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 /
«27» сентября 2022г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Теоретические основы информационной безопасности

Уровень высшего образования:

бакалавриат

Направление подготовки / специальность:

01.03.02 "Прикладная математика и информатика" (3++)

Направленность (профиль) ОПОП:

Искусственный интеллект и анализ данных

Форма обучения:

очная

Рассмотрен и утвержден

на заседании Ученого совета факультета ВМК

(протокол №7, от 27 сентября 2022 года)

Москва 2022

1. ФОРМЫ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

В процессе и по завершении изучения дисциплины оценивается формирование у студентов следующих компетенций:

Планируемые результаты обучения по дисциплине (модулю)		
Содержание и код компетенции.	**Индикатор (показатель) достижения компетенции**	**Планируемые результаты обучения по дисциплине, сопряженные с индикаторами достижения компетенций**
ОПК-1. Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.1 – Обладает фундаментальными знаниями, полученными в области математических и (или) естественных наук ОПК-1.2 – Умеет использовать их в профессиональной деятельности ОПК-1.3 – Имеет навыки выбора методов решения задач профессиональной деятельности на основе теоретических знаний	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; 3. навыками проведения анализа угроз и поиска уязвимостей в компьютерных системах.

1.1. Текущий контроль успеваемости

Текущий контроль успеваемости осуществляется путем оценки результатов выполнения заданий практических (семинарских) занятий, самостоятельной работы, предусмотренных учебным планом и посещения занятий/активность на занятиях.

В качестве оценочных средств текущего контроля успеваемости предусмотрены:

реферат

Примерные темы рефератов.

1. Понятие переполнения буфера и атаки на основе переполнения буфера.
2. Штатные механизмы защиты информации в локальных сетях.
3. Защита баз данных.
4. Строгие протоколы аутентификации.
5. Протокол Нидхема-Шредера для симметричной и асимметричной криптографии.
6. Протоколы на основе ключевых хеш-функций.

7. Использование цифровой подписи.
8. Матрица доступа, пятимерное пространства безопасности Хартсона, модели HRU и Take-Grant
9. MLS модель «военной безопасности», модель Белла-ЛаПадулы, решетки безопасности Деннинг. Модель Биба.
10. Тематические классификаторы и решетки мультирубрик.
11. Использование функциональной структуры организации для управления доступом, индивидуально групповая модель управления доступом.

1.2. Промежуточная аттестация

Промежуточная аттестация осуществляется в форме зачета
В качестве средств, используемых на промежуточной аттестации предусматривается:
Билеты

1.3. Типовые задания для проведения промежуточной аттестации

Вопросы к зачету

1. Активы, ущерб, угрозы, риски, уязвимости, нарушитель, атака, оценка возможностей противника.
2. Иерархическая декомпозиция компьютеров, сетевого взаимодействия. Модель BOC.
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.

2. КРИТЕРИИ ОЦЕНКИ ПО ДИСЦИПЛИНЕ

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине				
Оценка виды оценочных средств	**2 (не зачтено)**	**3 (зачтено)**	**4 (зачтено)**	**5 (зачтено)**
Знания **(виды оценочных средств: приведены в п. 1.2.)**	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения **(виды оценочных средств: приведены в п. 1.2.)**	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)** **(виды оценочных средств: приведены в п. 1.2..)**	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