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 /
«14» октября 2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность облачных технологий»

Уровень высшего образования:

магистратура

Направление подготовки / специальность:

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

Направленность (профиль) ОПОП:

Искусственный интеллект в кибербезопасности

Форма обучения:

очная

Рабочая программа рассмотрена и утверждена
на заседании Ученого совета факультета ВМК
(протокол №4, от 29 сентября 2021 года)

Москва 2021

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 01.04.02 "Прикладная математика и информатика" программы магистратуры в редакции приказа МГУ от 21 декабря 2021 года No 1404.

1. Место дисциплины (модуля) в структуре ОПОП ВО:
Дисциплина (модуль) относится к части дисциплин основной профессиональной образовательной программы, формируемых участниками образовательных отношений.

2. Входные требования для освоения дисциплины (модуля), предварительные условия:
учащиеся должны владеть знаниями по математическому анализу, линейной алгебре и теории вероятностей в объеме, соответствующем программе обучения основных образовательных программ 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), соотнесенные с требуемыми компетенциями выпускников.

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-8. Способен осуществлять эффективное управление проектами по разработке и внедрению систем искусственного интеллекта	ОПК-8.1. Исследует архитектуру информационных систем предприятий и организаций; применяет методологии и технологии реинжиниринга, проектирования и аудита информационных систем различных классов	ОПК-8.1. З-1. Знает новые научные принципы и методы реинжиниринга, проектирования и аудита информационных систем для решения профессиональных задач ОПК-8.1. У-1. Умеет разрабатывать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач
	ОПК-8.2. Применяет инструментальные средства поддержки технологии проектирования и аудита информационных систем и сервисов; методы оценки экономической эффективности и качества, управления надежностью и информационной безопасностью	ОПК-8.2. З-1. Знает особенности модернизации программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач ОПК-8.2. У-1. Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных

		систем для решения профессиональных задач
	ОПК-8.3. Исследует особенности процессного подхода к управлению информационными системами и системами искусственного интеллекта; применяет системы управления качеством	ОПК-8.3. З-1. Знает особенности процессного подхода к управлению информационными системами и системами искусственного интеллекта; системы управления качеством ОПК-8.3. У-1. Умеет применять системы управления качеством
	ОПК-8.4. Выбирает методологию и технологию проектирования информационных систем; обосновывает архитектуру информационных систем и систем искусственного интеллекта	ОПК-8.4. З-1. Знает методологию и технологию проектирования информационных систем ОПК-8.4. У-1. Умеет обосновывать архитектуру информационных систем и систем искусственного интеллекта
	ОПК-8.5. Управляет проектами по созданию (модификации) программного обеспечения, на всех стадиях жизненного цикла, оценивает эффективность и качество проекта; применяет современные методы управления проектами по разработке и внедрению систем искусственного интеллекта	ОПК-8.5. З-1. Знает особенности управления проектами по созданию (модификации) программного обеспечения на всех стадиях жизненного цикла, ОПК-8.5. У-1. Умеет оценивать эффективность и качество проекта; применять современные методы управления проектами и сервисами информационных систем и систем искусственного интеллекта
	ОПК-8.6. Использует инновационные подходы к проектированию информационных систем и систем искусственного интеллекта; принимает решения по информатизации предприятий в условиях неопределенности	ОПК-8.6. З-1. Знает инновационные подходы к проектированию информационных систем и систем искусственного интеллекта ОПК-8.6. У-1. Умеет принимать решения по информатизации предприятий в условиях неопределенности

ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.2. Комбинирует и адаптирует существующие информационно-коммуникационные технологии систем искусственного интеллекта с учетом требований информационной безопасности	ОПК-4.2. З-1 Знает : основные подходы к обеспечению безопасности систем, размещенных в облачных окружениях. ОПК-4.2. У-1 Умеет : проводить анализ защищенности вычислительных систем, развёрнутых в облачных окружениях. ОПК-4.2. В-1 Владеет: навыками построения защищенной инфраструктуры в облачных окружениях.

4. Объем дисциплины (модуля) составляет 3 з.е., в том числе 36 академических часа, отведенных на контактную работу обучающихся с преподавателем, 72 академических часов на самостоятельную работу обучающихся.

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

В курсе рассматриваются современные технологии контейнеризации и виртуализации вычислительных ресурсов и сетей. Проводится подробное сравнение технологий контейнеризации и виртуализации с точки зрения безопасности. Рассматриваются примеры уязвимостей,

свойственные данным технологиям. Детально рассматриваются технологии изоляции и управления привилегиями, реализованные в ОС Linux. Изучаются различные подходы к проектированию облачных провайдеров, а также проводится моделирование угроз для информационных систем, размещенных в облаке. Рассматриваются модели угроз для IaaS, PaaS, SaaS технологий, а также для технологии бессерверных вычислений.

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), часы из них						**Самостоятельная работа обучающегося, часы из них**		
		Занятия лекционного типа	Практические занятия	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**
Тема 1 Введение в облачные технологии. Архитектура облачных провайдеров. Основные модели угроз	2	2					2	0		0

Тема 2 Управление доступом в Linux системах	3	1					1	2		2
Тема 3 Механизмы изоляции в ОС Linux	17	1					1	16		16
Тема 4 Безопасность Docker	6	1					2	4		4
Тема 5 Безопасность Kubernetes	8	1					4	4		4
Тема 6 Технологии виртуализации и атаки на них	4	2					4	0		0
Тема 7 Альтернативные технологии изоляции исполняемого кода	2	2					2	0		0
Тема 8 Введение в технологии виртуализации сетей	2	2					2	0		0
Тема 9 Платформа OpenStack и примеры уязвимостей в ней	2	2					2	0		0
Тема 10 Атаки на бессерверные вычисления	14	2	8				10	4		4
Тема 11 Особенности проведения тестирований на проникновение в облачных окружениях	17	1	10				11	6		6
Тема 12 Особенности выполнения требований законодательства в облачных окружениях	1	1					1	0		0
Промежуточная аттестация - экзамен								36		36
Итого	108	18	18				36	72		72

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

Примерные практические контрольные задания для текущего контроля успеваемости.

ПКЗ ТК1. Демонстрация возможностей работы с инструментальной базой.

Примерные варианты заданий:

1. Перехват зашифрованного трафика с помощью Fiddler на этапе авторизации по протоколу oauth 2.0.
2. Эксплуатация существующих уязвимостей с помощью Metasploit Framework.
3. Анализ приложения с помощью WinDbg, IdaPro.

ПКЗ ТК2. Разработка приложений с уязвимостями «переполнения» и демонстрация эксплуатации их.

Примерные варианты заданий:

1. Разработка приложения win32 console application с уязвимостью переполнения стека, разработка эксплоита типа переполнения стека.
2. Разработка приложения win32 console application с уязвимостью переполнения обработчика исключений, разработка эксплоита типа переполнения обработчика исключений на стеке.

ПКЗ ТК3. Поиск уязвимостей.

Примерные варианты заданий:

1. Использование фаззинга для поиска уязвимостей в существующем ПО или собственном.
2. Обфускация бинарного шеллкода.
3. Нахождение возможностей передачи управления.

Создание Rop-цепочек для полезной нагрузки.

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

Список вопросов для экзамена.

1. Основные особенности архитектуры публичных облаков.
2. Модель угроз для облачных сервисов.
3. Модель управления доступом в Linux системах.
4. Linux namespaces и особенности их использования.

5. Особенности использования Seccomp для построения изолированных окружений.
6. Использование мандатных систем управления доступа для построения песочниц.
7. Механизмы работы Linux capabilities.
8. Типовые атаки на Docker.
9. Типовые атаки на Kubernetes.
10. Атаки на современные системы виртуализации.
11. Сравнение технологий виртуализации сетей.
12. Примеры уязвимостей в платформе OpenStack.
13. Особенности проведения тестирований на проникновение в облачных окружениях.
14. Атаки на бессерверные вычисления.
15. Особенности выполнения требований регуляторов в облачных окружениях.

Методические материалы для проведения процедур оценивания результатов обучения

Особенности организации процесса обучения

Для эффективного освоения курса рекомендуется перед каждым занятие привести в порядок конспекты лекций. После каждого занятия рекомендуется найти и прочитать дополнительную литературу по теме лекции и прочитать свои конспекты.

Система контроля и оценивания

За каждую домашнюю выставляются баллы (максимум 40 баллов). Пусть M – максимальное число баллов, которое может набрать студент. В конце семестра баллы конвертируются в оценку O1 следующим образом:

меньше M/2 баллов: O1=2;

больше или равно M/2 баллов, но меньше 2M/3: O1=3;

больше или равно 2M/3 баллов, но меньше 5M/6: O1=4;

больше или равно 5M/6 баллов: O1=5.

На экзамене оценка O1 является стартовой. Окончательная оценка определяется исходя из оценки устного ответа студента, при этом она не может отличаться от стартовой оценки более чем на 1 балл.

Структура и график контрольных мероприятий

Сдача домашних заданий, устный экзамен в конце семестра.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)				
Оценка РО и соответствующие виды оценочных средств	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
Знания *Зачет*	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения *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) *Зачет, практические занятия*	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. Adkins H., Beyer B., Blankinship P., Oprea A., Lewandowski P., Stubblefield A. Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems, O'Reilly Media, 2020
2. Rice L. Container Security: Fundamental Technology Concepts that Protect Containerized Applications, O'Reilly Media, 2020
3. Dotson C., Practical Cloud Security: A Guide for Secure Design and Deployment, O'Reilly Media, 2019

Дополнительная литература

1. Google Cloud security foundations guide, Google Cloud Whitepaper, 2020
2. Malisow B. (ISC)2 CCSP Certified Cloud Security Professional Official Study Guide, Sybex, 2019

7.2. Перечень лицензионного программного обеспечения, в том числе отечественного производстваПри реализации дисциплины может быть использовано следующее программное обеспечение:

1. Программное обеспечение для подготовки слайдов лекций MS PowerPoint
2. Программное обеспечение для создания и просмотра pdf-документов Adobe Reader
3. Издательская система LaTeX.

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
5. http://www.fasi.gov.ru - Федеральное агентство по науке и инновациям

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Math-Net.Ru [Электронный ресурс] : общероссийский математический портал / Математический институт им. В. А. Стеклова РАН ; Российская академия наук, Отделение математических наук. - М. : [б. и.], 2010. - Загл. с титул. экрана. - Б. ц.
URL: http://www.mathnet.ru
2. Университетская библиотека Online [Электронный ресурс] : электронная библиотечная система / ООО "Директ-Медиа" . - М. : [б. и.], 2001. - Загл. с титул. экрана. - Б. ц. URL: www.biblioclub.ru
3. Универсальные базы данных East View [Электронный ресурс] : информационный ресурс / East View Information Services. - М. : [б. и.], 2012. - Загл. с титул. экрана. - Б. ц.
URL: www.ebiblioteka.ru
4. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] : информационный портал / ООО "РУНЭБ" ; Санкт-Петербургский государственный университет. - М. : [б. и.], 2005. - Загл. с титул. экрана. - Б. ц.
URL: www.eLibrary.ru

7.5. Описание материально-технического обеспечения.

Факультет ВМК, ответственный 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 факультета 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.

Жаболенко Антон Сергеевич, Гамаюнов Денис Юрьевич.

10. Язык преподавания - русский.