БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям

_____ О.Н. Чуприс

20.06.2018

Регистрационный № УД-5447уч.

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ХАОТИЧЕСКОЙ ДИНАМИКОЙ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности

1-98 80 03 Аппаратное и программно-техническое обеспечение информационной безопасности

2018 г.

Учебная программа составлена на основании ОСВО 1-98 80 03-2012, учебного плана № Р98-335/уч. от 24.05.2018, учебного плана № Р98к - 314/уч. от 19.04.2018 г.

СОСТАВИТЕЛЬ:
А. В. Сидоренко, профессор кафедры физики и аэрокосмических технологий Белорусского государственного университета

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой телекоммуникаций и информационных технологий факультета радиофизики и компьютерных технологий Белорусского государственного университета (протокол № 13 от 01.06.2018 г.)

Учебно-методической комиссией факультета радиофизики и компьютерных технологий (протокол № 10 от 19.06.2018 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа учебной дисциплины по выбору «Системы защиты информации с хаотической динамикой» разработана для студентов специальности 1-98 80 03 «Аппаратное и программно-техническое обеспечение информационной безопасности» и относится к циклу дисциплин специальной подготовки.

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

Основными задачами дисциплины являются:

- 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, Чуа для практической синхронизации сигналов динамического хаоса в телекоммуникационных системах при защите информации,
- обучить использованию методов информационного анализа сложных сигналов для разработки средств защиты информации в телекоммуникационных системах,
- ознакомить с принципами построения, структурным составом и схемными решениями аппаратуры с обеспечением защиты информации для технической реализации телекоммуникационных систем при использовании динамического хаоса в области безопасной передачи и криптографической защиты информации.

Для успешного усвоения дисциплины необходимы знания в объеме учебных дисциплин «Теория информации», «Компьютерные сети» первой ступени высшего образования. Знания, полученные при изучении учебной дисциплины «Системы защиты информации с хаотической динамикой» необходимы для успешного изучения учебной дисциплины «Программно-технические средства компьютерной безопасности».

Требования к освоению учебной дисциплины в соответствии с образовательным стандартом

В результате изучения дисциплины обучаемый 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 и сохранности,

– 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 безопасной передачи и криптографической защиты информации, в том числе, в беспроводных сетях и системах радиочастотной идентификации.

владеть:

– технологиями моделирования, проектирования и конфигурирования систем защиты информации на основе динамического хаоса.

Состав компетенций специалиста

Требования к академическим компетенциям специалиста:

- способность к самостоятельной научно-исследовательской деятельности (анализ, сопоставление, систематизация, абстрагирование, моделирование, проверка достоверности данных, принятие решений и др.), готовность генерировать и использовать новые идеи.

Требования к социально-личностным компетенциям специалиста:

- совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования своей личности;
- формировать и аргументировать собственные суждения и профессиональную позицию;
- анализировать и принимать решения по социальным, этическим, научным и техническим проблемам, возникающим в профессиональной деятельности;
- логично, аргументированно и ясно строить устную и письменную речь, использовать навыки публичной речи, ведения дискуссии и полемики.

Требования к профессиональным компетенциям специалиста:

- работать с научно-технической информацией с использованием современных информационных технологий;
- разрабатывать и совершенствовать методы исследования проблем информационной безопасности;
- осуществлять постановку и проведение теоретических и экспериментальных исследований в области информационной безопасности;
- обосновывать достоверность полученных научных результатов;
- формулировать выводы и рекомендации по применению результатов научно-исследовательской работы;
- оформлять научные статьи и доклады;
- составлять отчеты и презентации и научно-исследовательской работе, участвовать в работе научных конференций;
- осуществлять поиск, систематизацию и анализ информации по перспективным направлениям информационной безопасности,

инновационным технологиям, проектам и решениям;

- разрабатывать новые методы и технологии защиты информации;
- определять цели инноваций и способы их достижения.

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

Программа рассчитана на объем 122 учебных часа, из которых – 48 часов являются аудиторными. Распределение аудиторных часов по видам занятий следующее: лекций – 18 часов, лабораторных работ – 30 часов.

Форма текущей аттестации – зачет в 3 семестре.

Форма получения образования – очная.

Число зачетных единиц – 3,5.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

1. **Введение.** Системы защиты информации с хаотической динамикой как 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. Основные понятия теории информации. Количество и ценность информации. Генерация информации. Генерация, передача и прием конфиденциальной информации. Защита информации.
2. **Динамические системы.** Динамическая система и ее модель. Динамические уравнения и фазовые портреты динамических систем. Устойчивость. Линейный анализ устойчивости. Устойчивость состояний равновесия. Устойчивость периодических и квазипериодических решений. Бифуркации динамических систем. Бифуркации предельных циклов. Аттракторы динамических систем. Динамический хаос. Модели динамического хаоса. Модель Лоренца. Модель Ресслера. Система Чуа.
3. **Реконструкция динамических систем.** Реконструкция аттракторов по временным рядам. Экспериментальные данные. Метод реконструкции при защите информации. Модель модифицированного генератора с инерционной нелинейностью.
4. **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.
5. **Информационный анализ сигналов на основе методов 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.
6. **Динамический хаос для передачи сигналов при защите информации.** Проблема обеспечения защиты информации. Методы передачи информации с использованием синхронного хаотического отклика. Хаотическая маскировка. Переключение хаотических режимов. Нелинейное подмешивание информационного сигнала к хаотическому. Адаптивные методы приема. Система с нелинейным подмешиванием информационного сигнала к хаотическому. Математическая модель системы. Передача аналоговой информации. Система с суммированием хаотического и информационного сигналов. Повышение эффективности системы. Реализация системы с нелинейным подмешиванием информации. Генераторы хаоса в высокочастотном и сверхвысокочастотном диапазонах. Сравнительный анализ систем с

нелинейным подмешиванием и прямохаотических систем передачи информации.

7. **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.
8. **Динамический хаос в криптографии.** Особенности теории хаоса в криптографии. Основные принципы построения алгоритмов в криптографии. Фундаментальные соотношения между динамическим хаосом и криптографией. Хаотические отображения. Логистическое, tent-отображение, пилообразное, Чебышевское отображения. Анализ работы шифров на примере передачи изображений.
9. **Защита информации в RFID-системах.** Структура систем радиочастотной идентификации. Обеспечение защиты информации при радиочастотной идентификации. Основные для RFID-систем атаки: перехват, отказ в обслуживании, клонирование метки, раскрытия ключа, обезличивание метки, обезличивание считывателя. RFID- системы в мобильной коммерции. Протокол аутентификации ULRAS и его модификация. Хаотические отображения в RFID-системах. Расчет количественных параметров вероятности успешности атак.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов			Количество часов УСР	Материальное обеспечение занятия (наглядные, методические пособия и др.)	Литература	Форма контроля знаний
		Лекции	Практические занятия	Лабораторные занятия				
1	2	3	4	5	6	7	8	9
1.	**ВВЕДЕНИЕ. СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ХАОТИЧЕСКОЙ ДИНАМИКОЙ. ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИИ.**	**2**	-	-	-	Презентация 1	[1],[2] ,[3], [6]	Аудиторный тест по главе
1.2	Алгебраические манипуляции и программирование в среде Mathematica 5.2		-	**8**	-	Компьютерный класс, учебная лаборатория		Отчет по лабораторной работе
2.	**ДИНАМИЧЕСКИЕ СИСТЕМЫ**	**3**	-	-	-	Презентация 2а, 2б	[3],[5], [6], [7]	Аудиторный тест по главе
2.1	Линейный и нелинейный анализ устойчивости и бифуркаций для динамических систем		-	**6**	-	Компьютерный класс, учебная лаборатория		Отчет по лабораторной работе
3.	**РЕКОНСТРУКЦИЯ ДИНАМИЧЕСКИХ СИСТЕМ**	**1**	-	-	-	Презентация 3	[1], [3], [4]	Аудиторный тест по главе Реферат
3.1.	Восстановление аттрактора дл модели Лоренца с использованием экспериментальных данных биоэлектрических сигналов		-	**6**	-	Компьютерный класс, учебная лаборатория		Отчет по лабораторной работе
4.	**ИНФОРМАЦИОННЫЕ СИСТЕМЫ**	**1**	-	-	-	Презентация 4	[2], [3], [5]	Аудиторный тест по главе
5.	**ИНФОРМАЦИОННЫЙ АНАЛИЗ СИГНАЛОВ НА ОСНОВЕ МЕТОДОВ НЕЛИНЕЙНОЙ ДИНАМИКИ**	**1**	-	-	-	Презентация 5	[1], [2], [8]	Аудиторный тест по главе Контрольный опрос
6.	**ДИНАМИЧЕСКИЙ ХАОС ДЛЯ ПЕРЕДАЧИ СИГНАЛОВ ПРИ ЗАЩИТЕ ИНФОРМАЦИИ**	**4**	-	-	-	Презентация 6а, 6б	[3], [5], [6]	Аудиторный тест по главе Контрольный опрос
6.1	Генератор хаотических сигналов и анализ режимов его работы для прямохаотических систем передачи информации		-	**6**	-	Компьютерный класс, учебная лаборатория		Отчет по лабораторной работе

7.	**БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКОЙ ДИНАМИКИ**	**2**	-	-	-	Презентация 7	[5]	Аудиторный тест по главе
8.	**ДИНАМИЧЕСКИЙ ХАОС В КРИПТОГРАФИИ**	**3**	-	-	-	Презентация 8а, 8б	[1], [3], [5], [6]	Аудиторный тест по главе
8.1.	Применение динамического хаоса выявления DD_0S -атак		-	**4**	-	Компьютерный класс, учебная лаборатория		Отчет по лабораторной работе
9	**ЗАЩИТА ИНФОРМАЦИИ В RFID- СИСТЕМАХ**	**1**	-	-	-	Презентация 8	[5]	Аудиторный тест по главе Контрольный опрос
	ИТОГО	**18**		**30**				

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература:

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 литература:

1. *Анищенко В. С., Астахов В. В.* Нелинейные эффекты в хаотических и стохастических системах. М.-Ижевск: Институт компьютерных исследований, 2003. – 530 с.

2. *Магницкий Н. А., Сидоров С. В.* Изучение Новые методы хаотической динамики. М.: УРСС, 2004. – 320 с.

Примерный перечень лабораторных работ

1. Алгебраические манипуляции и программирование в среде Mathematica 5.2. – 8 часов.
2. Линейный и нелинейный анализ устойчивости и бифуркаций для динамических систем. – 6 часов.
3. Восстановление аттрактора для модели Лоренца с использованием экспериментальных данных биоэлектрических сигналов – 6 часов.
4. Генератор хаотических сигналов и анализ режимов его работы для прямохаотических систем передачи информации – 6 часов.
5. Применение теории хаоса для выявления DD_0S - атак – 4 часов.

Выполнение лабораторных работ

В лабораторном практикуме по дисциплине «Системы защиты информации с хаотической динамикой» запланировано изучение моделирования и принципов функционирования систем защиты информации на основе хаотической динамики с использованием современных элементов. Лабораторные работы выполняются на базе изданного практикума.

Отчеты по лабораторным работам студентов будут проводиться в форме индивидуального собеседования и тестирования.

Перечень используемых средств диагностики результатов учебной деятельности

Контроль качества образования осуществляется в форме текущей и итоговой аттестации магистрантов.

Основным средством диагностики усвоения знаний и овладения необходимыми умениями и навыками по дисциплине «Системы защиты информации с хаотической динамикой» являются:

- аудиторный тест по главе,
- отчет по лабораторной работе,
- контрольный опрос.

Методика формирования итоговой оценки

Итоговая оценка формируется на основе:

1. Правил проведения аттестации студентов (Постановление Министерства образования Республики Беларусь № 53 от 29 мая 2012 г.);
2. Положения 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 г.)

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)
«Теория информации»	телекоммуникаций и информационных технологий	нет	изменений не требуется протокол № 13 от 01.06.2018 г.
«Компьютерные сети»	телекоммуникаций и информационных технологий	нет	изменений не требуется протокол № 13 от 01.06.2018 г.
«Программно-технические средства компьютерной безопасности»	телекоммуникаций и информационных технологий	нет	изменений не требуется протокол № 13 от 01.06.2018 г.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УВО
на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
Телекоммуникаций и информационных технологий
(протокол № ____ от _____ 201__ г.)

Заведующий кафедрой

_____ _____ Ю. И. Воротницкий

УТВЕРЖДАЮ
Декан факультета

_____ _____ С. В. Малый