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 № УМС-575/01-1

от 30.08.2021 г.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

## ПРАКТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ КРИПТОСИСТЕМ

Направление подготовки (специальность) [1] 10.04.01 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 |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 108 | 12 | 12 | 0 | | 48 | 0 | Э |
| 3 | 3 | 108 | 12 | 12 | 0 | | 48 | 0 | Э |
| Итого | 6 | 216 | 24 | 24 | 0 | 0 | 96 | 0 | |

Москва, 2020

## АННОТАЦИЯ

В курсе рассматриваются следующие темы:
- шифры замены и перестановки, методы их анализа;
- теоретическая и практическая стойкость шифров, шифр Вернама;
- поточные шифры и принципы их построения;
- блочные шифры и принципы их построения;
- методы обеспечения целостности данных;
- криптосистемы с открытым ключом.
- управление ключами, инфраструктура открытых ключей, протокол Диффи-Хеллмана
- методы реализации криптосистем.

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – изучение современных международных и российских стандартов обеспечения информационной безопасности, криптографических методов и средств защиты информации.

## 2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Полученные в результате освоения учебной дисциплины знания, умения, навыки используются в процессе дипломного проектирования.

## 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** |
|---|---|---|---|
| научно- исследовательский | | | |
| выполнение научно-исследовательских работ по развитию физических, математических или технических методов обеспечения | методы обеспечения безопасности данных | ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем | З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, |

| | | | |
|---|---|---|---|
| безопасности данных | | безопасности и решать их с использованием новейшего отечественного и зарубежного опыта<br><br>*Основание:* Профессиональный стандарт: 06.032 | устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ;<br>У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.;<br>В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований. |

## 4. 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 |
|---|---|---|---|---|---|---|---|
| | *2 Семестр* | | | | | | |
| 1 | Первый раздел | 1-8 | | | 25 | КИ-8 | З-ПК-3, У-ПК-3, В-ПК-3 |
| 2 | Второй раздел | 9-15 | | | 25 | КИ-15 | З-ПК-3, У-ПК-3, В-ПК-3 |
| | *Итого за 2 Семестр* | | 12/12/0 | | 50 | | |
| | **Контрольные мероприятия за 2 Семестр** | | | | 50 | Э | З-ПК-3, У-ПК-3, В-ПК-3 |
| | *3 Семестр* | | | | | | |
| 1 | Первый раздел | 1-8 | | | 25 | КИ-8 | З-ПК-3, У-ПК-3, В-ПК-3 |
| 2 | Второй раздел | 9-16 | | | 25 | КИ-16 | З-ПК-3, У-ПК-3, В-ПК-3 |
| | *Итого за 3 Семестр* | | 12/12/0 | | 50 | | |
| | **Контрольные мероприятия за 3 Семестр** | | | | 50 | Э | З-ПК-3, У-ПК-3, В-ПК-3 |

* – 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 |
| Э | Экзамен |

## КАЛЕНДАРНЫЙ ПЛАН

| Недели | Темы занятий / Содержание | Лек., час. | Пр./сем., час. | Лаб., час. |
|---|---|---|---|---|
| | *2 Семестр* | 12 | 12 | 0 |
| **1-8** | **Первый раздел** | 6 | 6 | |
| 1 - 8 | **Особенности симметричных криптосистем**<br>Режимы блочного шифрования. Коды аутентичности сообщений, обеспечение целостности сообщений. Построение кодов аутентичности сообщений на основе блочных шифров.Стойкие к коллизиям и односторонние хэш-функции. Принципы построения хэш-функций. Построение кодов аутентичности сообщений с использование хэш-функций. Выработка симметричных ключей с использованием хэш-функций и источника энтропии. | Всего аудиторных часов | | |
| | | 6 | 6 | |
| | | Онлайн | | |
| | | | | |
| **9-15** | **Второй раздел** | 6 | 6 | |
| 9 - 15 | **Реализация симметричных криптосистем**<br>Особенности программной реализации симметричных криптосистем. Особенности аппаратной реализации симметричных криптосистем. | Всего аудиторных часов | | |
| | | 6 | 6 | |
| | | Онлайн | | |
| | | | | |
| | *3 Семестр* | 12 | 12 | 0 |
| **1-8** | **Первый раздел** | 6 | 6 | |
| 1 - 8 | **Особенности асимметричных криптосистем**<br>Основные принципы построения. Требования к энтропии открытого текста. Криптосистемы, основанные на теории кодирования. Криптосистемы, основанные на задаче о рюкзаке. Использование в криптографии парных отображений | Всего аудиторных часов | | |
| | | 6 | 6 | |
| | | Онлайн | | |
| | | | | |
| **9-16** | **Второй раздел** | 6 | 6 | |
| 9 - 16 | **Реализация асимметричных криптосистем**<br>Особенности программной реализации асимметричных криптосистем. Особенности аппаратной реализации асимметричных криптосистем. | Всего аудиторных часов | | |
| | | 6 | 6 | |
| | | Онлайн | | |
| | | | | |

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 |

## 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Основными образовательными технологиями в освоении дисциплин профессионального цикла являются традиционные технологии лекций и лабораторных работ. Интерактивные методики обеспечиваются решением индивидуальных задач студентами и коллективным обсуждением результатов и методов решения.

## 6. 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)** | **Аттестационное мероприятие (КП 2)** |
|---|---|---|---|
| ПК-3 | З-ПК-3 | Э, КИ-8, КИ-15 | Э, КИ-8, КИ-16 |
| | У-ПК-3 | Э, КИ-8, КИ-15 | Э, КИ-8, КИ-16 |
| | В-ПК-3 | Э, КИ-8, КИ-15 | Э, 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 | | B | Оценка «хорошо» выставляется студенту, если он твёрдо знает |

| | | | |
|---|---|---|---|
| 75-84 | | C | материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос. |
| 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. |

Оценочные средства приведены в Приложении.

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. 004 М 21 Глобальная культура кибербезопасности : , Москва: Горячая линия -Телеком, 2018

2. 004 М 21 Комментарии к Доктрине информационной безопасности Российской Федерации. : , Москва: Горячая линия -Телеком, 2018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

## 8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

## 9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

прилоежны

## 10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

приложены

Автор(ы):

Когос Константин Григорьевич, к.т.н.