диссипативные структуры. Аттракторы динамических систем.

Динамический хаос. Модели динамического хаоса. Модель Лоренца. Модель Ресслера. Система Чуа.

*. Всего часов: 11. В том числе аудиторных – 11.

4 **РЕКОНСТРУКЦИЯ ДИНАМИЧЕСКИХ СИСТЕМ**

Реконструкция аттракторов по временным рядам. Экспериментальные данные. Анализ непрерывных сигналов.

Глобальная реконструкция динамической системы. Особенности и недостатки алгоритма реконструкции. Метод реконструкции при защите информации. Модель модифицированного генератора с инерционной нелинейностью.

*. Всего часов: 11. В том числе аудиторных – 11.

5 **ИНФОРМАЦИОННЫЕ СИСТЕМЫ**

Характеристика информационных систем. Временной и пространственный горизонты прогнозирования.

Генерация ценной информации. Модели генерации ценной информации. Эволюция ценности информации. Конъюнктурная ценность информации. Прогностическая ценность информации.

*. Всего часов: 6. В том числе аудиторных – 6.

6 ИНФОРМАЦИОННЫЙ АНАЛИЗ СИГНАЛОВ НА ОСНОВЕ МЕТОДОЛОГИИ НЕЛИНЕЙНОЙ ДИНАМИКИ

Методы информационного анализа сложно структурированных сигналов типа динамического хаоса. Метод задержанной координаты. Метод выделения неустойчивых периодических орбит. Метод анализа с использованием вейвлет-преобразования.

Информационно-измерительная система для обработки и анализа динамической информации. Структурная схема. Особенности программного обеспечения.

*. Всего часов: 2. В том числе аудиторных – 2.

7 ДИНАМИЧЕСКИЙ ХАОС ДЛЯ ПЕРЕДАЧИ СИГНАЛОВ ПРИ ЗАЩИТЕ ИНФОРМАЦИИ

Проблема обеспечения защиты информации.

Методы передачи информации с использованием хаотического синхронного отклика. Хаотическая маскировка. Переключение хаотических режимов. Нелинейное подмешивание информационного сигнала к хаотическому сигналу. Адаптивные методы приема.

Система с нелинейным подмешиванием информационного сигнала к хаотическому сигналу. Математическая модель системы. Передача аналоговой информации. Оценка качества передачи информации.

Повышение эффективности применения схемы с нелинейным подмешиванием информации. Система с суммированием хаотического и информационного сигнала. Схема с предварительной частотной модуляцией хаотического сигнала. Реализация системы с нелинейным подмешиванием информации.

Прямохаотические системы передачи информации. Генераторы хаоса в высокочастотном и сверхвысокочастотном диапазонах. Особенности ввода и извлечения информации.

Сравнительный анализ систем с нелинейным подмешиванием и прямохаотических систем передачи информации.

*. Всего часов: 16. В том числе аудиторных – 16.

8 БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКОЙ ДИНАМИКИ

Беспроводные сенсорные сети и их особенности**.** Беспроводные сенсорные сети на сверхширокополосных сигналах. Сверхширокополосные приемопередатчики. Экспериментальные исследования алгоритма шифрования в сенсорной сети.

*. Всего часов: 2. В том числе аудиторных – 2.

9 ДИНАМИЧЕСКИЙ ХАОС В КРИПТОГРАФИИ

Особенности теории хаоса в криптографии**.** Основные принципы построения алгоритмов криптографии. Блочный и поточный шифры, их характеристики. Криптографические ключи. Фундаментальные соотношения между детерминированным хаосом и криптографией. Хаотические отображения. Логистическое, tent-отображение, пилообразное, Чебышевские отображения. Анализ работы шифров на примере передачи изображений.

*. Всего часов: 10. В том числе аудиторных – 10.

10 **ДЕТЕРМИНИРОВАННЫЙ ХАОС В СТЕГАНОГРАФИИ**.
Детерминированный хаос в стеганографии. Облачные вычисления.
*. Всего часов: 2. В том числе аудиторных – 2.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Формы контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4		5	6	8	9
1.	Тема 1. **Введение. Предмет и метод дисциплины**							
1.1.	Информационные аспекты нелинейной динамики как научная дисциплина, изучающая принципы построения сложных динамических систем и особенности использования динамического хаоса для передачи и шифрования информации.	1						Устный опрос
2.	Тема 2. **Основные понятия теории информации**							
2.1.	Определение понятия “информация”. Количество и ценность информации. Генерация информации. Генерация, передача и прием конфиденциальной информации.	1						Устный опрос
3.	Тема 3. **Динамические системы**							
3.1	Динамическая система и ее математическая модель. Динамические уравнения и фазовые портреты динамических систем.	1						
3.2.	Устойчивость. Линейный анализ устойчивости. Устойчивость периодических и	2			4			Письменный отчет по лаб.

	квазипериодических решений.							работе
3.3.	Бифуркации динамических систем. Бифуркации предельных циклов.	2						
3.4	Динамический хаос. Модели динамического хаоса. Модель Лоренца. Модель Рёсслера. Система Чуа.	2						Устный опрос
4.	Тема 4. **Реконструкция динамических систем**							
4.1.	Реконструкция аттракторов по временным рядам. Экспериментальные данные. Анализ непрерывных сигналов.	1			4			Письменный отчет по лаб. работе
4.2.	Глобальная реконструкция динамической системы. Метод реконструкции при защите информации. Модель модифицированного генератора с инерционной нелинейностью.	2			4			Письменный отчет по лаб. работе
5.	Тема 5. **Информационные системы.**							
5.1.	Характеристика информационных систем. Генерация ценной информации. Модели генерации ценной информации. Асимптотическая, конъюнктурная, прогностическая ценности информации.	2			4			Письменный отчет по лаб. работе
6.	Тема 6. **Информационный анализ сигналов на основе методологии нелинейной динамики**							
6.1.	Методы информационного анализа сложно структурированных сигналов типа динамического хаоса. Метод задержанной координаты. Метод выделения неустойчивых периодических орбит. Метод анализа с использованием вейвлет-преобразования.	2						Устный опрос
7.	Тема 7. **Динамический хаос для передачи сигналов при защите информации**							
7.1.	Проблема обеспечения защиты информации. Методы передачи информации с использованием хаотического синхронного отклика.	2						Устный опрос

7.2.	Система с нелинейным подмешиванием информационного сигнала к хаотическому сигналу. Математическая модель системы.	2			4			Письменный отчет по лаб. работе
7.3.	Повышение эффективности применения схемы с нелинейным подмешиванием информации.	2						
7.4.	Прямохаотические системы передачи информации. Генераторы хаоса в высокочастотном и сверхвысокочастотном диапазонах.	2			4			Письменный отчет по лаб. работе
8.	Тема 8. **Беспроводные сенсорные сети с использованием хаотической динамики.**							
8.1.	Беспроводные сенсорные сети и их особенности. Беспроводные сенсорные сети на сверхширокополосных сигналах. Экспериментальные исследования алгоритма шифрования в сенсорной сети.	2						Устный опрос
9.	Тема 9. **Динамический хаос в криптографии.**							
9.1.	Особенности теории хаоса в криптографии. Основные принципы построения алгоритмов криптографии.	2						Устный опрос
9.2.	Фундаментальные соотношения между детерминированным хаосом и криптографией. Хаотические отображения. Стойкость алгоритмов шифрования.	2			4			Письменный отчет по лаб. работе
9.3.	Анализ работы шифров на примере передачи изображений.	2						Устный опрос
10.	Тема 10. **Детерминированный хаос в стеганографии.**							
11.	Детерминированный хаос в стеганографии. Облачные вычисления.	2						Устный опрос
	Итого по видам занятий	34			28			

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень рекомендуемой литературы

Основная:

1. Сидоренко А. В. Информационные аспекты нелинейной динамики Мн.: БГУ, 2008. – 125 с.
2. Чернавский Д. С. Синергетика и информация. М: УРСС, 2004. – 290 с.
3. Дмитриев А. С., Панас А. И. Динамический хаос. Новые носители информации для систем связи. М.:Физматлит, 2002. – 253 с.
4. Сидоренко А. В. Методы информационного анализа биоэлектрических сигналов. Мн.: БГУ, 2003. – 189 с.
5. Сидоренко А. В. Информационные системы на основе динамического хаоса. Мн.: БГУ, 2016. – 152 с.
6. Сидоренко А. В. Информационные аспекты нелинейной динамики. Практикум. Мн.: БГУ, 2014. – 62 с.

Дополнительная:

7. Анищенко В. С., Астахов В. В. Нелинейные эффекты в хаотических и стохастических системах. М.-Ижевск: Институт компьютерных исследований, 2003. –530 с.
8. Магницкий Н. А., Сидоров С. В. Новые методы хаотической динамики. М.: УРСС, 2004. –320 с.

Примерный перечень лабораторных работ:

Лабораторная работа 1**.** Алгебраические манипуляции и программирование в среде Mathematica 5.2.

Лабораторная работа 2. Линейный и нелинейный анализ устойчивости и бифуркаций для динамических систем.

Лабораторная работа 3. Восстановление аттрактора для модели Лоренца с использованием экспериментальных данных биоэлектрических сигналов.

Лабораторная работа 4. Генератор хаотических сигналов и анализ режимов его работы для прямохаотических систем передачи информации.

Лабораторная работа 5. Применение теории хаоса для выявления DD_0S-атак.

Описание подходов к преподаванию учебной дисциплины

Основными методами и технологиями обучения, отвечающими целям и задачам изучения дисциплины «Информационные аспекты нелинейной динамики», являются:

– элементы проблемного изложения, реализуемые на лекционных занятиях;

– преподавание с использованием мультимедийной техники и прикладных компьютерных программ.

– коммуникативные технологии (учебные дискуссии, споры-диалоги).

Перечень используемых средств диагностики

Для контроля качества обучения используются следующие средства диагностики:

– устный опрос во время занятий;

– письменные отчеты по лабораторным работам;

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)
Информатика	Телекоммуникаций и информационных технологий	нет	Изменений не требуется Протокол №5 от 13.12.2016
Теория информации	Кафедра радиофизики и цифровых медиатехнологий	нет	Изменений не требуется Протокол №5 от 13.12.2016

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УВО НА _____ / _____ УЧЕБНЫЙ ГОД

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 20___ г.)
(название кафедры)

Заведующий кафедрой
_____ _____ _____
(ученая степень, звание) (подпись) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета
_____ _____ _____
(ученая степень, звание) (подпись) (И.О. Фамилия)