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 /
«__» _____2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины:

Информационная безопасность

Уровень высшего образования:

магистратура

Направление подготовки / специальность:

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

Направленность (профиль) ОПОП:

Перспективные методы искусственного интеллекта
в сетях передачи и обработки данных

Форма обучения:

очная

Рабочая программа рассмотрена и утверждена
на заседании Ученого совета факультета ВМК
(протокол №7, от 29 сентября 2021 года)

Москва 2021

Рабочая программа дисциплины (модуля) разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.04.02 "Прикладная математика и информатика"утвержденного Приказом Министерства образования и науки РФ от 10 января 2018 г. N 13.

1. Место дисциплины (модуля) в структуре ОПОП ВО:
дисциплина относится к базовой части ОПОП ВО.
Дисциплина входит в обязательную часть магистерской образовательной программы «Перспективные методы искусственного интеллекта в сетях передачи и обработки данных», изучается в 2-м семестре.

2. Входные требования для освоения дисциплины (модуля), предварительные условия (если есть):
Изучение дисциплины базируется на освоении знаний по математическому анализу, теории вероятностей, математической статистике, оптимизации в объеме, соответствующем основным образовательным программам бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки» и другим направлениям подготовки бакалавриата.
3. Результаты обучения по дисциплине (модулю):

Планируемые результаты обучения по дисциплине (модулю)		
Формируемые компетенции (*код и наименование компетенции*)	**Индикаторы достижения компетенций (*код и наименование индикатора*)**	**Результаты обучения *(знания, умения)***
ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.3. Использует современные подходы к верификации ПО в профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.3.З-1. Знает: современные подходы к верификации ПО, их достоинства и недостатки. ОПК-4.3. У-1. Умеет: применять подходы к уменьшению количества уязвимостей в исходном коде на основе систем типов.
ПК-8. Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	ПК-8.1. Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	ПК-8.1. З-1. Знает новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ПК-8.1. У-1. Умеет разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях
	ПК-8.2. Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач	ПК-8.2. З-1. Знает особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях

	с учетом требований информационной безопасности в различных предметных областях	ПК-8.2. У-1. Умеет модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

4. Объем дисциплины (модуля) составляет 4 з.е., в том числе 72 академических часа контактная работа с преподавателем -36академических часа занятий лекционного типа, 36 академических часов занятий практического типа,72 академических часа на самостоятельную работу обучающихся.

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий:
5.1. Структура дисциплины (модуля) по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий (в строгом соответствии с учебным планом)

Наименование разделов и тем дисциплины (модуля), **Форма промежуточной аттестации по дисциплине (модулю)**	**Номинальные трудозатраты обучающегося**			**Всего академических часов**	**Форма текущего контроля успеваемости* (наименование)**
	Контактная работа (работа во взаимодействии с преподавателем) Виды контактной работы, академические часы		**Самостоятельная работа обучающегося, академические часы**		
	Занятия лекционного типа	Практические занятия			
Тема 1. Задачи и методы обеспечения информационной безопасности	6	6	12	24	Опрос
Тема 2. Теоретические основы информационной безопасности операционных систем и баз данных	6	6	12	24	Опрос
Тема 3. Информационная безопасность вычислительных сетей	6	6	12	24	Опрос
Тема 4. Методическое и организационное обеспечение информационной безопасности	6	6	12	24	Опрос
Тема 5. Проблемные вопросы обеспечения информационной безопасности автоматизированных систем и вычислительных сетей	6	6	12	24	Опрос
Тема 6. Использование средств машинного обучения и искусственного интеллекта в управлении информационной безопасностью	6	6	12	24	Опрос

Другие виды самостоятельной работы (отсутствуют)	—	—			—
Промежуточная аттестация (экзамен)					
Итого	*72*		*72*	144	—

5.2. Содержание разделов (тем) дисциплины

№ п/п	Наименование разделов (тем) дисциплины	Содержание разделов (тем) дисциплин
1.	Тема 1. Задачи и методы обеспечения информационной безопасности	Термины и определения. Классификация угроз несанкционированного доступа к информации в АС. Общая характеристика источников угроз несанкционированного доступа в АС. Общая характеристика уязвимостей АС и вычислительных сетей. Угрозы программно-математических воздействий. Компьютерные вирусы и “троянские кони”. Модели нарушителя. Основные функции систем защиты информации. Процедура проверки подлинности субъектов и объектов, параметры парольной идентификации, особенности аутентификации в вычислительных сетях: задачи аутентификации, авторизации и акаунтинга (AAA). Модель системы защиты с полным перекрытием, субъектно-объектная модель системы защиты, понятие изолированной системы, особенности моделирования механизмов безопасности операционных систем и баз данных, основные виды моделей и политик управления доступом — ограниченность моделей и проблемы изменения прав доступа. Методы аутентификации и разграничения доступа в операционных системах Windows и Linux.
2.	Тема 2. Теоретические основы информационной безопасности операционных систем и баз данных	Строгие протоколы аутентификации. Протокол Нидхема-Шредера для симметричной и асимметричной криптографии. Протоколы на основе ключевых хеш-функций. Использование цифровой подписи. Матрица доступа, пятимерное пространства безопасности Хартсона, модели HRU и Take-Grant, основные результаты, их достоинства и недостатки, основные направления развития. MLS модель «военной безопасности», модель Белла-ЛаПадулы, решетки безопасности Деннинг. Модель Биба.

		Тематические классификаторы и решетки мультирубрик. Использование функциональной структуры организации для управления доступом, индивидуально групповая модель управления доступом.
3.	Тема 3. Информационная безопасность вычислительных сетей	Субъекты и объекты компьютерных атак в сетях, виды сетевых атак; методы защиты вычислительных сетей: задачи аутентификации, авторизации и акаунтинга (AAA), сервера безопасности (RADIUS, Kerberos). Задачи фильтрации сетевого трафика. Межсетевые экраны. Фильтрация пакетов. Анализ приложений. Анализ состояний. Прокси сервер. DLP системы. Понятие DMZ. Управление доступом в распределенных системах. Методы оптимизации и методы теории игр при моделировании систем защиты. Теоретико-игровые модели сетевых атак. Модели «доверия» в социальных сетях. Реальность угроз. Типы атак. Структура типовой атаки. Сканирование. Атаки на разных уровнях протокола TCP\IP (ARP-спуффинг, атаки на маршрутизатор, атаки на DNS, атаки HTTP). Методы обнаружения вторжений. Построение VPN, протоколы SSL,SSH,TLS,IPSec. Сети с открытым доступом к каналам связи. Аутентификация, Авторизация – повышенные требования для WiFi, GSM, LTE сетей. Контроль доступа. Основные уязвимости и риски.
4.	Тема 4. Методическое и организационное обеспечение информационной безопасности	Критериальные пространства безопасности. Задача оценки эффективности защиты информации. Понятие риска безопасности, вероятностная модель Клементса. Идентификация рисков, основания для управления рисками для обеспечения непрерывности. Измерение эффективности систем защиты в качественных и количественных шкалах. Экономические модели оценки эффективности. Классификации и упорядоченные классы требований безопасности. Стандарты безопасности. Субъективность оценки эффективности, понятие доверия в безопасности, методы доверия, требования доверия, управление доверием, обеспечение уровня доверия к среде. Принципиальные ограничения моделей эффективности в условиях критических объектов безопасности и угроз инсайдера. Эволюция подходов и моделей управления безопасностью. Процессный характер управления, этапы и факторы управления. Система управления, иерархия политик безопасности. Технологии и инструменты аудита

		безопасности. Мониторинг безопасности, идентификация событий безопасности, нормализация, корреляция и классификация событий безопасности. Управление фильтрацией прикладного уровня, мониторинг прикладного потока через контур сегмента вычислительной среды, угрозы ошибок фильтрации, задача оптимального фильтра. Технологии управление правами для различных моделей доступа, проблема администратора, расщепление полномочий. Технологии управление безопасностью в виртуальных средах: сертификация среды обработки, доверенный супервизор, функциональная и ресурсная инкапсуляция. Идеология «Общих критериев», сеть высокоуровневых сущностей, диалектика зависимости целей, предположений, угроз и политик для среды и объекта защиты, стойкость функций безопасности.
5.	Тема 5. Проблемные вопросы обеспечения информационной безопасности автоматизированных систем и вычислительных сетей	Виртуальные вычисления в центрах обработки данных, «облачные вычисления». Понятие, виды (по памяти, по времени, статистические), обнаружение и методы противодействия; утечки информации в статистических БД; теоретико-вероятностная модель «невыводимости» и «невлияния». Понятие анонимных сетей. Примеры анонимных сетей. TOR. I2P. Уязвимости. Обнаружение. Безопасность SDN. Разделение потока данных и управляющего потока. Возможные виды атак. Скрытые каналы**.**
6.	Тема 6. Использование средств машинного обучения и искусственного интеллекта в управлении информационной безопасностью.	Методы ИИ в управлении информационной безопасностью. Основные функции и методы управления ИБ. Задачи обнаружения, адаптации и прогнозирования. Роль ИИ в управлении ИБ. Особенности управления ИБ КИИ. Типы ИИ используемые в системах управления ИБ: • байесовская модель; • деревья решения (решающие деревья); • метод опорных векторов; • искусственные нейронные сети, включая сверточные нейронные сети, сети глубокого обучения, машину Больцмана, сети Хопфилда, сети Кохонена и другие решения, основанные на использовании искусственных нейронов; • бустинг и бэггинг. Возможности и ограничения при использовании ИИ в управлении ИБ

		(классификация, кластеризация, регрессия, распознавание образов, ведение полноценных диалогов и т.д.). Машинное обучение систем управления ИБ . Понятие событий безопасности - элементарные и агрегированные события. Наборы данных (датасеты) для машинного обучения. Состав и методы получения наборов данных (датасетов) для обучения и тестирования качества обучения, различающихся по источникам и типу данных. Дата сеты сетевого трафика: KDD Cup 1999, NSL-KDD (2009), UNSW-NB15 (2015), CAIDA (2002-2016), CSE-CIC-IDS2018 и др. Дата сеты интернет трафика: MAWI (2011)URL (2016), Tor-nonTor (2017), UMASS (2018). Дата сеты VPN трафика: VPN-nonVPN (2016). Метрики оценки качества обучения.

6. Фонд оценочных средств (ФОС, оценочные и методические материалы) для оценивания результатов обучения по дисциплине (модулю).

6.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости, критерии и шкалы оценивания (в отсутствие утвержденных соответствующих локальных нормативных актов на факультете)

1. Граф «угроза - объект» - как базовая модель СЗИ
2. Основные функции и методы реализации СЗИ
3. Угрозы безопасности КС
4. Процедуры подтверждения подлинности (идентификация и аутентификация)
5. Статические биометрические методы идентификации и их характеристики
6. Динамические биометрические методы идентификации и их характеристики
7. Методы взлома парольной защиты и модификации схемы «простой пароль»
8. Методы парольной аутентификации PAP, CHAP, MsChap
9. ЭЦП как средство аутентификации любых цифровых данных
10. Субъектно-объектная модель компьютерной системы. Монитор безопасности
11. Модели (политики) безопасности в субъектно-объектной модели КС
12. Модели на основе матрицы доступа (варианты принудительного и добровольного управления доступом, проблема «троянских коней»)
13. Модель Харрисона-Руззо-Ульмана (модель HRU). Критерий безопасности и основные теоремы модели HRU
14. Расширения модели HRU
15. Теоретико-графовая модель «take-grant». Распространение (утечка) прав доступа в графе модели «take-grant», состоящем из субъектов
16. Теоретико-графовая модель «take-grant». Распространение (утечка) прав доступа в графе модели «take-grant», состоящем из субъектов и объектов
17. Критерий безопасности и основная теорема модели «take-grant»
18. Расширенная модель Take–Grant, “неявные” информационные потоки.
19. Достоинства и недостатки дискреционных моделей
20. Основные положения моделей мандатного доступа. Решетка уровней и функции безопасности. MLS решетка.
21. Модель Белла-Ла Падулы. Критерий безопасности модели Белла-Ла Падулы.
22. Достоинства и недостатки модели Белла-Ла Падулы

23. Модификации модели Белла-Ла Падулы (Мак-Лин, LWM)

24. Основные ограничения моделей мандатного доступа.

25. Модели безопасности на основе тематической политики доступа

26. Дескрипторная тематическая классификация в модели тематической политики доступа

27. Иерархическая тематическая классификация в модели тематической политики доступа

28. Тематические решетки в модели тематической политики доступа

29. Решетка мультирубрик в модели тематической политики доступа

30. Модели ролевого доступа

31. Модели индивидуально-группового доступа

32. Политики безопасности в Windows и Linux.

33. Понятие скрытых каналов утечки информации в моделях разграничения доступа. Виды скрытых каналов утечки информации. Понятие скрытых каналов по памяти и скрытых каналов по времени.

34. Статистический скрытый канал передачи информации

35. Автоматная модель невлияния Гогена-Месигера (GM-модель)

36. Понятие целостности данных. Мандатная модель целостности Биба.
37. Модели комплексной оценки защищенности КС
38. Угрозы сети традиционные и «типично сетевые»
39. Оценка рисков нарушения ИБ
40. Стандарты в сфере безопасности ИТ (типы объектов, шкалы)
41. Развитие стандартов, ГОСТ и РД.
42. Защищенные протоколы. Уязвимости протоколов интернет.
43. Анонимность в интернет.
44. Анонимные сети
45. Защищенные протоколы.
46. Сертификаты и ЭЦП. Иерархия сертификатов.
47. Аутентификация и авторизация.
48. Протокол аутентификации Kerberos
49. Управление доступом. Межсетевые экраны. DMZ.
50. Сканирование сетей.
51. Перехват данных. Снифинг. Включение в разрыв сети. Методы защиты.
52. Перехват данных. Ложные запросы. Перехват TCP-соединения. Методы защиты.
53. Атаки на отказ в обслуживании. Цели и основные методы атак.Методы защиты

6.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации по дисциплине, критерии и шкалы оценивания

1. Эволюция подхода к управлению ИБ: реактивный, системно-сервисный, архитектурный, развитие пространства критериев ИБ, принципиально процессный характер управления ИБ, содержание этапов жизненного цикла управления.
2. Содержание и инструменты уровней управления ИБ, концептуальные принципы безопасности, основания дифференциации защищаемых информационных активов, диалектика и компоненты понятия угрозы, методы формирования модели угроз, виды политик ИБ.
3. Иерархическая классификация объектов защиты и требований безопасности в традиционной идеологии управления ИБ, ограничения традиционной идеологии, стандартизация управления ИБ, система стандартов 27-го подкомитета ISO.

4. Идеология анализа и управления информационными рисками, исчисляемые факторы при двух-, трех- и четырехфакторном анализе рисков, вероятностное расширение модели Клементса, проблемы экспертного оценивания и количественной интерпретации качественных шкал.
5. Модель высокоуровневых понятий в идеологии общих критериев, диалектика взаимодействия угроз, политик, предположений и целей безопасности в профиле защиты, функциональные требования безопасности и требования доверия, оценочные уровни доверия.
6. Управление специальными методами безопасности, безопасность критических объектов информационной инфраструктуры, привлечение фактора необратимости, делегирование управления ИБ, динамические политики ИБ.
7. Управление защитой от угроз инсайдера, принципиальная избыточность полномочий, факторы избыточности, ограниченность мониторинга событий безопасности и традиционных методов защиты, методы компенсации потенциала угроз инсайдера.

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: опрос, тесты)*	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения *(виды оценочных средств: практические задания)*	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: выполнение и защита курсовой работы, отчет по практике, отчет по НИР и т.п.)*	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

7. Ресурсное обеспечение:

7.1. Перечень основной и дополнительной литературы

Основная литература

1. Основы управления информационной безопасностью: учебное пособие. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - М.: Горячая Линия-Телеком, 2012. - 244 с.
2. Смелянский Р.Л., Антоненко В.А. Концепции программного управления и виртуализации сетевых сервисов в современных сетях передачи данных. М. Курсю 2020.- 259с.
3. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных структур. М. Горячая Линия-Телеком, 2021. - 239 с.

Дополнительная литература

1. ГрушоА.А.,Тимонина Е.Е. Теоретические основы защиты информации. М.:Яхтсмен, 1996. - 192с.
2. Мельников Д.А. Информационная безопасность открытых систем [Текст] : Учебник/ Д. А. Мельников. - М. : Флинта: Наука, 2013. - 448 с. - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7. 004.056(075.8) - М-482
3. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : [Учеб.пособие] / В. Ф. Шаньгин. - М. : ДМК Пресс, 2012. - 592 с. - Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 978-5-94074-637-9.
4. Галатенко В.А. Стандарты информационной безопасности [Текст] : Курс лекций: Учеб.пособие / В. А. Галатенко ; Под ред. В.Б. Бетелина. - 2-е изд. - М. : Интернет-Университет Информационных технологий, 2012. - 264 с. - 2000 экз. - ISBN 978-5-9556-0053-6 : 262-51; 262-50.
5. 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.

7.2. Перечень лицензионного программного обеспечения, в том числе отечественного производства

При реализации дисциплины может быть использовано следующее программное обеспечение:

1. Операционная система Ubuntu 18.04.
2. Операционная система ALT Linux MATE Starterkit 9 лицензия GPL
3. Статистический пакет MATLAB (или свободный аналог Octave)
4. Операционная система Microsoft Windows 10 Education академическая лицензия
5. Программный продукт Python 3.5.1 (64-bit)Python Software Foundation

7.3. Перечень профессиональных баз данных и информационных справочных систем

1. http://www.edu.ru – портал Министерства образования и науки РФ
2. http://www.ict.edu.ru – система федеральных образовательных порталов «ИКТ в образовании»
3. http://www.openet.ru - Российский портал открытого образования
4. http://www.mon.gov.ru - Министерство образования и науки Российской Федерации

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. mk.cs.msu.ru
2. http://www.intuit.ru/studies/courses
3. Сетевой журнал «Хаер» https://xakep.ru/
4. Журнал «Защита информации. Инсайд»; Сайт журнала http://www.inside-zi.ru/
5. Информационный бюллетень "JetInfo". Издатель: компания «ИнфосистемыДжет».Сайт журнала www.jetinfo.ru.

7.5. Описание материально-технического обеспечения.

Образовательная организация, ответственная за реализацию данной Программы, располагает соответствующей материально-технической базой, включая современную вычислительную технику, объединенную в локальную вычислительную сеть, имеющую выход в Интернет. Используются специализированные компьютерные классы, оснащенные современным оборудованием. Материальная база соответствует действующим санитарно-техническим нормам и обеспечивает проведение всех видов занятий (лабораторной, практической, дисциплинарной и междисциплинарной подготовки) и научно-исследовательской работы обучающихся, предусмотренных учебным планом.

8. Соответствие результатов обучения по данному элементу ОПОП результатам освоения ОПОП указано в Общей характеристике ОПОП.

9. Разработчик (разработчики) программы.

к.т.н., с.н.с., Пилюгин Павел Львович