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

Наименование дисциплины (модуля):

Дополнительные главы практической безопасности

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 №_14_, 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): учащиеся должны владеть базовыми знаниями по практической веб-безопасности, реверс-инжинирингу, эксплуатации бинарных уязвимостей, криптографии и разработке

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-4. Способен осуществлять эффективное управление проектами по разработке и внедрению систем искусственного интеллекта	ОПК-4.1. Исследует архитектуру информационных систем предприятий и организаций; применяет методологии и технологии реинжиниринга, проектирования и аудита информационных систем различных классов ОПК-4.2. Применяет инструментальные средства поддержки технологии проектирования и аудита информационных систем и сервисов; методы оценки экономической эффективности и качества, управления надежностью и информационной безопасностью ОПК-4.3. Исследует особенности процессного подхода к управлению информационными системами и системами искусственного интеллекта; применяет системы управления качеством ОПК-4.4. Выбирает методологию и технологию проектирования информационных систем; обосновывает архитектуру информационных	ОПК-4.1. З-1. Знает новые научные принципы и методы реинжиниринга, проектирования и аудита информационных систем для решения профессиональных задач ОПК-4.1. У-1. Умеет разрабатывать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач ОПК-4.2. З-1. Знает особенности модернизации программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач ОПК-4.2. У-1. Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач ОПК-4.3. З-1. Знает особенности процессного подхода к управлению информационными системами и системами искусственного интеллекта; системы управления качеством

	систем и систем искусственного интеллекта ОПК-4.5. 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-4.6. Использует инновационные подходы к проектированию информационных систем и систем искусственного интеллекта; принимает решения по информатизации предприятий в условиях неопределенности ОПК-4.7. Проводит реинжиниринг прикладных и информационных процессов	ОПК-4.3. У-1. Умеет применять системы управления качеством ОПК-4.4. З-1. Знает методологию и технологию проектирования информационных систем ОПК-4.4. У-1. Умеет обосновывать архитектуру информационных систем и систем искусственного интеллекта ОПК-4.5. З-1. Знает особенности управления проектами по созданию (модификации) программного обеспечения на всех стадиях жизненного цикла, ОПК-4.5. У-1. Умеет оценивать эффективность и качество проекта; применять современные методы управления проектами и сервисами информационных систем и систем искусственного интеллекта ОПК-4.6. З-1. Знает инновационные подходы к проектированию информационных систем и систем искусственного интеллекта ОПК-4.6. У-1. Умеет принимать решения по информатизации предприятий в условиях неопределенности ОПК-4.7. З-1. Знает особенности процессного подхода, принципы реинжиниринга прикладных и информационных процессов ОПК-4.7. У-1. Умеет проводить реинжиниринг прикладных и информационных процессов

ПК-5. Способен руководить проектами по созданию, поддержке и использованию системы искусственного интеллекта на основе нейросетевых моделей и методов	ПК-5.1. Руководит работами по оценке и выбору моделей искусственных нейронных сетей и инструментальных средств для решения поставленной задачи ПК-5.2. Руководит созданием систем искусственного интеллекта на основе моделей искусственных нейронных сетей и инструментальных средств	ПК-5.1. З-1. Знает функциональность современных инструментальных средств и систем программирования в области создания моделей искусственных нейронных сетей ПК-5.1. У-1. Умеет проводить оценку и выбор моделей искусственных нейронных сетей и инструментальных средств для решения задач машинного обучения ПК-5.1. У-2. Умеет применять современные инструментальные средства и системы программирования для разработки и обучения моделей искусственных нейронных сетей ПК-5.2. З-1. Знает принципы построения систем искусственного интеллекта на основе искусственных нейронных сетей, методы и подходы к планированию и реализации проектов по созданию систем искусственного интеллекта ПК-5.2. У-1. Умеет руководить выполнением коллективной проектной деятельности для создания, поддержки и использования систем искусственного интеллекта на основе искусственных нейронных сетей

4. Объем дисциплины (модуля) составляет 2 з.е., в том числе 36 академических часа, отведенных на контактную работу обучающихся с преподавателем, 36 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.

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, часы** *(виды самостоятельной работы – эссе, реферат, контрольная работа и пр. – указываются при необходимости)*
		Занятия лекционного типа*	Занятия семинарского типа*	**Всего**	
1. Веб-безопасность — XXE.	**3**	0	3	**3**	**0**
2. Текущий контроль успеваемости: практическое задание №1.	**4**	0	0	**0**	**4**
3. Веб-безопасность — небезопасная десериализация.	**5**	0	5	**5**	**0**
4. Текущий контроль успеваемости: практическое задание №2.	**8**	0	0	**0**	**8**
5. Веб-безопасность — template injection.	**3**	0	3	**3**	**0**
6. Ошибки неправильного использования криптографии в реальных приложениях.	**3**	0	3	**3**	**0**
7. Система типов в языке программирования Rust.	**3**	3	0	**3**	**0**
8. Фаззинг бинарных программ — основы	**3**	3	0	**3**	**0**
9. Текущий контроль успеваемости: практическое задание №3.	**6**	0	0	**0**	**6**

10. Фаззинг бинарных программ — примеры использования в реальной жизни.	**3**	3	0	**3**	**0**
11. Фаззинг бинарных программ — возникающие проблемы и способы их решения на основе специализированных фаззеров и техник: kAFL, Redqueen, Grimoire, etc	**3**	3	0	**3**	**0**
12. Текущий контроль успеваемости: практическое задание №4.	**6**	0	0	**0**	**6**
13. Веб-безопасность — атаки на race condition в веб-приложениях	**3**	3	0	**3**	**0**
14. Текущий контроль успеваемости: практическое задание №5.	**6**	0	0	**0**	**6**
15. Эскалация привилегий (LPE) в Windows	**3**	3	0	**3**	**0**
16. Текущий контроль успеваемости: практическое задание №6.	**6**	0	0	**0**	**6**
17. Внутреннее устройство WebAssembly и некоторые аспекты его безопасности	**3**	3	0	**3**	**0**
Итоговая аттестация: зачет	**1**	1	0	**1**	**0**
Итого	**72**	**36**	**0**	**36**	**36**

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

6.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

Практическое задание № 1

В наборе веб-приложений, содержащих уязвимость XXE различного вида, найти эту уязвимость и проэксплуатировать её, получив, в конечном итоге, данные, содержащиеся на сервере.

Практическое задание № 2

В наборе веб-приложений, содержащих уязвимости типа XXE, небезопасная десериализация, а также неправильное использование криптографии, найти эти уязвимости и проэксплуатировать их, получив, в конечном итоге, данные, содержащиеся на сервере.

Практическое задание № 3

В наборе программ на компилируемых языках найти уязвимости с помощью фаззинга бинарных программ.

Практическое задание № 4

В веб-приложении, содержащем уязвимость, вызванную ошибкой типа «race condition», найти эту уязвимость и использовать её для обхода ограничения числа попыток повторения бизнес-действия для пользователя.

Практическое задание № 4

В веб-приложении, содержащем уязвимость типа «template injection», найти эту уязвимость и проэксплуатировать её для того чтобы получить данные, содержащиеся на сервере.

Практическое задание № 6

Имея возможность исполнять код на системе под управлением ОС Windows, содержащей ошибки конфигурации и уязвимые программы, позволяющие повысить привилегии, осуществить повышение привилегий и считать данные из файла, чтение которого изначально недоступно для текущего пользователя.

6.2. Итоговый контроль успеваемости.
Проводится в форме зачета. Список вопросов:

1. Веб-безопасность, понятие атаки XXE.
2. Веб-безопасность — небезопасная десериализация.
3. Веб-безопасность — атака типа template injection.
4. Ошибки неправильного использования криптографии в реальных приложениях.
5. Система типов в языке программирования Rust.
6. Фаззинг бинарных программ: основные инструменты и подходы
7. Фаззинг бинарных программ — примеры использования в реальной жизни.

8. Фаззинг бинарных программ — возникающие проблемы и способы их решения на основе специализированных фаззеров и техник: kAFL, Redqueen, Grimoire, etc

9. Веб-безопасность — атаки на race condition в веб-приложениях

10. Эскалация привилегий (LPE) в Windows

11. Внутреннее устройство WebAssembly и некоторые аспекты его безопасности

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)				
Оценка РО и соответствующие виды оценочных средств	2	3	4	5
Знания *Экзамен*	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения *Самостоятельные работы, 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) *Экзамен*	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
Соответствие результатов обучения и компетенций, в развитии которых участвует дисциплина (модуль)				
Результаты обучения				Компетенция, с частичным формированием которой связано достижение результата обучения

Знать: 1. ряд сложных уязвимостей в приложениях, причины их возникновения; 2. основные техники поиска уязвимостей в бинарных программах с помощью фаззинга; 3. базовые механизмы привилегий в ОС Windows, принипы, лежащие в основе техник их обхода и ряд существующих техник. **Уметь:** 1. эксплуатировать ряд сложных уязвимостей в приложениях; 2. применять фаззинг бинарных программ для поиска уявзимостей; 3. искать способы эскалации привилегий на системе под управлением ОС Windows и использовать их. **Владеть:** 1. навыками поиска сложных уязвимостей (в т. ч. с помощью фаззинга бинарных программ), определения их причин и их эксплуатации 2. навыками эскалации привилегий на системах под управлением ОС Windows.	СПК-ДГПБ-1.А СПК-ДГПБ-1.Б СПК-ДГПБ-1.В

7. Ресурсное обеспечение:
7.1. Перечень основной и дополнительной литературы

Основная литература

1. Джон Эриксон: Хакинг. Искусство эксплойта. СПб: Питер, 2018.

Дополнительная литература

2. Michał Zalewski. The Tangled Web: A Guide to Securing Modern Web Applications
3. Michał Zalewski. Binary fuzzing strategies: what works, what doesn't
4. Timur Yunusov, Alexey Osipov. XML data retrieval

5. Rob J. van Emous. Towards Systematic Black-Box Testing for Exploitable Race Conditions in Web Apps
6. Sergej Schumilo, Cornelius Aschermann, and Robert Gawlik, Thorsten Holz. kAFL: Hardware-Assisted Feedback Fuzzing for OS Kernels
7. James Forshaw. Between a Rock and a Hard Link
8. Intel PT: Intel 64 and IA-32 Architectures Software Developer's Manual, Volume 3 (3A, 3B, 3C & 3D),

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

При реализации дисциплины может быть использовано следующее программное обеспечение:

Программное обеспечение для подготовки слайдов лекций MS PowerPoint, MS Word
Программное обеспечение для создания и просмотра pdf-документов Adobe Reader
Издательская система LaTeX
Язык программирования Python и среда разработки Jupiter Notebook (вместе с библиотеками numpy, scikit-learn, pandas)
Язык программирования R и среда разработки R Studio

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.

Сигалов Даниил Алексеевич.

10. Язык преподавания - русский.