Федеральное государственное бюджетное образовательное учреждение
высшего образования
Московский государственный университет имени М.В. Ломоносова
Факультет Вычислительной математики и кибернетики

УТВЕРЖДАЮ
Декан факультета ВМК

_____ / Соколов И.А. /
«05» 09 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование дисциплины:

Как уберечь мир от киберармагеддона: уязвимости, угрозы, решения

код и наименование дисциплины (модуля)

Уровень высшего образования:

бакалавриат, магистратура, специалитет

указывается: бакалавриат, магистратура или специалитет

Направление подготовки (специальность):

(код и название направления/специальности)

Направленность (профиль) ОПОП:

(если дисциплина (модуль) относится к вариативной части программы)

Форма обучения:

очная с использованием дистанционных образовательных технологий

очная, очно-заочная, заочная

Рабочая программа рассмотрена и одобрена
на заседании Ученого совета факультета
(протокол № 5, 30.06.2022)

Москва 2022 г.

1. Место дисциплины (модуля) в структуре ОПОП реализуется в рамках МФК.

2. Входные требования для освоения дисциплины (модуля), предварительные условия: не требуются.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников.

Компетенции выпускников (коды)	**Индикаторы (показатели) достижения компетенций**	**Планируемые результаты обучения по дисциплине (модулю), сопряженные с компетенциями**
Новая УК ОС МГУ Способен применять полученные знания для анализа и прогноза процессов и деятельности с точки зрения международной информационной безопасности, а также повышения уровня личной киберграмотности и кибергигиены.	УК-N (Ин.1ук) Знает основные термины и аспекты, связанные с проблематикой развития информационного общества и угроз информационной безопасности, формирования системы международной информационной безопасности, управления Интернетом, военно-политического использования технологий искусственного интеллекта.	**Знать:** Основные термины и аспекты, связанные с проблематикой развития информационного общества и угроз информационной безопасности, формирования системы международной информационной безопасности, управления Интернетом на региональном и международном уровнях, создания цифровой границы; военно-политического использования технологий искусственного интеллекта. **Уметь** Применять полученные знания для анализа процессов и деятельности с точки зрения международной информационной безопасности. **Владеть:** Владеет методами и технологиями повышения уровня личной кибергигиены и киберграмотности.
	УК-N (Ин.2ук) Умеет проводить поиск, обработку и анализ данных для изучения процессов и деятельности с точки зрения международной информационной безопасности.	
	УК-N (Ин.3ук) Владеет методами и технологиями повышения уровня личной кибергигиены и кибергамотности..	

4. Объем дисциплины (модуля) 1 з.е., в том числе 24 академических часа на контактную работу обучающихся с преподавателем, 12 академических часа на самостоятельную работу обучающихся.

5. Формат обучения очное обучение с возможностью использования *дистанционных образовательных технологий*

6. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических 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** ***Виды самостоятельной работы, часы***	
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	**Всего**	**Работа в среде электронного обучения**	**Всего**
Тема 1. Сценарии киберармагеддона.	3	2				2	1	1
Тема 2. Технологический колониализм и цифровой суверенитет.	3	2				2	1	1
Тема 3. Интернет как общечеловеческое достояние и инструмент влияния.	3	2				2	1	1
Тема 4. Цифровые границы – теория и практика.	3	2				2	1	1
Тема 5. Подходы к обеспечению безопас-ности глобального информационного пространства.	3	2				2	1	1
Тема 6.	3	2				2	1	1

Информационная безопасность и международное право.								
Тема 7. Военно-политическое использование киберпространства.	3	2				2	1	1
Тема 8. Угроза использования ИКТ в террористических и экстремистских целях.	3	2				2	1	1
Тема 9. Международное сотрудничество в области противодействия киберпреступности.	3	2				2	1	1
Тема 10. Новейшие ИКТ, как источники новых уязвимостей и угроз: Интернет вещей, социальные медиа, блокчейн.	3	2				2	1	1
Тема 11. Формирование системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях.	3	2				2	1	1

Тема 12. Как уберечь мир от киберармагеддона? Подведение итогов.	3	2				2	1	1
Промежуточная аттестация	*Опрос-тестирование*						Зачет	
Итого	36	24				24	12	12

** Текущий контроль успеваемости может быть реализован в рамках занятий семинарского типа, групповых или индивидуальных консультаций*

*** Практическая подготовка (при наличии) осуществляется на базе ...(указать – структурное подразделение МГУ или организацию (предприятие), практическая подготовка на базе которого осуществляется на основании Договора)*

**** Часы на проведение промежуточной аттестации выделяются из часов самостоятельной работы обучающегося.*

7. Фонд оценочных средств для оценивания результатов обучения по дисциплине (модулю)

РЕЗУЛЬТАТ ОБУЧЕНИЯ по дисциплине (модулю)	**СРЕДСТВА ОЦЕНИВАНИЯ**	**ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ по дисциплине (модулю)**			
		2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
Знать:					
Основные термины и понятия информационной безопасности	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Виды угроз информационной безопасности	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Характеристики угроз информационной безопасности	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Основные аспекты формирования системы международной информационной безопасности	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания

Основные аспекты проблемы управления интернетом	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Основные аспекты военно-политического использования технологий искусственного интеллекта	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Уметь					
Проводить поиск, обработку и анализ данных для изучения процессов и деятельности с точки зрения международной информационной безопасности	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Владеть					
методами и технологиями повышения уровня личной киберграмотности и кибергигиены	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания

Типовые задания и иные материалы, необходимые для оценки результатов обучения

Примерные тестовые задания

Вопрос 1.

Чем обусловлена привлекательность использования ИКТ-инструментов для решения военно-политических задач?

- Сложность атрибуции
- Доступность
- Эффективность
- Всё вышеперечисленное

Вопрос 2.

Эффективным механизмом снижения опасности возникновения конфликтов и разрешения межгосударственных противоречий, связанных с враждебным использованием ИКТ государствами, может стать...

- ...создание глобальной сети файерволлов.
- ...внедрение норм и правил ответственного поведения государств в ИКТ-среде.
- ...распространение практики публичной атрибуции кибератак.

- ...практика ответных кибератак.

Вопрос 3.
Как называются ИКТ-уязвимости, против которых ещё не создано защиты?

- Уязвимости первого месяца
- Уязвимости судного дня
- Уязвимости нулевого дня
- Ничего из вышеперечисленного

Вопрос 4.
Одним из видов социальной инженерии является т.н. «фишинг». Как он работает? (восстановите последовательность)

- Проводится массовая рассылка поддельных электронных писем
- Пользователь переходит по ссылке на сайт, внешне неотличимый от настоящего
- Пользователь вводит свои данные
- Личные сведения используются мошенниками для доступа к учетной записи пользователя

Вопрос 5.
Откуда чаще всего злоумышленники получают информацию о человеке, против которого готовится целевой фишинг?

- Из газет.
- Из социальных сетей.
- В личной беседе.
- Путём анкетирования.

Вопрос 6.
Что поможет пользователю эффективно защититься от киберугроз? (выберите нужные варианты)

- файерволл
- антивирус
- киберграмотность
- кибергигиена
- биометрическая защита
- игнорировние проблем
- "пиратское" программное обеспечение

Вопрос 7.

Можно ли «взломать» систему с искусственным интеллектом?

- Да, используя грубую силу
- Нет, системы ИИ абсолютно устойчивы
- Да, ИИ подвержены угрозам информационной безопасности, в том числе кибер-когнитивным воздействиям

Вопрос 8.
Как сегодня внедрить этику в искусственный интеллект?

- Применяя три закона робототехники
- Через создание думающих роботов
- Ответственно разрабатывая, внедряя и используя ИИ

Вопрос 9.
Укажите основные недостатки Конвенции о преступности в сфере компьютерной информации (Будапештская конвенция 2001 г.)

- Отдельные положения документа входят в противоречие с национальным суверенитетом государств
- Конвенция не учитывает развитие методов и появление новых видов киберпреступности
- Конвенция закрыта для широкого международного участия
- Конвенция не обязательна для исполнения
- Конвенция провоцирует возникновение "тихих гаваней"

Вопрос 10.
Цифровой колониализм - это...

- возникновение зависимости развивающихся и слабо развитых стран от крупнейших цировых платформ
- основание колоний пользователей в виртуальном пространстве
- конкуренция крупнейших цифровых платформ за пользователей в развитых странах

Вопросы к зачету:

1. Основные источники (акторы) угроз, исходящих из ИКТ-среды, их характер и значимость.
2. Существенные особенности ИКТ-среды в техническом, правовом и международном аспекте.
3. Феномен кибероружия и проблемы его регулирования.
4. Цифровизация войны – основные проявления, новые угрозы и проблема регулирования.

5. Концепция цифрового суверенитета и цифровой колониализм.
6. Эволюция феномена информационного общества и его характерные черты.
7. Критически важная инфраструктура – сущность, угрозы, обеспечение информационной безопасности.
8. Кибер-конгитивные угрозы искусственному интеллекту: сущность и причины явления.
9. Основные аспекты человеческого измерения этики искусственного интеллекта.
10. Российские инициативы в области международной информационной безопасности.
11. Международное сотрудничество в области противодействия угрозе использования ИКТ в военно-политических целях.
12. Кибертерроризм: сущность явления и основные проявления, проблемы противодействия.
13. Международное сотрудничество в области противодействия кибертерроризму.
14. Киберпреступность: сущность явления и основные проявления, проблемы противодействия.
15. Международное сотрудничество в области противодействия киберпреступности.
16. Актуальные проблемы управления сетью Интернет.

8. Ресурсное обеспечение:

- Перечень основной и дополнительной учебной литературы
  - Основная литература
    1. Садовничий В.А. Как защитить человека от инфогенных рисков и угроз? В сборнике «Научные проблемы национальной безопасности Российской Федерации», выпуск 5. М., 2012 г. С. 302.
    2. Материалы международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» (2012-2015 гг.)
    3. Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности. Журнал Международные процессы.
    4. Крутских А.В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности. Журнал Международная жизнь.
    5. Крутских А.В. Кто владеет Интернетом, тот владеет миром. Журнал Международная жизнь.
    6. Международная информационная безопасность: проблемы и решения. Сборник трудов / Под ред. С.А. Комова. – М.: 2009. – 240 с.
    7. Современное состояние и перспективы развития военного сотрудничества Российской Федерации в области международной информационной безопасности. Сборник материалов / Под общ. ред. С.А. Комова. – М.: 2014.

8. Проблемы информационной безопасности в полицентричном мире / П.А.Шариков. – Институт США и Канады РАН. – М.: Издательство «Весь Мир», 2015. 320 с.
9. Сетевой фактор. Интернет и общество. Взгляд / Б.Н.Мирошников. – М.: «Кучково поле», 2015. – 296 с.

- Дополнительная литература
  1. Стрельцов А.А. «Обеспечение информационной безопасности России. Теоретические и методологические основы» / Под ред. В.А. Садовничего и В.П. Шерстюка. – М., МЦНМО, 2002. – 296 с.
  2. Уэбстер Ф. Теории информационного' общества.- М.: Аспект Пресс, 2004.- 400 с.
  3. Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. – М.: Международные отношения, 2014. – 848 с.
  4. Будущее власти / С. Джозеф Най, мл.; пер. с англ. В.Н. Верченко. – М.: АСТ, 2014. – 444, [4] с. – (Политика)

- Перечень профессиональных баз данных и информационных справочных систем
  1. Российская национальная библиотека (РНБ). www. hbl-russia.ru http://www. nlr. ru.
  2. Российская государственная библиотека (РГБ). http://www. rsl. ru.
  3. ЭБС « Университетская библиотека онлайн» http:www.biblioclub.ru
  4. ЭБС «Znanium.com» http://znanium.com/
  5. ЭБС «Юрайт» https://biblio-online.ru/

9. Язык преподавания.
Русский

10. Преподаватель (преподаватели).
Шаряпов Р.А. – к.полит.н., в.н.с. Центра проблем информационной безопасности ВМК МГУ; Карасев П.А. – к.полит.н., с.н.с. Центра проблем информационной безопасности ВМК МГУ; Ященко В.В. – к.ф.-м.н., зам. руководителя Центра проблем информационной безопасности ВМК МГУ.

11. Разработчики программы.
Шаряпов Р.А. – к.полит.н., в.н.с. Центра проблем информационной безопасности ВМК МГУ; Карасев П.А. – к.полит.н., с.н.с. Центра проблем информационной безопасности ВМК МГУ; Ященко В.В. – к.ф.-м.н., зам. руководителя Центра проблем информационной безопасности ВМК МГУ.