Федеральное государственное бюджетное образовательное

учреждение высшего образования

Московский государственный университет имени М.В. Ломоносова

Факультет вычислительной математики и кибернетики

**УТВЕРЖДАЮ**

декан факультета вычислительной математики и кибернетики

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/И.А. Соколов /**

**«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Наименование дисциплины:**

**Теоретические основы информационной безопасности**

**Уровень высшего образования:**

**бакалавриат**

**Направление подготовки / специальность:**

**01.03.02 «Прикладная математика и информатика» (3++)**

**Направленность (профиль):**

**Математические методы обработки информации и принятия решений**

**Форма обучения:**

**очная**

**Москва 2023**

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 01.03.02, 01.04.02 "Прикладная математика и информатика" программы бакалавриата Утвержден приказом МГУ от 30 августа 2019 года № 1041 (в редакции приказов МГУ от 11 сентября 2019 года № 1109, от 10 июня 2021 года № 609, от 7 октября 2021 года № 1048, от 21 декабря 2021 года № 1404, от 2 ноября 2022 года № 1299)

**1.** Дисциплина относится к *вариативной* части ОПОП ВО.

**2.** Входные требования для освоения дисциплины (модуля): учащиеся должны владеть знаниями по дискретной математике, алгебре, теории вероятностей и математической статистике, алгоритмам и алгоритмическим языкам, архитектуре ЭВМ и языку ассемблера, операционным системам и системам программирования в объеме, соответствующем программе первого и второго года обучения основных образовательных программ бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

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

Компетенции выпускников, частично формируемые при реализации дисциплины (модуля):

* **ОПК-2.Б** Способность применять и модифицировать математические модели, а также интерпретировать полученные математические результаты при решения задач в области профессиональной деятельности
* **ОПК-3.Б** Способность решать задачи в области прикладной математики и информатики с использованием современных информационных технологий, учитывая основные требования информационной безопасности
* **ПК-2.Б** Способность понимать и применять в научно-исследовательской деятельности современный математический аппарат

Планируемые результаты обучения по дисциплине (модулю):

**Знать:**

1. основные понятия, определения и факты теории защиты компьютерных систем.

**Уметь:**

1. применять на практике основные методы теории защиты информации в компьютерных системах.

**Владеть:**

1. навыками решения практических задач теории компьютерной безопасности;
2. методами использования теории построения политик безопасности компьютерных систем (ПК-1);
3. навыками проведения анализа угроз и поиска уязвимостей в компьютерных системах.

**4.** Формат обучения: занятия проводятся с использованием меловой или маркерной доски, интерактивные материалы демонстрируются с помощью ноутбука и проектора.

**5.** Объем дисциплины (модуля) составляет 2 з.е., в том числе 36 академических часа, отведенных на контактную работу обучающихся с преподавателем, 36 академических часов на самостоятельную работу обучающихся.

**6.** Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий.

|  |  |  |
| --- | --- | --- |
| **Наименование и краткое содержание разделов и тем дисциплины (модуля),****Форма промежуточной аттестации по дисциплине (модулю)** | **Всего****(часы**) | В том числе |
| **Контактная работа (работа во взаимодействии с преподавателем)****Виды контактной работы, часы** | **Самостоятельная работа обучающегося,** **часы**  |
| Занятия лекционного типа\* | Занятия семинарского типа\* | **Всего** |  |
| 1. Основные понятия информационной безопасности, атаки на компьютерные системы.
 | **12** | 8 | 0 | **8** | **4** |
| 1. Сети и сетевые атаки.
 | **8** | 6 | 0 | **6** | **2** |
| 1. Парадигма ограничения доступа в компьютерной безопасности.
 | **6** | 4 | 0 | **4** | **2** |
| 1. Дискреционная политика безопасности.
 | **8** | 6 | 0 | **6** | **2** |
| 1. Управление информационными потоками в информационных системах. Многоуровневая политика безопасности.
 | **8** | 6 | 0 | **6** | **2** |
| 1. Текущий контроль успеваемости: реферат
 | **8** | 0 | 0 | **0** | **8** |
| 1. Модель невлияния.
 | **4** | 2 | 0 | **2** | **2** |
| 1. Компьютерный аудит и системы обнаружения вторжений.
 | **6** | 4 | 0 | **4** | **2** |
| Промежуточная аттестация: устный экзамен | **12** | 0 | 0 | **0** | **12** |
| **Итого** | **72** | **36** | **0** | **36** | **36** |

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.

**Примерные темы реферата**.

1. Понятие переполнения буфера и атаки на основе переполнения буфера.
2. Штатные механизмы защиты информации в локальных сетях.
3. Защита баз данных.

**Вопросы к экзамену**.

1. Активы, ущерб, угрозы, риски, уязвимости, нарушитель, атака, оценка возможностей противника.
2. Иерархическая декомпозиция компьютеров, сетевого взаимодействия. Модель ВОС.
3. Атаки на электронные компоненты компьютеров, механизмы защиты. Уязвимости и механизмы защиты в микропроцессорах.
4. Атаки на операционные системы (ОС), механизмы защиты ОС. Вредоносный код (ВК), руткит-технологии. Механизмы поиска ВК, механизмы ограничения функционирования ВК в ОС.
5. Вирусы и сетевые черви. Распространение ВК через социальные сети. Ботнеты и DDoS атаки.
6. Сети физические и логические, синхронные и асинхронные каналы, модуляция, клиент-серверная архитектура, сетевая ОС.
7. Маршрутизация, коммутация, мультиплексирование. Маршрутизаторы.
8. Ethernet, CSMA/CD, Aloha. Коммутируемые сети Ethernet, мосты, коммутаторы, отказ от разделяемой среды.
9. Субъектно-объектная модель компьютерной системы. Парадигма ограничений доступа. Аксиома безопасности через контроль доступа.
10. Основные идеи формирования политики безопасности (ПБ) с использованием ограничений доступа. Условия, при которых ПБ можно четко определить.
11. Дискреционная ПБ, нестойкость к атакам с помощью троянского коня. Ролевая ПБ.
12. Условия защиты от распространения прав. Модель «take-grant».
13. Модель информационного потока. Доказательство того, что read и write формируют информационные потоки. Скрытые каналы.
14. Многоуровневая ПБ, решетки, функции классификаций и мандатный контроль доступа. Устойчивость к атакам с помощью троянского коня.
15. Модель Белла-Лападула с постоянными грифами объектов. BST теорема. Модель “low-water-mark” с постоянным уровнем допуска.
16. Модель невлияния. Теоремы о невлиянии. Слабости автоматного подхода к модели невлияния.
17. Компьютерный аудит. Деревья атак. Системы обнаружения вторжений.

**Экзаменационный билет** состоит из двух вопросов, например

1. Субъектно-объектная модель компьютерной системы. Парадигма ограничений доступа. Аксиома безопасности через контроль доступа.
2. Модель невлияния. Теоремы о невлиянии.

|  |
| --- |
| **ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)**  |
| ОценкаРО исоответствующие виды оценочных средств  | 2 | 3 | 4 | 5 |
| **Знания***Экзамен* | Отсутствие знаний | Фрагментарные знания | Общие, но не структурированные знания | Сформированные систематические знания |
| **Умения***написание и защита рефератов на заданную тему*  | Отсутствие умений | В целом успешное, но не систематическое умение | В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера) | Успешное и систематическое умение |
| **Навыки (владения, опыт деятельности)***Экзамен* | Отсутствие 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 |

|  |
| --- |
| **Соответствие результатов обучения и компетенций, в развитии которых участвует дисциплина (модуль)** |
| Результаты обучения | Компетенция, с частичным формированием которой связано достижение результата обучения |
| **Знать:**1. основные классы уязвимостей компьютерных систем и сетей;
2. общую теорию и методы решения задач обеспечения информационной безопасности;
3. математические модели информационной безопасности.

**Уметь:** 1. применять на практике общую теорию и методы обеспечения информационной безопасности компьютерных систем и сетей;
2. формировать политику безопасности в реальных компьютерных системах и сетях.

**Владеть:** 1. навыками синтеза информационной безопасности компьютерных систем и сетей;
 | ОПК-2.БОПК-3.Б |
| **Владеть:** 1. навыками использования методов обеспечения информационной безопасности в реальных компьютерных системах и сетях;
 | ПК-2.Б |

8. Ресурсное обеспечение:

Основная литература:

1. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. Учебное пособие. М.: Академия, 2009.
2. Олифер В.Г., Олифер Н.А. Основы компьютерных сетей. Учебное пособие. СПб.: Питер, 2009.
3. Расторгуев С.П. Основы информационной безопасности. Учебное пособие. М.: Академия, 2007.

Дополнительная литература:

1. J. Pieprzyk, T. Hardjono, J. Seberry. Fundamentals of Computer Security. Berlin Heidelberg New York: Springer-Verlag, 2003.

Информационные справочные системы: <https://www.anti-malware.ru/>

Материально-техническое обеспечение: аудитория с партами, меловой или маркерной доской.

9. Язык преподавания: русский.

10. Преподаватели: профессор факультета ВМК МГУ, д.ф.-м.н., проф. А.А. Грушо,

 доцент факультета ВМК МГУ, д.т.н., проф. Е.Е. Тимонина.

11. Авторы программы: профессора факультета ВМК МГУ А.А. Грушо, Е.Е. Тимонина,