

Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе


А.Л. Толстик
06.01.2016



Регистрационный № УД- 1855 / уч.

**ТЕСТИРОВАНИЕ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУ-
ЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ**

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

1-98 01 01 Компьютерная безопасность (по направлениям)

2016 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-98 01 01-2013 и учебного плана Р 98-138/уч., 30.05.2013.

Составитель:

Е. В. Вечерко, ассистент кафедры математического моделирования и анализа данных Белорусского государственного университета.

Рекомендована к утверждению:

Кафедрой математического моделирования и анализа данных Белорусского государственного университета (протокол № 8 от 01 декабря 2015 г.);

Учебно-методической комиссией факультета прикладной математики и информатики Белорусского государственного университета (протокол № 3 от 17 декабря 2015 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи дисциплины «Тестирование генераторов случайных и псевдослучайных последовательностей» – получить знания по применению статистических методов для решения следующих важных задач криптографии:

- тестирование физических датчиков случайных чисел;
- предварительный анализ стойкости криптографических алгоритмов.

Принципы изложения материала: ознакомление с методиками тестирования физических датчиков случайных чисел и предварительного анализа стойкости криптографических алгоритмов, опубликованных в стандартах международного уровня; самостоятельное выполнение отдельных пунктов методик.

Учебная дисциплина «Тестирование генераторов случайных и псевдослучайных последовательностей» относится к циклу дисциплин вузовского компонента и взаимосвязана с учебными дисциплинами «Криптографические методы», «Теория вероятностей и математическая статистика» и «Статистический анализ данных». Методы, излагаемые в дисциплине «Тестирование генераторов случайных и псевдослучайных последовательностей», могут быть использованы при изучении ряда других дисциплин по специальности «Компьютерная безопасность».

В результате изучения дисциплины студент должен:

– **знать:**

принципы применения статистических методов для решения задач криптологии;

порядок тестирования физических датчиков случайных чисел;

способы предварительного анализа стойкости криптографических алгоритмов;

– **уметь:**

применять статистические методы для тестирования физических датчиков случайных чисел;

применять статистические методы для предварительного анализа стойкости криптографических алгоритмов;

– **владеть:**

основными методами статистического тестирования физических датчиков случайных чисел;

основными методами статистического анализа стойкости криптографических алгоритмов.

В соответствии с образовательным стандартом специальности 1-98 01 01 «Компьютерная безопасность» учебная программа предусматривает для изучения дисциплины всего 68 часа, из них 34 аудиторных часов, в том числе лабораторных занятий – 26 часов, УСП – 8 часов (3 курс, 6 семестр).

Форма текущей аттестации по учебной дисциплине – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Введение. Предмет и цель курса. Необходимость использования физических датчиков случайных чисел и особенности их применения. Способы предварительного анализа стойкости криптографических алгоритмов.

Раздел I. Тестирование физических датчиков случайных чисел

Тема 1.1. Принципы тестирования физических датчиков случайных чисел. Построение и выбор статистических критериев для тестирования. Мощность критерия.

Тема 1.2. Архитектура физических датчиков случайных чисел Intel и VIA. Изучение архитектуры физических датчиков случайных чисел Intel и VIA. Выделение типовых поломок и сбояв.

Тема 1.3. Стандарты тестирования последовательностей FIPS 140-2, NIST SP 800-22. Изучение методов тестирования FIPS 140-2, NIST SP 800-22. Составление плана тестирования.

Тема 1.4. Стандарт тестирования последовательностей AIS 31. Изучение методов тестирования AIS 31. Составление плана тестирования.

Тема 1.5. Программная реализация статистических критериев 3-9 из NIST SP 800-22. Проведение статистического тестирования модельных выборок и выходных последовательностей физических генераторов на основе критериев №3-9 из NIST SP 800-22.

Тема 1.6. Программная реализация статистических критериев 10-15 из NIST SP 800-22. Проведение статистического тестирования модельных выборок и выходных последовательностей физических генераторов на основе критериев №10-15 из NIST SP 800-22.

Программная реализация статистических критериев DIEHARD. Проведение статистического тестирования модельных выборок и выходных последовательностей физических генераторов на основе критериев DIEHARD.

Тема 1.6. Подготовка заключения о выходных последовательностях. Подготовка заключения о вероятностных свойствах.

Раздел II. Предварительный анализ стойкости блочного шифра

Тема 2.1. Принципы тестирования генераторов псевдослучайных последовательностей. Принципы тестирования генераторов псевдослучайных последовательностей.

Тема 2.2. Сценарии тестирования блочного шифра. Сценарии тестирования блочного шифра.

Тема 2.3. Построение выборок для тестирования согласно сценариям. Построение выборок на основе выходных последовательностей блочного шифра согласно сценариям тестирования.

Тема 2.4. Тестирование построенных выборок на основе критериев №3-9. Проведение статистического тестирования построенных выборок на основе критериев №3-9.

Тема 2.5. Тестирование построенных выборок на основе критериев №10-15. Проведение статистического тестирования построенных выборок на основе критериев №10-15.

Тема 2.6. Подготовка заключения о блочном шифре. Подготовка заключения о вероятностных свойствах.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

№п/п	Название раздела, темы	Количество часов				Количество часов УСР	Форма контроля знаний
		Аудиторные					
		Лекции	Практ. и сем. занятия	Лаб. занятия	Иное		
	Введение			2			
	Предмет, цель и задачи дисциплины			2			
1	Тестирование физических датчиков случайных чисел			14		4	
1.1	Принципы тестирования физических датчиков случайных чисел			2			Опрос. Проверка выполнения лабораторных работ
1.2	Архитектура физических датчиков случайных чисел Intel и VIA			2			Опрос. Проверка выполнения лабораторных работ
1.3	Стандарты тестирования последовательностей FIPS 140-2, NIST SP 800-22			2			Опрос. Проверка выполнения лабораторных работ
1.4	Стандарт тестирования последовательностей AIS 31			2			Опрос. Проверка выполнения лабораторных работ
1.5	Программная реализация статистических критериев №3-9 из NIST SP 800-22			2			Опрос. Проверка выполнения лабораторных работ
1.6	Программная реализация статистических критериев №10-15 из NIST SP 800-22			2			Опрос. Проверка выполнения лабораторных работ
1.7	Программная реализация статистических критериев DIEHARD			2			Опрос. Проверка выполнения лабораторных работ
1.8	Подготовка заключения о выходных последовательностях					4	Зачет задания
2	Предварительный анализ стойкости блочного шифра			10		4	
2.1	Принципы тестирования генераторов псевдослучайных последо-			2			Опрос. Проверка выполнения

	вательностей						лабораторных работ
2.2	Сценарии тестирования блочного шифра			2			Опрос. Проверка выполнения лабораторных работ
2.3	Построение выборок для тестирования согласно сценариям			2			Опрос. Проверка выполнения лабораторных работ
2.4	Тестирование построенных выборок на основе критериев №3-9			2			Опрос. Проверка выполнения лабораторных работ
2.5	Тестирование построенных выборок №10-15			2			Опрос. Проверка выполнения лабораторных работ
2.6	Подготовка заключения о блочном шифре					4	Зачет задания
ИТОГО				26		8	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Рекомендуемая литература

Основная

1. Харин Ю. С., Агиевич С. В., Васильев Д. В., Матвеев Г. В. Криптология. — Минск: БГУ, 2013.
2. FIPS Publication 140–2. Security Requirements for Cryptographic Modules. National Institute of Standards and Technology. 2001
3. NIST Special Publication 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology. 2000.
4. Application Notes and Interpretation of the Scheme 31: Functionality classes and evaluation methodology for physical random number generators. Bundesamt für Sicherheit in der Informationstechnik. 2001.
5. Menezes A.J., van Oorschot P. C., Vanstone S.A. Handbook of Applied Cryptography. — CRC Press, 1996.
6. Soto J. Randomness Testing of the AES Candidate Algorithms. <http://www.nist.gov/aes/>.

Дополнительная

1. Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим методам защиты информации. — Минск, БГУ, 2001.

Организация управляемой самостоятельной работы студентов

Управляемая самостоятельная работа (УСР) студентов – это самостоятельная работа, выполняемая по заданию и при методическом руководстве преподавателя, а также контролируемая преподавателем на определенном этапе обучения. Целью УСР является целенаправленное обучение студентов основным навыкам и умению индивидуальной самостоятельной работы.

На освоение учебного материала в рамках УСР для дисциплины «Тестирование генераторов случайных и псевдослучайных последовательностей» отводится 8 аудиторных часа.

В рамках УСР дисциплины «Тестирование генераторов случайных и псевдослучайных последовательностей» выносятся следующие темы:

1. Подготовка заключения о выходных последовательностях.
2. Подготовка заключения о блочном шифре.

Контроль осуществляется в виде зачета задания.

Результативность самостоятельной работы студентов во многом определяется наличием активных методов ее контроля:

- входной контроль знаний и умений студентов в начале изучения очередной дисциплины;
- текущий контроль, то есть регулярное отслеживание уровня усвоения материала на лекциях, практических и лабораторных занятиях;
- промежуточный контроль по окончании изучения раздела или модуля курса;
- самоконтроль, осуществляемый студентом в процессе изучения дисциплины при подготовке к контрольным мероприятиям;
- итоговый контроль по дисциплине в виде зачета или экзамена;
- контроль остаточных знаний и умений спустя определенное время после завершения изучения дисциплины.

Рекомендации по контролю качества усвоения знаний и проведению аттестации

На лекционных занятиях по учебной дисциплине «Тестирование генераторов случайных и псевдослучайных последовательностей» рекомендуется использовать элементы проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Для аттестации обучающихся на соответствие их персональных достижений поэтапным и конечным требованиям образовательной программы создаются фонды оценочных средств, включающие типовые задания, контрольные работы и тесты. Оценочными средствами предусматривается оценка способности обучающихся к творческой деятельности, их готовность вести поиск решения новых задач, связанных с недостаточностью конкретных специальных знаний и отсутствием общепринятых алгоритмов.

Для диагностики компетенций в рамках учебной дисциплины рекомендуется использовать следующие формы:

- устная форма: собеседования, устные промежуточные и итоговый зачеты.
- письменная форма: тесты, контрольные опросы, контрольная работа.
- устно-письменная форма: отчеты по домашним практическим упражнениям с их устной защитой.

Контрольные мероприятия проводятся в соответствии с учебно-методической картой дисциплины. В случае неявки на контрольное мероприятие по уважительной причине студент вправе по согласованию с преподавателем выполнить его в дополнительное время. Для студентов, получивших неудовлетворительные оценки за контрольные мероприятия, либо не явившихся по неуважительной причине, по согласованию с преподавателем и с разрешения заведующего кафедрой мероприятие может быть проведено повторно.

Оценка текущей успеваемости рассчитывается как среднее оценок за каждую из письменных контрольных работ, оценки за отчеты по домашним практическим упражнениям и оценки за итоговый тест.

Итоговая аттестация предусматривает проведение зачета. При этом рекомендуется использовать оценивание успеваемости на основе модульно-рейтинговой системы.

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)
Криптографические методы	Кафедра математического моделирования и анализа данных	нет	Оставить содержание учебной дисциплины без изменения, протокол № 8 от 01 декабря 2015 г.
Теория вероятностей и математическая статистика	Кафедра математического моделирования и анализа данных	нет	Оставить содержание учебной дисциплины без изменения, протокол № 8 от 01 декабря 2015 г.
Статистический анализ данных	Кафедра математического моделирования и анализа данных	нет	Оставить содержание учебной дисциплины без изменения, протокол № 8 от 01 декабря 2015 г.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ

на ____/____ учебный год

№№ Пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры дискретной математики и алгоритмики (протокол № ____ от _____ 201_ г.)

Заведующий кафедрой

(ученая степень, звание)

(подпись)

(И.О. Фамилия)

УТВЕРЖДАЮ

Декан факультета

(ученая степень, звание)

(подпись)

(И.О.Фамилия)