Аннотация к рабочей программе дисциплины

«Теория автоматов»

Рабочая программа учебной дисциплины «Теория автоматов» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин вариативной части учебного плана Б1.В.02.

Трудоёмкость дисциплины в зачетных единицах составляет 3 з.е., в академических часах – 108 часов. Учебным планом предусмотрены лекционные занятия – 18 часов, практические занятия – 36 часов, самостоятельная работа студента – 54 часов. Дисциплина реализуется на 3 курсе в 5 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Теория автоматов» логически и содержательно связана с такими курсами, как «Информатика», «Дискретная математика», «Методы программирования».

Курс раскрывает понятия теории конечных автоматов, грамматик; разъясняет иерархию языков в зависимости от сложности их представления и распознавания; прививает навыки построения конечных моделей для решения задач распознавания и умения доказывать неразрешимость проблем для различных вычислительных моделей.

Цель изучения дисциплины «Теория автоматов» заключается в развитии у студентов теоретических представлений и практических навыков применения регулярных и контекстно-свободных языков, конечных автоматов и автоматов с магазинной памятью, конечных преобразователей и преобразователей с магазинной памятью.

Задачи дисциплины**:**

– изучение основных понятий теории автоматов, формальных языков и трансляций, направленных на повышение эффективности разработки компьютерных программ и оптимизацию программного кода;

– получение базовых знаний, которые необходимы для последующего изучения дисциплин.

Для успешного изучения дисциплины «Теория автоматов» у обучающихся должны быть сформированы следующие предварительные компетенции:

– способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);

– способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);

– способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);

– способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
ПК-3 – способность проводить анализ безопасности компьютерных систем	Знает	защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и

на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности		логике аудита; основные средства и методы анализа программных реализаций; физическую организацию баз данных и принципы (основы) их защиты; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы индентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений
	Умеет	формулировать настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищённые протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях
	Владеет	навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространённых семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; методиками анализа сетевого трафика
ПК-4 – способность проводить анализ и участвовать в разработке математических	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной

моделей безопасности компьютерных систем		среды и безопасности информационных потоков
	Умеет	разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
	Владеет	методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов

Для формирования вышеуказанных компетенций в рамках дисциплины «Теория автоматов» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: конспект (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2).