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 №8/1/2025 от 25.08.2025 г.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

## СИСТЕМЫ АНАЛИТИЧЕСКИХ ВЫЧИСЛЕНИЙ

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** |
|---|---|---|---|---|---|---|---|---|---|
| 6 | 2 | 72 | 30 | 0 | 15 | | 27 | 0 | 3 |
| Итого | 2 | 72 | 30 | 0 | 15 | 0 | 27 | 0 | |

# АННОТАЦИЯ

Цель освоения учебной дисциплины «Системы аналитических вычислений» - изучение возможностей проведения аналитических вычислений и приобретение навыков использования систем аналитических вычислений применительно к задачам, связанным с защитой информации.

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель освоения учебной дисциплины «Системы аналитических вычислений» - изучение возможностей проведения аналитических вычислений и приобретение навыков использования систем аналитических вычислений применительно к задачам, связанным с защитой информации.

В курсе рассматриваются следующие темы:

 аналитические вычисления и системы аналитических вычислений (САВ);

 представления булевых функций и вектор-функций и алгоритмы преобразования булевых функций из одного вида в другой с применением САВ;

 числовые характеристики булевых функций и вектор-функций и анализ алгоритмов их вычисления;

 исследование функций стандартных алгоритмов защиты информации с применением САВ;

 построение линейного регистра сдвига, эквивалентного линейному автомату, и исследование его свойств;

 построение линейной рекуррентной зависимости (алгоритм Берлекэмпа-Мэсси) для данной двоичной последовательности с применением САВ;

 восстановление начального состояния комбинирующего генератора по выходной последовательности;

 построение графа де Брёйна с применением САВ;

 реализация с применением САВ некоторых методов восстановления начального отрезка линейной рекуррентной последовательности по нерегулярной выборке;

 методы факторизации целых чисел и их реализация с применением САВ.

## 2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Полученные знания используются при изучении следующих дисциплин:

- Моделирование систем защиты информации;
- Аудит информационных технологий и систем обеспечения безопасности;
- Информационная безопасность открытых систем;
- Защита информации в банковских системах;
- Разработка и эксплуатация защищенных автоматизированных систем;
- Защищенный электронный документооборот в кредитно-финансовой сфере.

## 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-1.2 [1] - способен разрабатывать и анализировать алгоритмы решения профессиональных задач, реализовывать их в современных программных комплексах<br><br>*Основание:*<br>Профессиональный стандарт: 06.032 | З-ПК-1.2[1] - знать алгоритмы решения профессиональных задач;<br>У-ПК-1.2[1] - уметь разрабатывать и анализировать алгоритмы решения профессиональных задач, реализовывать их в современных программных комплексах;<br>В-ПК-1.2[1] - владеть принципами разработки и анализа алгоритмов решения профессиональных задач |
| организационно-управленческий | | | |
| организация работы по эксплуатации системы защиты информации | системы защиты информации | ПК-1.2 [1] - способен анализировать, оценивать и коммуницировать риски информационной безопасности в контексте бизнес-целей<br><br>*Основание:*<br>Профессиональный стандарт: 06.032 | З-ПК-1.2[1] - принципы качественного и количественного анализа рисков, методики расчета финансовых/репутационных потерь от инцидентов, знает требования стандартов управления рисками, нормативные акты и отраслевые стандарты, процедуры аудита и взаимодействия с регуляторами, принципы разработки политик ИБ под конкретные требования регуляторов, принципы визуализации данных (панели мониторинга (dashboard), инфографика), бизнес-метрики, релевантные |

| | | | |
|---|---|---|---|
| | | | заинтересованным сторонам, методы управления ожиданиями заинтересованных сторон;<br>У-ПК-1.2[1] - приоритезировать риски на основе их влияния на бизнес-процессы, формулировать рекомендации по информационной безопасности на языке бизнес-метрик, предлагать технические/организационные меры на основе юридических требований, готовить документацию для аудита, интегрировать соответствие регуляторным требованиям в ИТ-процессы, транслировать технические риски в бизнес-последствия, разрабатывать сбалансированные решения, включая поэтапное внедрение защиты с минимальным влиянием на релизы, проводить обучающие сессии для руководителей подразделений;<br>В-ПК-1.2[1] - принципами оценки рисков с учетом бизнес-последствий |
| эксплуатационный | | | |
| эксплуатация технических и программно-аппаратных средств защиты информации | программно-аппаратные средства защиты информации | ПК-1 [1] - способен устанавливать, настраивать и проводить техническое обслуживание средств защиты информации<br><br>*Основание:* Профессиональный стандарт: 06.032 | З-ПК-1[1] - знать требования к проведению технического обслуживания средств защиты информации ;<br>У-ПК-1[1] - уметь устанавливать, настраивать и проводить техническое обслуживание средств защиты информации;<br>В-ПК-1[1] - владеть навыками проведения технического обслуживания средств защиты информации |

## 4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

| Направления/цели воспитания | Задачи воспитания (код) | Воспитательный потенциал дисциплин |
|---|---|---|
| Профессиональное воспитание | Создание условий, обеспечивающих, | Использование воспитательного потенциала дисциплин |

| | | |
|---|---|---|
| | формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения (В18) | 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:<br>- 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:<br>- формирования способности отделять настоящие научные исследования от лженаучных посредством проведения со студентами занятий и регулярных бесед;<br>- 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 | 1. Использование воспитательного потенциала дисциплин "Информатика (Основы программирования)", |

| | | |
|---|---|---|
| | 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) | 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.<br>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.<br>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.<br>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.<br>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 |
|---|---|---|---|---|---|---|---|
| | *6 Семестр* | | | | | | |
| 1 | Первый раздел | 1-8 | 16/0/7 | | 25 | КИ-8 | В-ПК-1.2, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-1.2, У-ПК-1.2 |
| 2 | Второй раздел | 9-15 | 14/0/8 | | 25 | КИ-15 | З-ПК-1.2, У-ПК-1.2, В-ПК-1.2, З-ПК-1, У-ПК-1, В-ПК-1 |
| | *Итого за 6 Семестр* | | 30/0/15 | | 50 | | |
| | **Контрольные мероприятия за 6 Семестр** | | | | 50 | З | З-ПК-1.2, У-ПК-1.2, В-ПК-1.2, З-ПК-1, У-ПК-1, В-ПК-1 |

* – 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. |
|---|---|---|---|---|
| | *6 Семестр* | 30 | 0 | 15 |
| **1-8** | **Первый раздел** | 16 | 0 | 7 |
| 1 - 8 | **Раздел 1**<br>Системы аналитических вычислений (CAB);<br>применение CAB для анализа булевых функций и вектор-функций;<br>числовые характеристики булевых функций и вектор-функций и анализ алгоритмов их вычисления;<br>исследование функций стандартных алгоритмов защиты информации. | Всего аудиторных часов | | |
| | | 16 | 0 | 7 |
| | | Онлайн | | |
| | | 0 | 0 | 0 |
| **9-15** | **Второй раздел** | 14 | 0 | 8 |
| 9 - 15 | **Раздел 2**<br>Применение CAB для анализа генераторов битовых последовательностей<br>Факторизация целых чисел | Всего аудиторных часов | | |
| | | 14 | 0 | 8 |
| | | 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 |

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

| Недели | Темы занятий / Содержание |
|---|---|
| | *6 Семестр* |
| 1 - 8 | **Лабораторная работа1**<br>1. Исследование функций KASUMI (A5/3). |
| 9 - 12 | **Лабораторная работа 4**<br>Факторизация |
| 13 - 15 | **Лабораторная работа5**<br>Факторизация чисел |

## 6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Дисциплина сформирована как курс лекций и лабораторных работ, при выполнении которых используются современные программно-технические средства и системы компьютерной алгебры.

Для самостоятельной работы студентов используется рекомендуемая преподавателем учебная литература.

## 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-1 | З-ПК-1 | З, КИ-8, КИ-15 |
| | У-ПК-1 | З, КИ-8, КИ-15 |
| | В-ПК-1 | З, КИ-8, КИ-15 |
| ПК-1.2 | З-ПК-1.2 | З, КИ-8, КИ-15 |
| | У-ПК-1.2 | З, КИ-8, КИ-15 |
| | В-ПК-1.2 | З, КИ-8, КИ-15 |

**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 |
| 60-64 | | E | |

| | | | |
|---|---|---|---|
| | | | знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала. |
| 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:

1. 53 А64 Анализ и представление результатов эксперимента : учебно-методическое пособие, Воронов С.А. [и др.], Москва: НИЯУ МИФИ, 2015

2. 004 А 51 Машинное обучение: новый искусственный интеллект : пер. с англ., Алпайдин Э., Москва: Альпина Паблишер, 2017

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 занятий.

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

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.

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

Целью данных методических рекомендаций является повышение эффективности теоретических и практических занятий по дисциплине вследствие более четкой их организации преподавателем.

Данные рекомендации разработаны на основе многолетнего опыта преподавания и публикаций учебно-методического характера, а также многочисленных отечественных и зарубежных научных публикации по рассматриваемой тематике.

При изучении дисциплины рекомендуется использовать следующие средства обучения:

- рабочую программу дисциплины;
- рекомендуемую основную и дополнительную литературу;
- методические указания, пособия и учебники;
- фонд оценочных средств.

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 и самостоятельной работе.

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

Данная дисциплина выполняет функции теоретической и практической подготовки студентов.

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 предполагают самостоятельную проработку материала учебных пособий.

Автор(ы):

Велигура Александр Николаевич, к.ф.-м.н., с.н.с.