Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и
образовательным инновациям
_____ О. И. Чуприс
«18» 12 2018 г.

Регистрационный № УД-6268 /уч.

ТЕОРИЯ КОНЕЧНЫХ АВТОМАТОВ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности первой ступени высшего образования:

1-98 01 01 Компьютерная безопасность (по направлениям)
направления специальности
1-98 01 01-01 Компьютерная безопасность
(математические методы и программные системы)

2018 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-98 01 01-2013 и учебных планов Р98-138/уч., Р98и-141/уч. от 30.05.2013.

СОСТАВИТЕЛИ:

А.Н. Гайдук, старший преподаватель кафедры математического моделирования и анализа данных факультета прикладной математики и информатики Белорусского государственного университета.

В.В. Пьянов, ассистент кафедры математического моделирования и анализа данных факультета прикладной математики и информатики Белорусского государственного университета.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математического моделирования и анализа данных Белорусского государственного университета (протокол № 13 от 29 марта 2018 г.);

Научно-методическим Советом Белорусского государственного университета (протокол № 7 от 13 июля 2018 г.).

Одна / Бодягин И.А., зав. кафедрой ММАД /

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цель преподавания учебной дисциплины – изложение теоретических аспектов теории конечных автоматов и практических результатов моделирования различных процессов и систем. Кроме того, целью преподавания дисциплины является изучение студентами методов проведения анализа программных реализаций; изучение студентами основных каналов утечки информации.

В рамках поставленной цели ***задачи*** учебной дисциплины состоят в следующем:

1) изучение основных понятий теории конечных автоматов и их свойства;
2) приобретение практических навыков для решения прикладных задач теории конечных автоматов;
3) изучение современных средств и методов обнаружения некоторых каналов утечки информации, возможностей DLP-систем по ее предотвращению.

Учебная дисциплина «Теория конечных автоматов. Информационная безопасность и безопасность информационных технологий» относится к циклу дисциплин специализации.

Учебная программа составлена с учетом межпредметных связей с учебными дисциплинами. Так, основой для изучения дисциплины «Теория конечных автоматов. Информационная безопасность и безопасность информационных технологий» являются дисциплины «Геометрия и алгебра» и «Теория вероятностей и математическая статистика». Знания, полученные в результате изучения дисциплины, будут использованы при изучении дисциплины «Компьютерная безопасность распределенных систем», а также способствовать успешному прохождению преддипломной практики и подготовки дипломной работы.

В результате освоения учебной дисциплины студент магистратуры должен:

знать:

– основные понятия теории конечных автоматов и их свойства;

– операции с автоматами;

– метод определения веса ограниченно-детерминированной функции;

– метод построения автомата приведенного вида;

– метод построения диагностического дерева;

– основные методы анализа программных реализаций;

– основные каналы утечки информации;

– основные возможности DLP-систем;

уметь:

– использовать модель конечного автомата при решении прикладных задач информационных технологий;

– применять при анализе программных реализаций метод экспериментов с «черным ящиком», статический и динамический методы;

– применять комплексный подход при анализе программных реализаций;

владеть:

– математическим аппаратом теории конечных автоматов;

– навыками использования средств анализа программ.

Освоение учебной дисциплины «Теория конечных автоматов. Информационная безопасность и безопасность информационных технологий» должно обеспечить формирование следующих академических, социально-личностных и профессиональных компетенций:

академические компетенции**:**

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

социально-личностные компетенции:

СЛК-3. Обладать способностью к межличностным коммуникациям.

профессиональные компетенции:

ПК-2. Формулировать задачи, возникающие при организации защиты информации.

ПК-13. Владеть современными средствами телекоммуникаций.

ПК-21. Эксплуатировать программные, аппаратно-программные и технические средства и системы защиты информации; разрабатывать необходимую документацию.

Структура содержания учебной дисциплины включает такие дидактические единицы, как темы (разделы), в соответствии с которыми разрабатываются и реализуются соответствующие лекционные и семинарские занятия. Примерная тематика занятий приведена в информационно-методической части.

Дисциплина изучается в 7 семестре. Всего на освоение учебной дисциплины «Теория конечных автоматов. Информационная безопасность и безопасность информационных технологий» отведено 159 часов, в том числе 68 аудиторных часов, из них: лекции – 34 часа, лабораторные занятия – 30 часов, управляемая самостоятельная работа – 4 часа.

Трудоемкость учебной дисциплины составляет 2 зачетные единицы.

Форма текущей аттестации – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел I. Введение

Тема 1.1. Понятие о конечных автоматах и способах их задания. Определение абстрактного конечного автомата. Способы задания конечных автоматов. Диаграмма Мура. Частные случаи конечных автоматов. Примеры конечных автоматов.

Тема 1.2. Функционирование конечных автоматов. Канонические уравнения функционирования конечного автомата. Структурный и абстрактный конечные автоматы. Синтез конечных автоматов.

Раздел II. Автоматы как преобразователи

Тема 2.1. Поведение конечных автоматов. Анализ и синтез конечных автоматов.

Тема 2.2. Детерминированные и ограниченно-детерминированные функции. Определение детерминированной и ограниченно-детерминированной функции. Информационное дерево. Остаточная функция. Вес ограниченно-детерминированной функции. Реализация конечным автоматом ограниченно-детерминированной функции. Усеченное информационное дерево. Теорема о числе ограниченно-детерминированных функций заданного веса.

Тема 2.3. Периодические свойства ограниченно-детерминированных функций. Теорема о преобразовании сверхслова с помощью ограниченно-детерминированных функций заданного веса. Теорема о минимальном периоде ограниченно-детерминированных функций.

Тема 2.4. Неотличимые состояния конечного автомата. Критерий неотличимости состояний конечного автомата. Критерий неотличимости состояний двух конечных автоматов.

Тема 2.5. Отличимость конечных автоматов. Определение вложимости и слабой вложимости конечных автомата. Теорема показывающая, что отношения вложимости и слабой вложимости не являются симметричными. Определение слабой неотличимости и отличимости конечных автоматов. Граф конечного автомата. Классы конечных автоматов. Конечный автомат приведенного вида. Изоморфизм конечных автоматов.

Тема 2.6. Эксперименты с автоматами. Понятие эксперимента с конечными автоматами. Типы экспериментов с автоматами. Построение диагностического дерева для конечного автомата. Оценки сложности экспериментов с автоматами. Теорема о длине простого условного установочного эксперимента.

Раздел III. Автоматы как акцепторы

Тема 3.1. Представление событий конечными автоматами. Определение представления события конечным автоматом. Операции над событиями. Регулярные события.

Тема 3.2. Теорема Клини. Вспомогательные леммы. Теорема Клини. Построение регулярных событий.

Раздел IV. Информационная безопасность и безопасность информационных технологий

Тема 4.1. Безопасность программного обеспечения и актуальность задачи анализа программ. Инструменты и методы анализа. Безопасность программного обеспечения. Актуальность задачи анализа программных реализаций. Обзор методов проведения анализа: метод экспериментов с «черным ящиком», статический метод, динамический метод. Инструментарий для анализа программных реализаций для ОС Windows: отладчик MSVS, IDA, Hiew, SoftICE, Reflector.

Тема 4.2. Уязвимости в программном обеспечении. Типичные ошибки, приводящие к уязвимостям в программном обеспечении (переполнения буферов, отсутствие проверок входных данных, некорректный контекст безопасности, устаревшие функции, и другие). Некоторые методики поиска уязвимостей. Уязвимость «нулевого дня». Понятие эксплоита и шелл-кода. Некоторые методики поиска уязвимостей. Пример эксплуатации локальной уязвимости операционной системы Windows, приводящей к повышению привилегий. Ошибки в прикладном программном обеспечении, приводящие к нарушению безопасности всей системы.

Тема 4.3. Комплексное применение методов анализа. Комплексное применение различных методов, средств и подходов к анализу программных реализаций недокументированных алгоритмов. Особенности анализа параллельного кода. Особенности анализа кода в режиме ядра. Вспомогательные инструменты анализа программ.

Тема 4.4. Защита программного обеспечения от анализа. Актуальность защиты программного обеспечения от анализа. Способы защиты: встроенная защита, пристыковочная защита. Методы защиты: динамическое изменение кода программы, искусственное усложнение кода программы, нестандартные обращения к функциям ОС, искусственное усложнение алгоритмов обработки данных, выявление факта выполнения под отладчиком.

Тема 4.5. Информационная безопасность организации. Информационная безопасность организации. Утечки информации, классификация каналов утечки информации. Системы предотвращения утечки информации (DLP-системы). Виды DLP-систем. Знакомство с DLP-

системой «Контур информационной безопасности» SearchInform. Состав комплекса. Этапы выявления утечек информации.

Тема 4.6. Методы социальной инженерии. Понятие социальной инженерии. Kali Linux как средство проведения атак социальной инженерии. Техники социальной инженерии. Использование поисковых средств в социальной инженерии. Утилиты Maltego, Recon-NG, CUPP, CeWL, SEToolkit. Принципы проведения фишинговых атак.

Тема 4.7. Принципы использования программного комплекса SearchInform. Установка и первоочередная настройка программного комплекса SearchInform. Принципы использования программного комплекса SearchInform для мониторинга утечек конфиденциальной информации.

Тема 4.8. Настройка программного комплекса SearchInform для контроля содержимого экранов пользователей и поиска конфиденциальной информации без проведения синтаксического анализа. Реализации периодического и оперативного контроля экранов пользователей. Поиск конфиденциальной информации без проведения синтаксического анализа. Методы формирования критериев поиска конфиденциальной информации «по атрибутам» и «нераспознанных».

Тема 4.9. Настройка программного комплекса SearchInform для поиска конфиденциальной информации на основе подобия текстовых фрагментов. Формирование критерия «Поиск похожих». Формирование критерия «Поиск по цифровым отпечаткам» на основании имеющейся библиотеки цифровых отпечатков. Формирование критерия «Поиск по цифровым отпечаткам» на основании нового каталога цифровых отпечатков. Формирование сложных запросов. Формирование критерия «Фразовый поиск».

Тема 4.10. Оценка защищенности компьютерных систем и сетей организации. Методики проведения тестирования на проникновение. Фреймворк Metasploit. Сканирование на наличие уязвимостей, утилиты Nessus, Nmap, Wmap. Использование Metasploit Community Edition, Armitage.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов			Количество часов в УСР	Форма контроля знаний
		Лекции	Семинарские Занятия	Лабораторные занятия		
1	**Введение**	**6**				
1.1	Понятие конечного автомата. Способы задания конечных автоматов.	2				Устный опрос
1.2	Функционирование конечных автоматов. Операции над конечными автоматами.	2				Устный опрос
	Абстрактный конечный автомат и структурный конечный автомат. Синтез конечных автоматов.	2				Устный опрос
2	**Автоматы как преобразователи**	**22**				
2.1	Поведение конечных автоматов. Анализ и **с**интез конечных автоматов.	2				Устный опрос
2.2	Детерминированные и ограниченно-детерминированные функции.	2				Устный опрос
	Вес о.-д. функции. Реализация о.-д. функций автоматами.	2				Устный опрос
2.3	Периодические свойства ограниченно-детерминированных функций	2				Устный опрос. Коллоквиум
2.4	Неотличимые состояния конечного автомата.	4				Устный опрос. Защита подготовленного реферата.

2.5	Отличимость конечных автоматов. Вложимость и слабая вложимость конечных автомата.	2				Устный опрос
	Граф конечного автомата. Классы конечных автоматов. Конечный автомат приведенного вида.	2				Устный опрос
2.6	Эксперименты с автоматами. Понятие эксперимента с конечными автоматами. Типы экспериментов с автоматами.	2				Устный опрос
	Построение диагностического дерева для конечного автомата..	2				Устный опрос
	Оценки сложности экспериментов с автоматами.	4				Устный опрос. Коллоквиум
3	**Автоматы как акцепторы**	**6**				
3.1	Представление событий конечными автоматами. Операции над событиями. Регулярные события.	2				Устный опрос
3.2	Теорема Клини. Построение регулярных событий.	4				Устный опрос
4	**Информационная безопасность и безопасность информационных технологий**			**30**	**4**	
4.1	Безопасность программного обеспечения и актуальность задачи анализа программ. Инструменты и методы анализа.			4		Защита лабораторной работы

4.2	Уязвимости в программном обеспечении			4		Защита лабораторной работы
4.3	Комплексное применение методов анализа			2	2	Защита лабораторной работы. Контрольная работа №1.
4.4	Защита программного обеспечения от анализа			4		Защита лабораторной работы
4.5	Информационная безопасность организации			4		Защита лабораторной работы.
4.6	Методы социальной инженерии			4		Защита лабораторной работы
4.7	Принципы использования программного комплекса SearchInform.			2		Защита лабораторной работы.
4.8	Настройка программного комплекса SearchInform для контроля содержимого экранов пользователей и поиска конфиденциальной информации без проведения синтаксического анализа.			2		Защита лабораторной работы
4.9	Настройка программного комплекса SearchInform для поиска конфиденциальной информации на основе подобия текстовых фрагментов			2	2	Защита лабораторной работы. Контрольная работа №2
4.10	Оценка защищенности компьютерных систем и сетей организации			2		Защита лабораторной работы.
ИТОГО		**34**		**30**	**4**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Hopcroft, J. E.Introduction to Automata Theory, Languages, and Computation (3rd Edition) / J. E Hopcroft, R. Motwani , J. D. Ullman. - Pearson, 2006.– 535 p.
2. Renji, T Finite Automata and Application to Cryptography / T. Renji. – Springer, 2009.– 350~p.
3. Проскурин В.Г. Защита программ и данных. Издательство: Академия, 2012. – 208 с.
4. Садердинов А.А., Трйнев В.А., Федулов А.А. Информационная безопасность предприятия: учебное пособие. -2-е изд. – М., Издательско-торговая корпорация «Дашком и Ко», 2005. – 336 с.
5. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учебное пособие для вузов. – М.: Радио и связь, 2000. – 168 с.

Перечень дополнительной литературы

1. Гилл, А. Введение в теорию конечных автоматов / А. Гилл. – М.: Наука, 1966. – 272 с.
2. Кудрявцев, В.Б. Введение в теорию абстрактных автоматов / В.Б. Кудрявцев, А.С. Подколзин, Ш. Ушчумлич. – М.: Изд-во Моск. ун-та, 1985. – 174 с.
3. М. Руссинович, Д. Соломон. Внутреннее устройство Microsoft Windows, 6-е издание (Часть 1). Издательство: Питер, 2013. – 800 с.
4. К. Касперски. Техника и философия хакерских атак. М.: Солон-Пресс, 2004

Рекомендуемая тематика контрольных работ

1) Контрольная работа №1. Защита программного обеспечения от анализа.

2) Контрольная работа №2. Использование программного комплекса SearchInform.

Методические рекомендации по организации самостоятельной работы обучающихся

Для организации самостоятельной работы студентов по учебной дисциплине следует использовать современные информационные

технологии: разместить в сетевом доступе комплекс учебных и учебно-методических материалов (учебно-программные материалы, ссылки на учебные издания для теоретического изучения дисциплины, методические указания к лабораторным занятиям, материалы текущего контроля и текущей аттестации, позволяющие определить соответствие учебной деятельности обучающихся требованиям образовательных стандартов высшего образования и учебно-программной документации, в т.ч. вопросы для подготовки к зачету, задания, тесты, вопросы для самоконтроля, тематика рефератов и др., список рекомендуемой литературы, информационных ресурсов и др.). Эффективность самостоятельной работы студентов проверяется в ходе текущего и итогового контроля знаний. Для общей оценки качества усвоения студентами учебного материала рекомендуется использование рейтинговой системы.

Перечень рекомендуемых средств диагностики

Для текущего контроля качества усвоения знаний студентами используется следующий диагностический инструментарий:

1. Устная форма: устные опросы; защиты отчетов по домашним заданиям, при выполнении студентами магистратуры лабораторных работ; проведение коллоквиума; защита подготовленного студентом реферата (рефераты используются для обобщения и систематизации учебного материала; в процессе подготовки реферата студент мобилизует и актуализирует имеющиеся умения, приобретает самостоятельно новые знания, необходимые для раскрытия темы, сопоставляя разные позиции и точки зрения).
2. Письменная форма: письменные контрольные работы по отдельным темам учебной дисциплины.

Методика формирования итоговой оценки

Формой текущей аттестации по учебной дисциплине «Теория конечных автоматов. Информационная безопасность и безопасность информационных технологий» учебным планом предусмотрены зачет и экзамен.

Рекомендуется использовать рейтинговую оценку знаний студента, дающую возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине. Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний в рейтинговую оценку:

- подготовка реферата – 15 %;
- работа на лабораторных занятиях – 35 %;
- контрольные работы – 30 %;

- коллоквиум – 20 %.

Итоговая оценка формируется на основе:

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

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)
Компьютерная безопасность распределенных систем	Информационных систем управления	нет	Оставить содержание учебной дисциплины без изменения, протокол № 13 от 29.03.2018 г.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

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

Заведующий кафедрой

_____ _____ _____

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____