Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КРИПТОЛОГИИ И ДИСКРЕТНОЙ МАТЕМАТИКИ

ОДОБРЕНО УМС ИИКС

Протокол № 4/1/2023

от 25.04.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

БУЛЕВЫ ФУНКЦИИ И КОНЕЧНЫЕ АВТОМАТЫ / BOOLEAN FUNCTIONS AND FINITE AUTOMATA

Направление подготовки (специальность) [1] 10.03.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
5	2	72	32	16	0		24	0	З
Итого	2	72	32	16	0	0	24	0	

АННОТАЦИЯ

Дисциплина содействует формированию научного мировоззрения и системного мышления; посвящена изучению основных разделов теории булевых функций и теории конечных автоматов, используемых для изучения свойств криптографических систем, их синтеза и анализа. Основное внимание уделяется свойствам булевых функций, важных с точки зрения их криптографических приложений, а также способам построения и анализа шифрующих автоматов.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель освоения учебной дисциплины состоит в формировании у обучаемых знаний основных математических конструкций, лежащих в основе криптографических и стеганографических методов защиты информации.

Данная дисциплина участвует в формировании следующих профессиональных компетенций:

- способность применять соответствующий математический аппарат для решения профессиональных задач;
- способность участвовать в развитии математических, физических и/или технических методов обеспечения безопасности компьютерных систем.

Задачи дисциплины:

- изучение основных теоретических положений и методов решения теоретических и прикладных задач в области алгебры логики и теории конечных автоматов;
- приобретение навыков использования математических моделей применительно к задачам практического характера;
- формирование способности у студента применять изучаемый в курсе математический аппарат для исследования свойств функций и алгоритмов;
- получение студентом необходимой математической подготовки для изучения криптологии: схем симметричного и асимметричного шифрования, алгоритмов электронной подписи и криптографических протоколов.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Учебная дисциплина является базой для изучения следующих учебных дисциплин и/или составных частей учебных дисциплин:

- Криптографические методы защиты информации;
- Теория информационной безопасности и методология защиты информации;
- Технология построения защищенных автоматизированных систем.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектно-технологический			
проектирование и разработка систем информационной безопасности	технологии обеспечения информационной безопасности компьютерных систем	ПК-2 [1] - способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов *Основание:* Профессиональный стандарт: 06.032	З-ПК-2[1] - знать действующие нормативные и методические документы по проектированию подсистемы безопасности информации ; У-ПК-2[1] - уметь проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов; В-ПК-2[1] - владеть принципами проектирования подсистемы безопасности информации
организационно-управленческий			
организация работы по эксплуатации системы защиты информации	системы защиты информации	ПК-4 [1] - способен разрабатывать предложения по совершенствованию системы управления безопасностью информации в организации *Основание:* Профессиональный стандарт: 06.032	З-ПК-4[1] - знать методы построения системы управления безопасностью информации ; У-ПК-4[1] - уметь разрабатывать предложения по совершенствованию системы управления безопасностью информации в организации; В-ПК-4[1] - владеть принципами

			построения системы управления безопасностью информации

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения (В18)	Использование воспитательного потенциала дисциплин профессионального модуля для формирования у студентов ответственности за свое профессиональное развитие посредством выбора студентами индивидуальных образовательных траекторий, организации системы общения между всеми участниками образовательного процесса, в том числе с использованием новых информационных технологий.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование научного мировоззрения, культуры поиска нестандартных научно-технических/практических решений, критического отношения к исследованиям лженаучного толка (В19)	1.Использование воспитательного потенциала дисциплин/практик «Научно-исследовательская работа», «Проектная практика», «Научный семинар» для: - формирования понимания основных принципов и способов научного познания мира, развития исследовательских качеств студентов посредством их вовлечения в исследовательские проекты по областям научных исследований. 2.Использование воспитательного потенциала дисциплин "История науки и инженерии", "Критическое мышление и основы научной коммуникации", "Введение в специальность", "Научно-исследовательская работа", "Научный семинар" для: - формирования способности отделять настоящие научные исследования от лженаучных посредством проведения со студентами занятий и регулярных бесед; - формирования критического мышления, умения рассматривать

		различные исследования с экспертной позиции посредством обсуждения со студентами современных исследований, исторических предпосылок появления тех или иных открытий и теорий.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование профессионально значимых установок: не производить, не копировать и не использовать программные и технические средства, не приобретённые на законных основаниях; не нарушать признанные нормы авторского права; не нарушать тайны передачи сообщений, не практиковать вскрытие информационных систем и сетей передачи данных; соблюдать конфиденциальность доверенной информации (В40)	1. Использование воспитательного потенциала дисциплин "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры написания и оформления программ, а также привития навыков командной работы за счет использования систем управления проектами и контроля версий. 2.Использование воспитательного потенциала дисциплины "Проектная практика" для формирования культуры решения изобретательских задач, развития логического мышления, путем погружения студентов в научную и инновационную деятельность института и вовлечения в проектную работу. 3.Использование воспитательного потенциала профильных дисциплин для формирования навыков цифровой гигиены, а также системности и гибкости мышления, посредством изучения методологических и технологических основ обеспечения информационной безопасности и кибербезопасности при выполнении и защите результатов учебных заданий и лабораторных работ по криптографическим методам защиты информации в компьютерных системах и сетях. 4.Использование воспитательного потенциала дисциплин " "Информатика (Основы программирования)",

		Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры безопасного программирования посредством тематического акцентирования в содержании дисциплин и учебных заданий. 5.Использование воспитательного потенциала дисциплины "Проектная практика" для формирования системного подхода по обеспечению информационной безопасности и кибербезопасности в различных сферах деятельности посредством исследования и перенятия опыта постановки и решения научно-практических задач организациями-партнерами.

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	5 Семестр						
1	Первый раздел	1-8	16/8/0		25	КИ-8	З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-4, У-ПК-4, В-ПК-4
2	Второй раздел	9-16	16/8/0		25	КИ-16	З-ПК-

							2, У-ПК-2, В-ПК-2, З-ПК-4, У-ПК-4, В-ПК-4
	Итого за 5 Семестр		32/16/0		50		
	Контрольные мероприятия за 5 Семестр				50	З	З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-4, У-ПК-4, В-ПК-4

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	5 Семестр	32	16	0
1-8	**Первый раздел**	16	8	0
1	**Элементарные булевы функции и способы их задания.** Определение булевой функции. Существенные переменные. Элементарные булевы функции. Табличное задание булевых функций. Вес. Равновероятная функция. Геометрическое и графическое задание булевых функций. Реализация функций формулами. Двойственная и самодвойственная функции.	Всего аудиторных часов		
		2	1	0
		Онлайн		
		0	0	0
2 - 3	**Нормальные формы булевых функций.** Дизъюнктивная нормальная форма (ДНФ). Теорема о	Всего аудиторных часов		
		4	2	0

	разложении функции по переменным. Совершенная ДНФ. Конъюнктивная нормальная форма (КНФ). Совершенная КНФ. Теорема о разложении булевой функции в виде многочлена Жегалкина. Степень нелинейности булевой функции. Теорема о разложении булевой функции в виде действительного многочлена.	Онлайн		
		0	0	0
4	**Спектральное представление булевых функций** Теорема о разложении в ряд Фурье. Спектр Уолша. Теорема о связи коэффициентов Фурье и Уолша.	Всего аудиторных часов		
		2	1	0
		Онлайн		
		0	0	0
5 - 6	**Полнота и замкнутость систем булевых функций.** Шефферова функция. Замыкание множества булевых функций, замкнутые классы, полные системы булевых функций. Важнейшие замкнутые классы булевых функций: классы функций, сохраняющих константу, классы самодвойственных, монотонных, аффинных и линейных функций и их мощности. Оценки мощности класса монотонных функций. Леммы о несамодвойственной, немонотонной и нелинейной функциях. Критерий полноты системы булевых функций и его следствия.	Всего аудиторных часов		
		4	2	0
		Онлайн		
		0	0	0
7 - 8	**Минимизация булевых функций.** Задача минимизации булевых функций. Минимальные ДНФ. Импликанта булевой функции. Сокращенная ДНФ. Тупиковые ДНФ. Геометрическая интерпретация минимизации ДНФ. Метод Квайна–Мак-Класки нахождения сокращенной ДНФ булевой функции. Теорема о получении сокращенной ДНФ. Метод Петрика нахождения тупиковых ДНФ.	Всего аудиторных часов		
		4	2	0
		Онлайн		
		0	0	0
9-16	**Второй раздел**	16	8	0
9 - 10	**Псевдобулевы функции и функции k-значной логики.** Определение и свойства псевдобулевых функций. Представление булевых функций через базисы. Функции k-значной логики. Основные понятия и элементарные функции. Табличное задание функций k-значной логики. Формулы над множеством функций. Важнейшие элементарные функции. 1-ая и 2-ая формы функций k-значной логики. Важные классы функций k-значной логики. Замкнутые и полные классы. Распознавание полноты и критерии полноты. Теорема Кузнецова. Теорема Слупецкого. Существенная функция. Теорема Пикара. Теорема Саломаа. Особенности k-значных логик.	Всего аудиторных часов		
		4	2	0
		Онлайн		
		0	0	0
11 - 12	**Классификация булевых функций.** Постановка задачи классификации булевых функций. Эквивалентность булевых функций относительно групп преобразований. Определения и мощности групп преобразований, используемых для классификации булевых функций. Основные свойства эквивалентных булевых функций.	Всего аудиторных часов		
		4	2	0
		Онлайн		
		0	0	0
13 - 14	**Конечные автоматы.** Конечные автоматы Мили. Основные определения. Виды конечных автоматов Мили. Табличный способ задания автоматов Мили. Задание автоматов Мили автоматным	Всего аудиторных часов		
		4	2	0
		Онлайн		
		0	0	0

	графов. Задание автоматов формулами и алгоритмами; формулами и схемами. Неавтономный регистр сдвига. Внутренне автономный автомат, построенный на основе регистра сдвига. Однородные и согласованные автоматы. Объединение автоматов. Последовательное соединение и прямая сумма автоматов. Гомоморфизм и изоморфизм автоматов			
15 - 16	**Эквивалентность для конченых автоматов.** Реакция состояния и реакция автомата Мили. Эквивалентность состояний и автоматов Мили. Сокращенные автоматы. Теорема Хаффмана-Мили и следствия из нее. Теорема о сокращении. Различимость входных последовательностей автоматами Мили. Теорема Чена.	Всего аудиторных часов		
		4	2	0
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии сочетают в себе совокупность методов и средств для реализации определенного содержания обучения и воспитания в рамках дисциплины, включают решение дидактических и воспитательных задач, формируя основные понятия дисциплины, технологии проведения занятиий, усвоения новых знаний, технологии повторения и контроля материала, самостоятельной работы.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-2	З-ПК-2	З, КИ-8, КИ-16
	У-ПК-2	З, КИ-8, КИ-16

	В-ПК-2	З, КИ-8, КИ-16
ПК-4	З-ПК-4	З, КИ-8, КИ-16
	У-ПК-4	З, КИ-8, КИ-16
	В-ПК-4	З, КИ-8, КИ-16

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной учебной дисциплины в соответствии с планом лекций и семинарских занятий, графиком контроля знаний.

Успешное освоение дисциплины требует от студентов посещения лекций, активной работы во время семинарских занятий, выполнения всех домашних заданий, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Во время лекций рекомендуется писать конспект. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки.

При необходимости в конце лекции преподаватель оставляет время для того, чтобы студенты имели возможность задать вопросы по изучаемому материалу.

Лекции нацелены на освещение основополагающих положений теории алгоритмов и теории функций алгебры логики, наиболее трудных вопросов, как правило, связанных с доказательством необходимых утверждений и теорем, призваны способствовать формированию навыков работы с научной литературой. Предполагается также, что студенты приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Конспект лекций для закрепления полученных знаний необходимо просмотреть сразу после занятий. Хорошо отметить материал конспекта лекций, который вызывает затруднения для понимания. Можно попытаться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале,

рекомендуется сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

В процессе изучения учебной дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам, а также для выполнения домашних заданий, которые выдаются после каждого семинара.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами в ходе лекций, аудиторных практических занятий, лабораторных и самостоятельных занятий.

Данная дисциплина выполняет функции теоретической и практической подготовки студентов. Содержание дисциплины распределяется между лекционной и практической частями на основе принципа дополняемости: практические занятия, как правило, не дублируют лекции и посвящены рассмотрению практических примеров и конкретизации материала, введенного на лекции. В лекционном курсе главное место отводится общетеоретическим проблемам.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в отечественных и зарубежных научно-практических публикациях;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечении по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и работе на семинарских занятиях.

Автор(ы):

Епишкина Анна Васильевна, к.т.н.