Федеральное государственное бюджетное образовательное
учреждение высшего образования
Московский государственный университет имени М.В.Ломоносова
Филиал Московского государственного университета имени М.В.Ломоносова
в городе Сарове

УТВЕРЖДАЮ

Директор филиала МГУ в городе Сарове

_____ /В.В. Восводин/

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины:

«Основы информационной безопасности»

Уровень высшего образования:

магистратура

Направление подготовки / специальность:

02.04.02 "Фундаментальная информатика и информационные технологии" (3++)

Направленность (профиль)/специализация ОПОП:

Суперкомпьютерные технологии и фундаментальная информатика

Форма обучения:

очная

Саров 2022

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 02.04.02 "Фундаментальная информатика и информационные технологии" программы магистратуры - приказ МГУ 30 августа 2019 года № 1054 (в редакции приказа МГУ от 11 сентября 2019 года № 1109)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Основы информационной безопасности

Fundamentals of information security

2. УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ

Подготовка научно-педагогических кадров в магистратуре.

3. НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ

Направление 02.04.02 «Фундаментальная информатика и информационные технологии». Направленность (профиль) «Прикладная математика и информатика». Образовательная программа «Суперкомпьютерные технологии и фундаментальная информатика».

4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в вариативную часть магистерской образовательной программы «Суперкомпьютерные технологии математического моделирования и обработки данных», изучается во 3-м семестре.

5. АННОТАЦИЯ

В курсе изучаются основы информационной безопасности. Излагаются взгляды на информацию, как объект защиты с выделением характерных свойств защищаемой информации. Рассматриваются виды угроз информационной безопасности; методы и средства борьбы с угрозами информационной безопасности; понятие политики безопасности, существующие типы политик безопасности; действующие стандарты информационной безопасности.

The course examines the basics of information security. Views on information as an object of protection are presented, highlighting the characteristic properties of the protected information. The types of threats to information security are considered; methods and means of combating threats to information security; the concept of security policy, existing types of security policies; current information security standards.

6. ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенцийобразовательной программы:

Формируемые компетенции	Планируемые результаты обучения
УК-3. Способен разрабатывать, реализовывать и управлять проектом на всех этапах его жизненного цикла, предусматривать и учитывать проблемные ситуации и риски проекта.	**Знать** организационные структуры проектной деятельности; методы анализа информации. **Уметь:** работать с нормативно-правовыми и научными источниками информации. **Владеть:** системой понятий, характеризующих отличия в системах научных гипотез и научных методов; навыками и готовностью к самостоятельному выполнению заданий.
ОПК-1. Способен находить, формулировать и решать актуальные проблемы в области прикладной математики, фундаментальной информатики и информационно-коммуникационных технологий.	**Знать:** Актуальные проблемы современной прикладной математики и информатики; **Уметь:** анализировать источники информации для поиска новых актуальных проблем и способов их решения; **Владеть:** навыками применения передовых технологий для решения задач прикладной математики и информатики.
ОПК-4. Способен разрабатывать, комбинировать и адаптировать современные информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	**Знать:** информационно-коммуникационные технологии для решения задач в области профессиональной деятельности; требования информационной безопасности при решении задач, связанных с реализацией профессиональной деятельности. **Уметь:** Разрабатывать информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. **Владеть:** способность обеспечивать информационную безопасность при решении задач, связанных с реализацией профессиональной деятельности.
ПК-2. Способен в рамках задачи, поставленной специалистом более высокой квалификации, проводить научные исследования и (или) осуществлять разработки в области информатики и информационно-коммуникационных технологий с получением науч-	**Знать:** Принципы выбора математических моделей реальных явлений и процессов; типовые методы и алгоритмы исследования моделей реальных явлений и процессов. **Уметь:** создавать алгоритмические и математические модели типовых прикладных задач; проводить формализацию задачи, строить описательные и прогнозные модели с помощью совре-

ного и (или) научно-практического результата.	менных программных аналитических средств, оценивать и интерпретировать полученные результаты. **Владеть:** опыт проведения научных исследований в области информатики и информационно-коммуникационных технологий с получением научного или научно-практического результата.
МПК-1 Способность понимать и применять в исследовательской и прикладной деятельности современные суперкомпьютерные технологии, математический аппарат, вычислительные методы для проведения крупномасштабного математического моделирования и обработки данных на современных высокопроизводительных вычислительных системах.	**Знать:** компьютерные технологии, математический аппарат, вычислительные методы для проведения крупномасштабного математического моделирования и обработки данных на современных высокопроизводительных вычислительных системах. **Уметь:** применять в исследовательской и прикладной деятельности современные компьютерные технологии, математический аппарат, вычислительные методы для проведения крупномасштабного математического моделирования и обработки данных на современных высокопроизводительных вычислительных системах; **Владеть:** навыками разработки программ для проведения крупномасштабного математического моделирования и обработки данных на современных высокопроизводительных вычислительных системах.

Оценочные средства для промежуточной аттестации приведены в Приложении.

7. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетные единицы, всего 108 часов.

36 часов составляет контактная работа с преподавателем – 36 часов занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 0 часов групповых консультаций, 0 часов мероприятий текущего контроля успеваемости, 2 часа промежуточной аттестации.

72 чacf составляет самостоятельная работа учащегося.

8. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть базовыми знаниями по операционным системам и компьютерным сетям соответствующим основным образовательным программам бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

9. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения используются мультимедийные технологии, включая демонстрацию презентаций. Используются компьютеры с операционной системой Linux Debian (Ububtu, Kali Linux) и стандартным ПО (включая редакторы текстов), выходом в интернет. Также используется электронная информационная образовательная среда https://academtest.ruдля проверки знаний студентов.

10. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	**Всего (часы)**	В том числе								
		Контактная работа (работа во взаимодействии с преподавателем), часы из них						**Самостоятельная работа учащегося, часы** из них		
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости: коллоквиумы, практические контрольные занятия и др.	**Всего**	Выполнение домашних заданий	Подготовка рефератов и т.п..	**Всего**
Основы информационной безопасности										
Тема 1. Теоретические основы безопасности в автоматизированных системах и вычислительных сетях»	**2**	2	0	-	-	-	**4**	8	-	**8**
Тема 2. Технологии идентификации и протоколы аутентификации при обеспечения безопасности информации, обрабатываемой в	**14**	14	0	-	-	-	**8**	16	-	**16**

автоматизированных системах и сетях»										
Тема 3. Основные технологии используемые для обеспечения конфиденциальности и целостности информации, обрабатываемой в автоматизированных системах	**10**	10	0	-	-	-	**8**	16	-	**16**
Тема 4. Обеспечение информационной безопасности обрабатываемой в автоматизированных системах и вычислительных сетях	**10**	10	0	-	-	-	**16**	32	-	**32**
Итого	**72**						**36**	**72**		

11.УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к практическим заданиям текущего контроля и промежуточной аттестации.

12.РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная учебно-методическая литература:

1. Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс] : Учеб. пособие / А.В. Душкин [и др.]. - М. : Горячая линия-Телеком, 2018. - 248 с. - URL: https://e.lanbook.com/book/111053 (дата обращения: 01.09.2019)
2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учеб. пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с. - Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 978-5-9912-0147-6.

3. Шаньгин В.Ф. Информационнаябезопасность и защита информации [Текст] : [учеб. пособие] / В. Ф. Шаньгин. - М. : ДМК Пресс, 2014. - 702 с. - Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 978-5-94074-768-0. 004.056(075.8) - Ш-228
4. Гайдамакин, Николай Александрович. Учебно-методический комплекс дисциплины "Информационная безопасность АИС, баз и банков данных" [Электронный ресурс] / Н. А. Гайдамакин ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.].

Ресурсы сети “ИНТЕРНЕТ”

1. ЭБС издательства Лань –http://e.lanbook.com/.
2. Научная электронная библиотека eLIBRARY.RU–http://elibrary.ru/.
3. Библиографическая и реферативная база данных научной периодики «Scopus» - www.scopus.com.
4. Сайт Федеральной службы безопасности России (ФСБ России). -http://www.fsb.ru.
5. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). - http://www.fstec.ru.
6. Портал технического комитета по стандартизации «Защита информации». –http://tk.gost.ru/wps/portal/tk362
7. Информационно-аналитический Интернет-портал ISO27000.ru.– http://www.iso27000.ru

Материально-техническая база: для преподавания дисциплины аудитория, оборудованная проектором.

13. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

14. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

с.н.с. Центра проблем информационной безопасности ВМК МГУ им. М.В.Ломоносова, к.т.н.Пилюгин П.Л..

Приложение

Оценочные средства для промежуточной аттестации по дисциплине «Введение в информационную безопасность»

Средства для оценивания планируемых результатов обучения, критерии и показатели оценивания приведены ниже.

РЕЗУЛЬТАТ ОБУЧЕНИЯ	**КРИТЕРИИ и ПОКАЗАТЕЛИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ из соответствующих карт компетенций**				
	1	2	3	4	5
	Неудовлетворительно	**Неудовлетворительно**	**Удовлетворительно**	**Хорошо**	**Отлично**
З1 (МПК-1) Знать: основные принципы, методы и технологии идентификации и аутентификации; основные политики систем управления доступом, их свойства и критерии безопасности;	Отсутствие знаний	Фрагментарные представления об основных принципах, методах и технологиях идентификации и аутентификации; основных политиках систем управления доступом, их свойствах и критериях безопасности;	В целом сформированные, но неполные знания об основных принципах, методах и технологиях идентификации и аутентификации; основных политиках систем управления доступом, их свойствах и критериях безопасности;	Сформированные, но содержащие отдельные пробелы знания об основных принципах, методах и технологиях идентификации и аутентификации; основных политиках систем управления доступом, их свойствах и критериях безопасности;	Сформированные систематические знания об основных принципах, методах и технологиях идентификации и аутентификации; основных политиках систем управления доступом, их свойствах и критериях безопасности;
У1 (МПК-1) Уметь: анализировать и оценивать угрозы информационной безопасности автоматизированных систем при использовании различных протоколов аутентификации и различных политик разграничения доступа.	Отсутствие умений	Фрагментарные умения анализа и оценки угрозы информационной безопасности автоматизированных систем при использовании различных протоколов аутентификации и различных политик разграничения доступа.	В целом сформированное, но не систематическое умение анализа и оценки угрозы информационной безопасности автоматизированных систем при использовании различных протоколов аутентификации и различных политик разграничения доступа.	Сформированное, но содержащее отдельные пробелы умение анализа и оценки угрозы информационной безопасности автоматизированных систем при использовании различных протоколов аутентификации и различных политик разграничения доступа.	Сформированное систематическое умение анализа и оценки угрозы информационной безопасности автоматизированных систем при использовании различных протоколов аутентификации и различных политик разграничения доступа.

В1 (МПК-1) Владеть: навыками определения угроз несанкционированного доступа к информации и возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Отсутствие навыков	Фрагментарное владение навыками навыками определения угроз несанкционированного доступа к информации и возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	В целом сформированное, но не систематическое владение навыками навыками определения угроз несанкционированного доступа к информации и возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Сформированное, но содержащее отдельные пробелы владение навыками навыками определения угроз несанкционированного доступа к информации и возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Сформированное систематическое владение навыками навыками определения угроз несанкционированного доступа к информации и возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
З2 (МПК-2) Знать: технологии и основные методы управления доступом к информации применяемые на практике; основы администрирования систем обеспечения информационной безопасности вычислительных систем; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы; принципы и технологии обеспечения информацион-	Отсутствие знаний	Фрагментарные представления о технологиях и основных методах управления доступом к информации применяемые на практике; основ администрирования систем обеспечения информационной безопасности вычислительных систем; принципах и методах противодействия несанкционированному информационному воздействию на вычислительные системы; принципах и технологиях обеспечения ин-	В целом сформированные, но неполные знания о технологиях и основных методах управления доступом к информации применяемые на практике; основ администрирования систем обеспечения информационной безопасности вычислительных систем; принципах и методах противодействия несанкционированному информационному воздействию на вычислительные системы; принципах и техноло-	Сформированные, но содержащие отдельные пробелы знания о технологиях и основных методах управления доступом к информации применяемые на практике; основ администрирования систем обеспечения информационной безопасности вычислительных систем; принципах и методах противодействия несанкционированному информационному воздействию на вычислительные системы; принципах и техноло-	Сформированные систематические знания о технологиях и основных методах управления доступом к информации применяемые на практике; основ администрирования систем обеспечения информационной безопасности вычислительных систем; принципах и методах противодействия несанкционированному информационному воздействию на вычислительные системы; принципах и техноло-

ной безопасности компьютерных сетей;		формационной безопасности компьютерных сетей;	гиях обеспечения информационной безопасности компьютерных сетей;	гиях обеспечения информационной безопасности компьютерных сетей;	гиях обеспечения информационной безопасности компьютерных сетей;
У2 (МПК-2) Уметь: обосновывать требования к системе защиты автоматизированной системы от несанкционированного доступа к информации.	Отсутствие умений	Фрагментарные умения в обосновании требований к системе защиты автоматизированной системы от несанкционированного доступа к информации	В целом сформированное, но не систематическое умение в обосновании требований к системе защиты автоматизированной системы от несанкционированного доступа к информации	Сформированное, но содержащее отдельные пробелы умение в обосновании требований к системе защиты автоматизированной системы от несанкционированного доступа к информации	Сформированное систематическое умение в обосновании требований к системе защиты автоматизированной системы от несанкционированного доступа к информации
В2 (МПК-2) Владеть: навыками использования средств анализа структуры и уязвимостей автоматизированных систем и компьютерных сетей.	Отсутствие навыков	Фрагментарное владение навыками навыками использования средств анализа структуры и уязвимостей автоматизированных систем и компьютерных сетей.	В целом сформированное, но не систематическое владение навыками навыками использования средств анализа структуры и уязвимостей автоматизированных систем и компьютерных сетей.	Сформированное, но содержащее отдельные пробелы владение навыками навыками использования средств анализа структуры и уязвимостей автоматизированных систем и компьютерных сетей.	Сформированное систематическое владение навыками навыками использования средств анализа структуры и уязвимостей автоматизированных систем и компьютерных сетей.

Фонды оценочных средств

Фонды оценочных средств представлены набором тестов по отдельным лекциям, используемыми для текущего контроля, и итоговым тестом по всем модулям курса в системе электронной информационной образовательной среды https://academtest.ru. Для прохождения тестирования необходимо зарегистрироваться в https://www.academtest.ru/ регистрация производится по коду для группы «ИБ-Филиал_МГУ_Саров» .

Примерный перечень вопросов для зачета/теста:

1. Параметры FTE, FTA, FRR, FAR для биометрических методов.
2. Методы взлома парольной защиты. 9-ть методов модификации схемы «простой пароль».
3. Строгая Аутентификация на основе секрета. Одно- и двух- сторонняя аутентификация.
4. ISO symmetric key two-pass unilateral authentication protocol
5. ISO symmetric key three-pass mutual authentication
6. Распределение ключей симметричными алгоритмами. Одно- и двух- сторонняя аутентификация.
7. «Бесключевой» протокол Шамира
8. Протокол Wide-Mouth Frog
9. Аутентификация на основе симметричной криптографии. Протокол Нидхема-Шредера (ассиметричный и двухсторонний).
10. Аутентификация на основе симметричной криптографии. Протокол Нидхема-Шредера (ассиметричный и трехсторонний)
11. Аутентификация на основе симметричной криптографии. Атака на протокол Нидхема-Шредера.
12. Аутентификация на основе симметричной криптографии. Протокол Нидхема-Шредера при наличии нескольких серверов аутентификации и их отсутствии (отсутствии третьей стороны).
13. Модификация парольной аутентификации на основе асимметричной криптографии.
14. Модификация парольной аутентификации на основе основе ЭЦП
15. АутентификациянабазеЭЦП. ISO1 (public key unilateral authentication protocol)
16. АутентификациянабазеЭЦП. IS02 (public key two-pass mutual authentication protocol).

17. АутентификациянабазеЭЦП. IS03 (three-pass mutual authentication protocol)..
18. Аутентификация на основе асимметричной криптографии. Протокол Нидхема-Шредера.
19. Аутентификация на основе асимметричной криптографии. Атака на протокол Нидхема-Шредера.
20. Аутентификация на основе хеш-функций. PBKDF2/Аутентификация с использованием ключевых хэш-функций
21. Аутентификация с нулевой передачей знаний.
22. Субъектно-объектная модель компьютерной системы. Монитор безопасности в субъетно-объектной модели КС
23. Модель Харрисона-Руззо-Ульмана (модель HRU)
24. Критерий безопасности и основная теорема модели HRU
25. Теоретико-графовая модель «take-grant». Основные положения и отличия от модели HRU.
26. Распространение прав в модели «take-grant».
27. Утечка прав в модели «take-grant». Критерий безопасности и основная теорема модели «take-grant»
28. Расширенная модель take-grant»
29. Модель Деннинг. Решётка уровней и функции безопасности.
30. Модель Белла-ЛаПадулы
31. Модификации модели Белла-ЛаПадулы.
32. Тематические политики доступа.
33. Модели ролевого доступа.
34. Модели индивидуально группового доступа
35. Понятие целостности данных. Мандатная модель целостности Биба.
36. MAC, HMAC, ЭЦП в проверке целостности.
37. Методы обеспечения целостности.
38. Понятие скрытых каналов утечки информации в моделях разграничения доступа.
39. Виды скрытых каналов утечки информации
40. Методы изоляции.

41. Виртуализация. Проблемы безопасности.
42. Пассивные сетвые атаки
43. Метод немого хоста
44. Активные сетевые атаки
45. Десинхрогизация TCP соединения
46. Ранняя десинхрогизация TCP соединения
47. Идентификация и аутентификация в сети. WiFi
48. Идентификация и аутентификация в сети. GSM
49. Идентификация и аутентификация в сети. GPRS/LTE
50. Идентификация и аутентификация в сети. Kerberos
51. Управление доступом в распределенных системах
52. Межсетевые экраны и DMZ
53. DLP системы
54. События безопасности и инциденты, IDS/IPS
55. События безопасности и инциденты, SIEM
56. VPN
57. Защищенные протоколы PPTP
58. Защищенные протоколы IPSEC
59. Защищенные протоколы TLS
60. Анонимность в интернет, цепочки прокси

Методические материалы для проведения процедур оценивания результатов обучения

Для контроля знаний студентов по данной дисциплине необходимо проводить текущий и итоговый контроль. Текущий контроль выполняется в виде защит практических и индивидуальных работ, проверки домашних заданий. Итоговый контроль проводится в виде теста,

на котором обсуждаются теоретические вопросы курса. Случайным образом выбираются 30 вопросов из 172. Оценивание знаний, умений и навыков производится на основе балльно-рейтинговой системы. При рейтинговой системе все знания, умения и навыки, приобретаемые студентами в результате изучения дисциплины, оцениваются в баллах. Предполагается несколько форм контроля, по которым студенты получают баллы:

1. Посещаемость лекций (макс. 20 баллов).
2. Выполнение домашних заданий к каждой лекции (макс. 60 баллов).
3. Зачет (макс. 20 баллов).

Итоговая оценка за курс рассчитывается исходя из набранных студентом баллов (от 0 до 100 баллов). Критерии оценок:

- «незачет» меньше 50 баллов;
- «зачет» больше или равно 50 баллов