

Федеральное государственное бюджетное образовательное учреждение высшего про-
фессионального образования
Московский государственный университет имени М.В. Ломоносова
филиал МГУ в г. Севастополе
факультет компьютерной математики
кафедра вычислительной математики



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Наименование дисциплины:
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Уровень высшего образования:
БАКАЛАВРИАТ**

**Направление подготовки:
01.03.02 «ПРИКЛАДНАЯ МАТЕМАТИКА ИНФОРМАТИКА»**

**Направленность ОПОП
ОБЩИЙ**

**Форма обучения:
ОЧНАЯ**

Рабочая программа рассмотрена
на заседании кафедры вычислительной
математики
протокол
№ 1 от «05» 09 2024.
Заведующий кафедрой
Б.В. Ежов
(подпись)

Рабочая программа одобрена
Методическим советом
Филиала МГУ в г. Севастополе
Протокол № 1 от
«13» 09 2024.
Л.И. Теплова
(подпись)

Севастополь, 2024

Рабочая программа дисциплины разработана в соответствии с самостоятельно установленным образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.03.02 «Прикладная математика и информатика» (Утвержден приказом МГУ от 30 августа 2019 года № 1041 (в редакции приказа МГУ от 11 сентября 2019 года № 1109), приказами об утверждении изменений в ОС МГУ от 10 июня 2021 года № 609, от 21 декабря 2021 года № 1404).

Год (годы) приёма на обучение: 2021

курс – IV

семестр – 8

зачётных единиц – 3

академических часов – 108, в т.ч.:

лекций – 24 часов

самостоятельной работы – 84 часов

Формы промежуточной аттестации:

зачёт в 8 семестре.

1. Место дисциплины (модуля) в структуре ОПОП ВО.

Курс входит в вариативную часть образовательной программы. Дисциплина изучается в VIII семестре.

2. Входные требования для освоения дисциплины (модуля), предварительные условия (если есть).

Для успешного освоения дисциплины «Основы информационной безопасности» студент должен успешно освоить предшествующие дисциплины:

«Архитектура ЭВМ и язык Ассемблера», «Операционные системы» базовой части ОС МГУ;

«Введение в сети ЭВМ», «Сети ЭВМ и безопасность» вариативной части ОС МГУ.

3. Результаты обучения по дисциплине (модулю), соотнесённые с требуемыми компетенциями выпускников.

Планируемые результаты обучения по дисциплине (модулю):

Знать:

место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;

сущность и понятие информации, информационной безопасности и характеристику ее составляющих;

основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;

нормативные правовые акты и нормативные методические документы в областях обеспечения информационной безопасности;

основные подходы к планированию и организации работ и ресурсов для обеспечения информационной безопасности предприятия.

Уметь

применять действующую законодательную базу в области обеспечения информационной безопасности;

составлять и контролировать план выполняемой работы.

Владеть:

профессиональной терминологией в области информационной безопасности;

методами планирования работ и ресурсов для обеспечения информационной безопасности предприятия

4. Формат обучения _____ очный _____

5. Объем дисциплины (модуля) составляет 3 з.е., в том числе 24 академических часов, отведенных на контактную работу обучающихся с преподавателем (аудиторная нагрузка), 84 академических часов на самостоятельную работу обучающихся.

ТЕМАТИЧЕСКИЙ ПЛАН

Наименование разделов и тем дисциплины (модуля), Форма промежуточной аттестации по дисциплине (модулю)	Номинальные трудозатраты обучающегося			Всего академических часов	Формы текущего контроля успеваемости (по темам) / Форма промежуточной аттестации (по семестрам)
	Контактная работа (работа во взаимодействии с преподавателем) Виды контактной работы, академические часы		Самостоятельная работа обучающегося, академические часы СРС		
	Занятия лекционного типа*	Занятия семинарского типа*			
Информационная безопасность в системе национальной безопасности Российской Федерации.	4		18	8	Проверка выполнения задания самостоятельной работы.
Компьютерная система как объект информационной безопасности.	6		20	10	Проверка выполнения задания самостоятельной работы.
Защита информации, обрабатываемой в автоматизированных системах, от технических разведок.	8		20	10	Проверка выполнения задания самостоятельной работы.
Критерии защищённости компьютерных систем.	6		18	10	Проверка выполнения задания самостоятельной работы.
Промежуточная аттестация (зачет)			8	10	Проверка выполнения задания самостоятельной работы.
Всего, часов	24		84	108	
Промежуточная аттестация					Зачет

6.2. Содержание разделов (тем) дисциплины

А.План лекций

№ п/п	Номер занятия	Наименование темы и содержание лекции	Количество часов
1.	1.	<p>Информационная безопасность в системе национальной безопасности Российской Федерации Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание. Роль информационной безопасности (ИБ) в обеспечении национальной безопасности государства. Национальные интересы в информационной сфере. Источники и угрозы безопасности информации. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Государственная система защиты информации в РФ. Организационно-правовое обеспечение ИБ. Основные принципы засекречивания информации. Структура государственной системы информационной безопасности. Основные задачи в области ЗИ федеральных и региональных органов исполнительной власти. Национальные интересы и угрозы ИБ РФ в информационной сфере и их обеспечение. Интересы личности и государства в информационной сфере. Угрозы информационному обеспечению государственной политики РФ, конституционным правам и свободам ее граждан. Угрозы развитию отечественной индустрии информатизации, безопасности информационных и телекоммуникационных средств и систем. Внутренние и внешние источники угроз. Направления обеспечения ИБ государства</p>	2
2.	2.	<p>Компьютерная система как объект информационной безопасности. Компьютерная система как объект информационного воздействия. Основные компоненты автоматизированной системы (АС). Субъекты информационных отношений в АС, их безопасность. Уязвимость структурно-функциональных элементов АС. Угрозы безопасности информации, АС и субъектов информационных отношений. Основные источники угроз. Информационные риски, методы их оценки. Методы и средства обеспечения ИБ компьютерных систем. Каналы несанкционированного получения информации. Неформальная модель нарушителя компьютерных систем. Методы обеспечения ИБ: организационно-правовые, технические,</p>	2

		криптографические. Их характеристика. Криптографические методы защиты информации. Общие сведения о криптографии. Требования к криптосистемам. Криптографические методы защиты информации. Системы с симметричными ключами. Системы с открытыми ключами. Цифровые подписи. Криптографические хэш-функции.	
3.	3.	Защита информации (ЗИ), обрабатываемой в автоматизированных системах, от технических разведок Классификация и возможности технических разведок. Основные принципы разведки. Классификации технических разведок. Технология и методы добывания информации. Показатели эффективности добывания информации. Компьютерная разведка. Цель и общая характеристика компьютерной разведки. Классификация компьютерной разведки. Методы добывания информации из АС. Технические каналы утечки информации (ТКУИ) при эксплуатации АС. Типовая структура и виды ТКУИ. Основные показатели ТКУИ. Общая характеристика акустических, оптических, электрических и радиоэлектронных ТКУИ. Основные механизмы защиты, используемые в системах защиты информации (СЗИ) информационных систем (ИС). Перечень защитных механизмов, используемых в СЗИ ИС. Аутентификация и идентификация пользователей. Разграничение доступа субъектов к ресурсам ИС. Регистрация и оперативное оповещение о событиях безопасности. Защита периметра компьютерной сети.	2
4.	4.	Критерии защищённости компьютерных систем. Методы оценки защищённости компьютерных систем. Анализ существующих методик определения требований к защите информации (в США и России). Критерии и классы защищённости средств вычислительной техники (СВТ) и АС от несанкционированного доступа (НСД)..	2

7. Фонд оценочных средств (ФОС) для оценивания результатов обучения по дисциплине (модулю)

7.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

7.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации.

Вопросы к зачёту по курсу «Основы информационной безопасности» (VIII семестр)

1. Основные понятия информационной безопасности.
2. Информационные технологии и необходимость ИБ.
3. Система защиты информации и ее структуры.
4. Экономическая информация как товар и объект безопасности.
5. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
6. Персональные данные и их защита.
7. Информационные угрозы, их виды и причины возникновения.
8. Информационные угрозы для государства.
9. Информационные угрозы для компаний.
10. Информационные угрозы для личности (физического лица).
11. Действия и события, нарушающие информационную безопасность.
12. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
13. Способы воздействия информационных угроз на объекты.
14. Внешние и внутренние субъекты информационных угроз.
15. Компьютерные преступления и их классификация.
16. Исторические аспекты компьютерных преступлений и современность.
17. Субъекты и причины совершения компьютерных преступлений.
18. Вредоносные программы, их виды.
19. История компьютерных вирусов и современность.
20. Деятельность международных организаций в сфере информационной безопасности.
21. Государственное регулирование информационной безопасности в РФ.
22. Задачи ИБ в Национальной программе «Цифровая экономика Российской Федерации».
23. Доктрина информационной безопасности России.
24. Федеральные законы в сфере информатизации и информационной безопасности в РФ.
25. Уголовно-правовой контроль над компьютерной преступностью в РФ.
26. Политика безопасности и ее принципы.
27. Фрагментарный и системный подход к защите информации.
28. Методы и средства защиты информации.
29. Организационное обеспечение ИБ.
30. Организация конфиденциального делопроизводства.
31. Организационно-экономическое обеспечение ИБ.
32. Инженерно-техническое обеспечение компьютерной безопасности.
33. Организационно-правовой статус службы безопасности.
34. Защита информации в Интернете.
35. Электронная почта и ее защита.
36. Защита от компьютерных вирусов.
37. «Больные» мобильники и их «лечение».
38. Популярные антивирусные программы и их классификация.
39. Этапы и освоение защиты информации экономических объектов. 4
0. Криптографические методы защиты информации.
41. Оценка эффективности инвестиций в информационную безопасность.
42. Российские компании в сфере ИБ.
43. Фирмы, оценивающие работу персонала в компании.
44. Менеджмент и аудит ИБ на уровне предприятия.
45. Аудит ИБ автоматизированных банковских систем.
46. Аудит ИБ электронной коммерции.
47. Информационная безопасность предпринимательской деятельности.

- для зачёта

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)

Оценка РО и соответствующие виды оценочных средств	Незачтено	Зачтено		
		Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Знания (виды оценочных средств: устные и письменные опросы и контрольные работы, тесты, и т.п.)	Отсутстви е знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения (виды оценочных средств: практические контрольные задания, написание и защита рефератов на заданную тему и т.п.)	Отсутстви е умений	В целом успешное, но не систематическо е умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера)	Успешное и систематическое умение
Навыки (владения, опыт деятельности) (виды оценочных средств: выполнение и защита курсовой работы, отчет по практике, отчет по НИР и т.п.)	Отсутстви е навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но используемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач

8. Ресурсное обеспечение:

- Перечень основной и дополнительной литературы (учебники и учебно-методические пособия),

а) основная литература;

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/477968>
2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/473348>.
3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/469235>.

6) Описание материально-технического обеспечения.

- В материально-техническое обеспечение дисциплины входят аудитории, в том числе компьютерные классы, библиотечные фонды Филиала МГУ им. М.В. Ломоносова в г. Севастополе и наличие в библиотеке и в Интернете необходимых учебников, сборников упражнений, словарей и научной литературы, а также доступ к ресурсам сети Интернет.

9. Соответствие результатов обучения по данному элементу ОПОП результатам освоения ОПОП указано в общей характеристике ОПОП.

10. Язык преподавания. Русский

11. Преподаватель.

Гришин Игорь Юрьевич, доктор технических наук, профессор, профессор кафедры вычислительной математики.

12. Автор программы.

Гришин Игорь Юрьевич, доктор технических наук, профессор, профессор кафедры вычислительной математики.