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 2023г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Информационная безопасность

Уровень высшего образования:

бакалавриат

Направление подготовки / специальность:

02.03.02 "Фундаментальная информатика и информационные технологии" (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 2023 года)

Москва 2023

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-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-6.1. Знает принципы работы современных информационных технологий ОПК-6.2. Использует современные информационные технологии для решения задач профессиональной деятельности	Знать: угрозы безопасности информации в автоматизированных системах и вычислительных сетях; основные принципы, методы и технологии идентификации и аутентификации; основные политики систем управления доступом, их свойства и критерии безопасности; технологии и основные методы управления доступом к информации применяемые на практике; технологии регистрации и учета; технологии обеспечения и проверки целостности информации; технологии защиты информации и программного обеспечения от вредоносных программ; основы администрирования вычислительных систем; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы; технологии межсетевого экранирования и обнаружения вторжений; принципы организации информационных систем в соответствии с требованиями по защите информации. Уметь анализировать и оценивать угрозы информационной безопасности автоматизированных систем;

		осуществлять выбор функциональной структуры системы обеспечения безопасности информации, обрабатываемой в автоматизированных системах; обосновывать выбор технологий для обеспечения безопасности информации, обрабатываемой в автоматизированных системах; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. Владеть навыками использования методов и средств выявления угроз безопасности информации в автоматизированных системах; применения методов противодействия угрозам ИБ; разработки моделей угроз безопасности информации в автоматизированных системах; установки и настройки программных и программно-аппаратных средств защиты информации от несанкционированного доступа в операционных системах общего пользования; использования методик анализа сетевого трафика для исследования сети и обнаружения признаков сетевых атак; анализа функционирования сетевых средств безопасности.

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:

контрольная работа

Вариант контрольной работы №1

1. Дать определение следующим терминам:
    a. Безопасность информации
    b. Конфиденциальность
    c. Целостность
    d. Доступность
    e. Угроза
    f. Атака
    g. Объект
    h. Субъект
    i. Пользователь
    j. Граф доступов
    k. Политика безопасности
2. Описать принцип атаки «Троянским конем» в дискреционной политике безопасности.
3. Вычислить величину потока информации от X к Z для следующего оператора:
   if ((X==1)& (Y==1)) the Z=1;
   здесь X, Y, Z – биты, равномерно распределенные на множестве {0,1}.

Вариант контрольной работы №2

Задача 1. Для команды $(q_{i_0}, a_{i_0}) \rightarrow (q_{i_1}, a_{i_1}, 1)$ машины Тьюринга выписать команды модели ХРУ, которые ее представляют.

Задача 2. Постройте граф создания для систем МТМД.

command a1(x:α , y:β , z: β)
  «создать» субъект x с типом α
end;

command a2(x: α,y:γ, z: β, s: γ, o:δ)
  «создать» объект y с типом γ;
  «создать» субъект s с типом δ;
end;
command a3(x:ε, y: δ, z: β, s: γ ,o: δ)
  «создать» субъект o с типом δ;
  «создать» объект x с типом ε;
end;

Задача 3. Модель Take-Grant. Описание и основные теоремы.

1.2. Промежуточная аттестация

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

1.3. Типовые задания для проведения промежуточной аттестации

Вопросы к экзамену

1. Основные уязвимости информационных систем. Проблема защиты компьютерных систем. Основные понятия и определения компьютер-ной безопасности.
2. Угрозы безопасности. Модель нарушителя информационной без-опасности.
3. Понятие защищенности (безопасности) компьютерной информации. Конфиденциальность, целостность и доступность информации.
4. Субъектно-объектная модель компьютерной системы. Понятие пото-ка, доступа и правил разграничения доступа. Основные типы политик разграничения доступа.
5. Монитор безопасности КС и гарантирование выполнение политики безопасности.
6. Изолированная программная среда.
7. Дискреционные модели безопасности компьютерных систем. Пяти-мерное пространство Хартсона
8. Модели безопасности на основе матрицы доступа. Способы органи-зации матрицы доступа и управления доступом в компьютерных си-стемах
9. Дискреционные модели распространения прав доступа. Модель и теоремы безопасности Харрисона-Руззо-Ульмана.
10. Модель TAKE-GRANT.
11. Расширенная модель TAKE-GRANT.
12. Основы политики мандатного доступа. Решетка безопасности.
13. Модель Белла-ЛаПадулы и основная теорема безопасности
14. Основные расширения модели Белла-ЛаПадулы.
15. Скрытые каналы утечки информации и теоретико-информационные модели безопасности (модель невлияния и модель невыводимости).
16. Модели ролевого доступа. Иерархические системы ролей. Прин-ципы наделения ролей полномочиями.
17. Модели обеспечения целостности. Дискреционная модель Кларка-Вильсона.
18. Модели обеспечения целостности. Мандатная модель Кена Биба.
19. Объединение мандатных моделей Белла-Лападулы и Кена Биба.

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