

**Федеральное государственное автономное образовательное  
учреждение высшего образования  
«Московский физико-технический институт  
(национальный исследовательский университет)»**

**УТВЕРЖДЕНО**  
**Директор физтех-школы**  
**аэрокосмических технологий**  
**С.С. Негодяев**

	<b>Рабочая программа дисциплины (модуля)</b>
<b>по дисциплине:</b>	Информационная безопасность
<b>по направлению:</b>	Информатика и вычислительная техника
<b>профиль подготовки:</b>	Программная инженерия передовая инженерная школа радиолокации, радионавигации и программной инженерии кафедра технологий проектирования сложных технических систем
<b>курс:</b>	1
<b>квалификация:</b>	магистр

Семестр, формы промежуточной аттестации: 2 (весенний) - Дифференцированный зачет

Аудиторных часов: 75 всего, в том числе:

лекции: 45 час.

семинары: 30 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 60 час.

Всего часов: 135, всего зач. ед.: 3

Программу составили:

А.А. Приходько, канд. физ.-мат. наук

О.И. Кузьмин

Программа обсуждена на заседании кафедры технологий проектирования сложных технических систем  
30.08.2021

## Аннотация

Дисциплина «Информационная безопасность» включает в себя знакомство студента с математическими основами современных криптографических технологий и практиками информационной безопасности, принятых в современных бизнес-структурах. Практические задания выполняются с использованием языков C/C++ и Python, а в случае разработки Интернет-систем (Б, В) дополнительно допускается использование языка JavaScript.

### 1. Цели и задачи

#### Цель дисциплины

- формирование знаний и навыков, достаточных для того, чтобы эффективно применять и понимать современные практики информационной безопасности и самостоятельно осваивать специальные знания, необходимые для их разработки.

#### Задачи дисциплины

- сформировать понимание математических основ криптографии и умение решать ряд типовых задач в этой области;
- сформировать понимание основ прикладной криптографии и умение решения ряда типовых задач в этой области;
- познакомить студентов с современными практиками информационной безопасности, применяемыми на промышленных предприятиях и в бизнес-структурах.

### 2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-3 Способен выбирать и (или) разрабатывать подходы к решению типовых и новых задач в области информатики и вычислительной техники, учитывая особенности и ограничения различных методов решения	ОПК-3.2 Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
ОПК-4 Способен успешно реализовывать решение поставленной задачи, провести анализ результата и представить выводы, применяя знания и навыки в области математики, естественных наук и информационно-коммуникационных технологий	ОПК-4.1 Способен применять знания и навыки по использованию информационно-коммуникационных технологий для поиска и изучения научной литературы, применения прикладных программных продуктов
ПК-2 Понимает и способен применить в научно-исследовательской и прикладной деятельности основные законы естествознания, современный математический аппарат и алгоритмы, современные информационно-коммуникационные технологии	ПК-2.1 Знает основы научно-исследовательской деятельности в области информационных технологий, владеет знанием основ философии и методологии науки; знанием методов научных исследований и навыками их проведения

### 3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- определения основных объектов и понятий из области математических основ криптографии;
- основные алгоритмы и подходы прикладной криптографии;
- ключевые концепции и подходы современных практик информационной безопасности.

уметь:

- применять знания из области математических основ криптографии для анализа и разработки криптографических алгоритмов;
- применять знания курса для анализа различных решений в области информационной безопасности.

владеть:

- математическим аппаратом прикладной криптографии;
- концепциями и понятиями современных практик информационной безопасности.

#### 4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

##### 4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Теория множеств и булева логика	2	1		3
2	Основы арифметики	2	2		4
3	Алгебраические структуры	4	2		4
4	Алгоритмические проблемы в кольцах $\mathbb{Z}/n\mathbb{Z}$	2	2		4
5	Кольца многочленов и поля Галуа	3	2		4
6	Матричные группы и линейные динамические системы	4	2		4
7	Эллиптическая криптография	3	2		4
8	Алгоритмы	2	2		4
9	Простейшие алгоритмы криптографии	3	2		4
10	Шифрование	2	2		4
11	Обмен ключами	3	2		3
12	Криптография с открытым ключом и цифровая подпись	2	2		4
13	Инфраструктура PKI	2	1		4
14	Понятие информационной безопасности	3	2		4
15	Основные концепции и термины информационной безопасности	4	2		4
16	Разработка и внедрение политики информационной безопасности	4	2		2
Итого часов		45	30		60
Подготовка к экзамену		0 час.			
Общая трудоёмкость		135 час., 3 зач.ед.			

##### 4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 2 (Весенний)

###### 1. Теория множеств и булева логика

Множества и отображения. Основные операции над множествами. Бинарные отношения. Перестановки. Логические формулы и предикаты.

## 2. Основы арифметики

Деление с остатком. Алгоритм Евклида. Простые числа и основная теорема арифметики. Китайская теорема об остатках. Распределение простых чисел.

## 3. Алгебраические структуры

Группы. Коммутативные группы. Группа перестановок. Кольца. Алгебраические свойства кольца вычетов  $\mathbb{Z}/n\mathbb{Z}$ .

## 4. Алгоритмические проблемы в кольцах $\mathbb{Z}/n\mathbb{Z}$

Диофантовы уравнения. Функция Эйлера. Быстрое возведение в степень. Дискретный логарифм. Надёжные датчики случайных чисел.

## 5. Кольца многочленов и поля Галуа

Алгоритм деления. Разложение на множители. Неприводимые многочлены. Арифметика в полях Галуа. Расширения и автоморфизмы полей.

## 6. Матричные группы и линейные динамические системы

Классические матричные группы. Линейные динамические системы в  $\mathbb{R}^n$  и их спектральные свойства. Матрицы с целочисленными коэффициентами. Линейные динамические системы над полями вычетов и полями Галуа. Автоморфизм Фробениуса.

## 7. Эллиптическая криптография

Конструкция эллиптической кривой над конечными полями. Проективные координаты. Эллиптическая арифметика. Теорема Хассе.

## 8. Алгоритмы

Понятие об алгоритмической сложности. Графы и деревья. Конечные автоматы и автоморфизмы деревьев. Классы P и NP. Криптоанализ – основные подходы. Представление о квантовых вычислениях.

## 9. Простейшие алгоритмы криптографии

Исторический обзор. Криптоанализ схем шифрования с биективным преобразованием. Хеширование - подходы и алгоритмы.

## 10. Шифрование

Понятие о схеме симметричного шифрования. Основные алгоритмы. Блочные шифры. Подходы к надёжному созданию ключей шифрования.

## 11. Обмен ключами

Использование схем ключевого обмена в телекоммуникационных системах. Алгоритм Диффи-Хеллмана. Алгоритмы ключевого обмена ГОСТ.

## 12. Криптография с открытым ключом и цифровая подпись

Принципы и подходы к созданию асимметричных схем шифрования и подписи. Алгоритм RSA. Алгоритмы ГОСТ.

### 13. Инфраструктура PKI

Стандарты представления криптографических сообщений. ASN.1. Дерево объектных идентификаторов OID. Сертификаты открытых ключей электронной цифровой подписи. Стандарты ГОСТ. Удостоверяющие центры и инфраструктура PKI. Практика внедрения инфраструктуры PKI в Российской Федерации.

### 14. Понятие информационной безопасности

Понятие информационной безопасности. Социальная инженерия как инструмент для предотвращения угроз информационной безопасности. Применение искусственного интеллекта при решении задач социальной инженерии. Структура построения государственной системы и основные законодательные требования по вопросам информационной и кибербезопасности в РФ.

### 15. Основные концепции и термины информационной безопасности

Основные термины и определения информационной безопасности. Ответственность должностных лиц за выполнение законодательных требований по вопросам ИБ. Инсайдеры и исходящие от них угрозы информационной безопасности. Кибероружие и кибервойны.

### 16. Разработка и внедрение политики информационной безопасности

Разработка и внедрение политики информационной безопасности. Обеспечение безопасного доступа к информационным активам. Перспективные вопросы информационной безопасности и кибербезопасности. Тест Тьюринга. Достижение состояния технологической сингулярности.

## 5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

учебная аудитория, оснащенная компьютером и мультимедийным оборудованием (проектор, звуковая система).

## 6. Перечень рекомендуемой литературы

### Основная литература

1. Информационная безопасность [Текст] : учеб. пособие для вузов / М. М. Котухов, А. Н. Кубанков, А. О. Калашников ; М-во обр. и науки РФ ; Федеральное агентство по обр.; Моск. физико-техн. ин-т (гос. ун-т) ; Академия ИБС .— М. : Академия ИБС : МФТИ, 2009 .— 194 с.
2. Информационная безопасность компьютерных систем и сетей [Текст] / В. Ф. Шаньгин - М.ФОРУМ : ИНФРА-М, 2012

### Дополнительная литература

1. Безопасность и управление доступом в информационных системах [Текст] : учеб. пособие для студентов средн. проф. образования / А. В. Васильков, И. А. Васильков .— М. : ФОРУМ, 2010 .— 368 с.
2. Алгоритмы телекоммуникационных сетей [Текст] : в 3 ч. : учеб. пособие для вузов. Ч. 3. Процедуры, диагностика, безопасность / Ю. А. Семенов .— М. : Интернет-Ун-т Информ. Технологий : БИНОМ. Лаб. знаний, 2007 .— 511 с.

## 7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Не используются

## **8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)**

На занятиях используются мультимедийные технологии, включая демонстрацию презентаций.  
На компьютерах в компьютерных классах должна быть установлены операционная система Windows.

## **9. Методические указания для обучающихся по освоению дисциплины (модуля)**

Студент, изучающий курс должен, с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике.

В результате изучения дисциплины студент должен знать основные определения, понятия, алгоритмы, уметь писать многопроцессные и многопоточные приложения в среде операционной системы Linux, корректно организовывать взаимодействие процессов и потоков, как локальных, так и удаленных, работать с файлами и устройствами ввода-вывода.

Успешное освоение курса требует напряжённой работы студента. В программе курса приведено минимально необходимое время для работы студента над темой.

Самостоятельная работа включает в себя:

- чтение и конспектирование рекомендованной литературы;
- проработку учебного материала (по конспектам лекций, учебной и научной литературе), доказательство отдельных утверждений, свойств;
- решение задач, предлагаемых студентам на лекциях.

Руководство и контроль за самостоятельной работой студента осуществляется в форме индивидуальных консультаций.

Показателем владения материалом служит умение решать теоретические и практические задачи. Для формирования умения применять теоретические знания на практике студенту необходимо решать как можно больше практических задач. При решении задач каждое действие необходимо аргументировать, ссылаясь на известные теоретические сведения. Программы должны легко читаться и иметь подробные комментарии.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов, следует обращаться за консультациями к лектору.

## ПРИЛОЖЕНИЕ

### ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

<b>по направлению:</b>	Информатика и вычислительная техника
<b>профиль подготовки:</b>	Программная инженерия передовая инженерная школа радиолокации, радионавигации и программной инженерии кафедра технологий проектирования сложных технических систем
<b>курс:</b>	1
<b>квалификация:</b>	магистр

Семестр, формы промежуточной аттестации: 2 (весенний) - Дифференцированный зачет

#### Разработчики:

А.А. Приходько, канд. физ.-мат. наук  
О.И. Кузьмин

## 1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-3 Способен выбирать и (или) разрабатывать подходы к решению типовых и новых задач в области информатики и вычислительной техники, учитывая особенности и ограничения различных методов решения	ОПК-3.2 Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
ОПК-4 Способен успешно реализовывать решение поставленной задачи, провести анализ результата и представить выводы, применяя знания и навыки в области математики, естественных наук и информационно-коммуникационных технологий	ОПК-4.1 Способен применять знания и навыки по использованию информационно-коммуникационных технологий для поиска и изучения научной литературы, применения прикладных программных продуктов
ПК-2 Понимает и способен применить в научно-исследовательской и прикладной деятельности основные законы естествознания, современный математический аппарат и алгоритмы, современные информационно-коммуникационные технологии	ПК-2.1 Знает основы научно-исследовательской деятельности в области информационных технологий, владеет знанием основ философии и методологии науки; знанием методов научных исследований и навыками их проведения

## 2. Показатели оценивания компетенций

В результате изучения дисциплины «Информационная безопасность» обучающийся должен:

### знать:

- определения основных объектов и понятий из области математических основ криптографии;
- основные алгоритмы и подходы прикладной криптографии;
- ключевые концепции и подходы современных практик информационной безопасности.

### уметь:

- применять знания из области математических основ криптографии для анализа и разработки криптографических алгоритмов;
- применять знания курса для анализа различных решений в области информационной безопасности.

### владеть:

- математическим аппаратом прикладной криптографии;
- концепциями и понятиями современных практик информационной безопасности.

## 3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

- 1 Основные операции над множествами. Бинарные отношения. Перестановки. Логические формулы и предикаты.
- 2 Определение коммутативных групп. Группа перестановок.
- 3 Алгебраические свойства вычетов  $\mathbb{Z}/n\mathbb{Z}$
- 4 Диофантовы уравнения.
- 5 Дискретный логарифм. Надежные датчики случайных чисел.
- 6 Кольца многочленов. Неприводимые многочлены.
- 7 Линейные динамические системы в  $\mathbb{R}^n$  и их спектральные свойства.
- 8 Линейные динамические системы над полями вычетов и полями Галуа. Автоморфизм Фробениуса.
- 9 Конструкция эллиптической кривой над конечными полями.
- 10 Проективные координаты. Эллиптическая арифметика. Теорема Хассе.



- 11 Понятие об алгоритмической сложности. Графы и деревья. Конечные автоматы и автоморфизмы деревьев.
- 12 Криптоанализ – основные подходы. Представление о квантовых вычислениях.
- 13 Понятие о схеме симметричного шифрования. Основные алгоритмы.
- 14 Блочные шифры. Подходы к надежному созданию ключей шифрования.
- 15 Использование схем ключевого обмена в телекоммуникационных системах. Алгоритм Диффи-Хеллмана.
- 16 Алгоритмы ключевого обмена ГОСТ.
- 17 Принципы и подходы к созданию асимметричных схем шифрования и подписи. Алгоритм RSA. Алгоритмы ГОСТ.
- 18 Стандарты представления криптографических сообщений. ASN.1. Дерево объектных идентификаторов OID.
- 19 Сертификаты открытых ключей электронной цифровой подписи. Стандарты ГОСТ.
- 20 Удостоверяющие центры и инфраструктура PKI. Практика внедрения инфраструктуры PKI в Российской Федерации.

#### **4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся**

1. Что такое «информационная безопасность»?
2. В чем состоит методика информационной защиты?
3. Что такое политики безопасности?
4. Какие подходы и методики управления информационной безопасностью вы знаете?
5. Расскажите об организационных структурах и составе стандартизирующих документов.
6. Что такое категоризация? Чем отличаются категории друг от друга? В чем отличия категоризации от классификации информации?
7. Расскажите о методике управления рисками в информационной безопасности.
8. Что такое уязвимости и как оценить потенциальные потери?
9. Какие типы требований информационной безопасности существуют? Перечислить. Охарактеризовать.
10. Какие типы криптографических алгоритмов вы знаете?
11. Что такое симметричные и асимметричные системы шифрования?
12. Что такое цифровая подпись и хэш-функции. Общее и различия?
13. Национальные (государственные) особенности криптографических систем?
14. Перечислить типы средств защиты операционных систем?
15. Объясните принципы защиты прикладного программного обеспечения?
16. Перечислить классы средств сетевой безопасности. Охарактеризовать каждый из классов.
17. Опишите архитектуру IP VPN по всем уровням сетевых взаимодействий?
18. Перечислить протоколы IP VPN по всем уровням сетевых взаимодействий?
19. Расскажите об архитектуре IPSec.
20. Перечислите все протоколы в архитектуре IPSec.
21. Расскажите о протоколах идентификации в архитектуре IPSec.
22. Расскажите о протоколах шифрования в архитектуре IPSec.
23. Расскажите о протоколах генерации и обмена ключей IKE.
24. Что такое инфраструктура открытых ключей (PKI – public key infrastructure)? Опишите архитектуру PKI, основные компоненты.

Билет 1

В чем состоят услуги третьей доверенной стороны при распределении ключей.

Билет 2

Расскажите о типах управления доступом и распределения прав.

Билет 3

Расскажите о безопасности сервисов человеко-машинного интерфейса

Билет 4

Расскажите о специфике поддержки криптографических баз данных.

## Критерии оценивания

Оценка «отлично (10)» выставляется обучающемуся, если показавшему всесторонние, систематизированные, глубокие знания предмета и в ходе беседы он верно и детально ответил на четыре (4) произвольных вопроса из выше приведенного перечня. Детальный ответ предполагает верные ответы на все уточняющие вопросы. Подготовка и защита инициативной курсовой работы является преимуществом.

Оценка «отлично (9)» выставляется обучающемуся, если в ходе беседы он верно, но не исчерпывающее детально ответил на четыре (4) произвольных вопроса из выше приведенного перечня (мог не ответить на некоторые уточняющие вопросы). Подготовка и защита инициативной курсовой работы является преимуществом.

Оценка «отлично (8)» выставляется обучающемуся, если в ходе беседы он верно, но не исчерпывающее детально ответил на четыре (4) произвольных вопроса из выше приведенного перечня (не ответил на уточняющие вопросы).

Оценка «хорошо (7)» выставляется обучающемуся, если в ходе беседы он верно и достаточно детально ответил на три (3) произвольных вопроса из выше приведенного перечня. Детальный ответ предполагает верные ответы на все уточняющие вопросы. Подготовка и защита инициативной курсовой работы является преимуществом.

Оценка «хорошо (6)» выставляется обучающемуся, если в ходе беседы он верно, но не исчерпывающее детально ответил на три (3) произвольных вопроса из выше приведенного перечня (не ответил на некоторые уточняющие вопросы). Подготовка и защита инициативной курсовой работы является преимуществом.

Оценка «хорошо (5)» выставляется обучающемуся, если в ходе беседы он верно и достаточно детально ответил на два (2) произвольных вопроса из выше приведенного перечня. Детальный ответ предполагает верные ответы на все уточняющие вопросы.

Оценка «удовлетворительно (4)» выставляется обучающемуся, если в ходе беседы он верно и достаточно детально ответил на один (1) произвольный вопрос из выше приведенного перечня. Детальный ответ предполагает верные ответы на все уточняющие вопросы. Подготовка и защита инициативной курсовой работы является преимуществом.

Оценка «удовлетворительно (3)» выставляется обучающемуся, если в ходе беседы он верно, но не исчерпывающее детально ответил на один (1) произвольный вопрос из выше приведенного перечня (не ответил на уточняющие вопросы).

Оценка «неудовлетворительно (2)» выставляется обучающемуся, если в ходе беседы он не смог ответить ни на один произвольный вопрос из выше приведенного перечня, но смог ответить на наводящие вопросы и вопросы с «подсказками».

Оценка «неудовлетворительно (1)» выставляется обучающемуся, если в ходе беседы он не смог ответить ни на один произвольный вопрос из выше приведенного перечня, а так же ни на один наводящий вопрос.

## 5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения дифференциального зачета обучающиеся могут пользоваться программой дисциплины, а также собственными конспектами занятий по предмету.

Дифференциальный зачет проводится по итогам текущей активности в ходе занятий, защиты инициативной курсовой работы, и путем организации специального опроса, проводимого в простой устной форме, в виде беседы преподавателя и студента.