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 /**

**«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Наименование дисциплины:**

**Безопасность программного обеспечения и сетей**

**Уровень высшего образования:**

**бакалавриат**

**Направление подготовки / специальность:**

**01.03.02 «Прикладная математика и информатика» (3++)**

**Направленность (профиль):**

**Математические методы обработки информации и принятия решений**

**Форма обучения:**

**очная**

**Москва 2023**

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 01.03.02, 01.04.02 "Прикладная математика и информатика" программы бакалавриата Утвержден приказом МГУ от 30 августа 2019 года № 1041 (в редакции приказов МГУ от 11 сентября 2019 года № 1109, от 10 июня 2021 года № 609, от 7 октября 2021 года № 1048, от 21 декабря 2021 года № 1404, от 2 ноября 2022 года № 1299)

**1.** Дисциплина относится к базовой части ОПОП ВО(*или к вариативной части ОПОП ВО, или является факультативом)*.

**2.** Входные требования для освоения дисциплины (модуля): учащиеся должны владеть знаниями поИнформационная безопасность компьютерных систем в объеме, соответствующем программе третьего года обучения основных образовательных программ бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки», 01.04.02 «Прикладная математика и информатика».

**3.** Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников*.*

Компетенции выпускников, частично формируемые при реализации дисциплины (модуля):

* **СПК-БПОС-1.Б.**Способность анализировать современное программное обеспечение, а также современные компьютерные сети, на предмет наличия или отсутствия уязвимостей, реализация которых приводит к нарушению безопасного их функционирования.

Планируемые результаты обучения по дисциплине (модулю):

**Знать:**

1. основные понятия, определения и факты безопасности программного обеспечения и сетей;
2. основные понятия локальных вычислительных сетей;
3. основные понятия стека TCP/IPи модели OSI;
4. основы теории и стандартные методы программирования на языках C/C++/Python.

**Уметь:**

1. извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов;
2. демонстрировать способность к анализу и синтезу;
3. демонстрировать способность к письменному и устному общению на русском языке;
4. публично представить собственные и известные научные результаты;
5. разрабатывать программные модули на языках C/C++/Python.

**Владеть:**

1. методами использования теории построения политик безопасности компьютерных систем;
2. проведения анализа угроз и поиска уязвимостей в компьютерных системах.

**4.** Формат обучения: занятия проводятся с использованием меловой или маркерной доски, интерактивные материалы демонстрируются с помощью ноутбука и проектора.

**5.** Объем дисциплины (модуля) составляет 3 з.е., в том числе 52 академических часа, отведенных на контактную работу обучающихся с преподавателем, 56 академических часов на самостоятельную работу обучающихся.

**6.**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** |
| Занятия лекционного типа\* | Занятия семинарского типа\* | **Всего** |
| 1. Основные понятия безопасности программного обеспечения. Обзор современных средств дизассемблирования и отладки программного обеспечения (WinDbg, IDA, ImmunityDbg). Обзор современных средств анализа сетевого трафика WireShark, Fiddler. Основные понятия и современные методы расшифровкиSSL-трафика. | **30** | 10 | 10 | **20** | **10** |
| 1. Атаки на сетевые протоколы канального и сетевого уровней. Обзор протоколов ARP, IP, DNS и их основных характеристик. Атаки типа «человек посередине» с помощью DNS/ARP-спуфинга. Обзор протоколов http,httpsи их основных характеристик. Атаки типа «человек посередине» с помощью на SSL-трафик на примере облачных протоколов. | **12** | 4 | 4 | **8** | **4** |
| 1. Обзор программных агентов (закладок) для демонстрации атак скрытого удаленного управления ОС на примере известных вредоносных программ. Атаки типа reverse-proxy. | **12** | 4 | 4 | **8** | **4** |
| 1. Уязвимости программного обеспечения. Эксплоиты (exploit). Современные среды раз-работки уязвимостей и исследования программ-ного обеспечения (Metasploit FW).Атаки на программное обеспечение типа «переполнение буфера» (overflow). Методы фаззинга и поиск уязвимостей. ФаззингCom-объектов с помощью ПО COMRaider. | **24** | 8 | 8 | **16** | **8** |
| 1. Текущий контроль успеваемости: практическое контрольное задание | **10** | 0 | 0 | **0** | **10** |
| Промежуточная аттестация: устный экзамен | **20** | 0 | 0 | **0** | **20** |
| **Итого** | **108** | 26 | 26 | **52** | **56** |

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

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

|  |  |
| --- | --- |
| **Зачетная работа** | |
| **Вариант 1** | **Вариант 2** |
| 1. Перехват зашифрованного трафика с помощью Fiddler на этапе авторизации по протоколу oauth 2.0.  2. Эксплуатация существующих уязвимостей с помощью MetasploitFramework.  3. Анализ приложения с помощью WinDbg, IdaPro.  4. Анализ трафикас помощьюWireShark. | 1. Разработка приложения win32 consoleapplication с уязвимостью переполнения стека, разработка эксплоита типа переполнения стека.  2. Разработка приложения win32 consoleapplication с уязвимостью переполнения обработчика исключений, разработка эксплоита типа переполнения обработчика исключений на стеке. |
| **Вариант 3** |  |
| 1. Использование фаззинга для поиска уязвимостей в существующем ПО или собственномс помощью ComRaider.  2. Обфускация бинарного шеллкодасредствами MetasploitFramework.  3. Нахождение возможностей передачи управления. |  |

**Вопросы к экзамену.**

Вредоносное программное обеспечение. Среда исполнения программного обеспечения (включая сетевое ПО) в ОС Windows. Интерфейс системных вызовов.

Отладка и дизассемблирование программного обеспечения. Современные средства отладки.

Средства разработки способов эксплуатации уязвимостей.

Уязвимость программного обеспечения. Эксплоит. Типы эксплоитов.

Атаки типа «переполнение буфера».

Атаки типа «модификации обработчика исключений».

ФаззингCom-объектов.

**Типовые задачи для экзамена.**

Поиск уязвимостей (методом фаззинга и реверсинжиниринга) и разработка средств демонстрации их эксплуатации.

Выбирается или разрабатывается пример программного обеспечения с уязвимостями типа переполнения или спрея и механизмами защиты. Требуется провести фаззинг и реверсинг программного обеспечения и найти условия эксплуатации уязвимости (отказ в обслуживании). Затем необходимо разработать систему передачи управления от уязвимого компонента на полезную нагрузку. Провести анализ и разбор сетевого трафика с целью поиска авторизационных данных.

**Экзаменационный билет** состоит из двух вопросов, например

1. Уязвимость программного обеспечения. Эксплоит. Типы эксплоитов.
2. Атаки типа «человек посередине».
3. Расшифровка SSLтрафика с помощью атаки типа «человек посередине».

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 знанияоб основных инструментах, потенциальных возможностях и особенностях применения современных средств поиска уязвимостей | Общие, но не структурированные знанияоб основных инструментах, потенциальных возможностях и особенностях применения современных средств поиска уязвимостей | Сформированные систематические знания об основных инструментах, потенциальных возможностях и особенностях применения современных средств поиска уязвимостей |
| **Умения**  *Экзамен*  *(и/или написание и защита рефератов на заданную тему и т.п.)* | Отсутствие умений | В целом успешное, но не систематическое умениерешать задачи в области обнаружения существующих уязвимостей и способов их эксплуатации | В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера)решать задачи в области обнаружения существующих уязвимостей и способов их эксплуатации | Успешное и систематическое умениерешать задачи в области обнаружения существующих уязвимостей и способов их эксплуатации |
| **Навыки  (владения, опыт деятельности)**  *Экзамен*  *(и/или и т.п.)* | Отсутствие навыков (владений, опыта) | Наличие отдельных навыков (наличие фрагментарного опыта)навыками выбора инструментов для поиска новых уязвимостей, созданием средств их апробации и противодействия | В целом, сформированные навыки (владения), но используемые не в активной форменавыками выбора инструментов для поиска новых уязвимостей, созданием средств их апробации и противодействия | Сформированные навыки (владения), применяемые при решении задачнавыками выбора инструментов для поиска новых уязвимостей, созданием средств их апробации и противодействия |

|  |  |
| --- | --- |
| **Соответствие результатов обучения и компетенций, в развитии которых участвует дисциплина (модуль)** | |
| Результаты обучения | Компетенция, с частичным формированием которой связано достижение результата обучения |
| **Знать:**   1. основной набор инструментов, потенциальные возможности и особенности применения современных средств поиска уязвимостей и анализа вредоносного кода.   **Уметь:**   1. решать базовые задачи по анализу программного обеспечения с целью поиска существующих уязвимостей и разработки средств демонстрации их эксплуатации.   **Владеть:**   1. навыками применения атаки типа «человек посередине» для воздействия на сетевой трафика | СПК-БПОС-1.Б**.** |

**8. Ресурсное обеспечение**:

Основная литература:

1. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. Учебное пособие. М.: Академия, 2009.

Дополнительная литература:

1. Олифер В.Г., Олифер Н.А. Основы компьютерных сетей. Учебное пособие. СПб.: Питер, 2009.
2. М. Руссинович, Д. Соломон. Внутреннее устройство MicrosoftWindows, 6-е издание (Часть 1). СПб.: Питер, 2013.
3. М. Руссинович, Д. Соломон, А. Ионеску. Внутреннее устройство MicrosoftWindows, 6-е издание (Часть 2). Основные подсистемы ОС. СПб.: Питер, 2014.

Информационные справочные системы:

1. corelan.be
2. reverse4you.com
3. cve-details.com
4. openrce.org
5. rapid7.com
6. github.com (rapid7 – msf)

Материально-техническое обеспечение: аудитория с партами, меловой или маркерной доской.

ПЭВМ под управлением ОС Windows 7, VMware player, IDA pro

9. Язык преподавания - русский.

10. Преподаватели: преподаватель ВМК МГУ М.В. Левыкин.

11. Авторы программы: преподаватель ВМК МГУ М.В. Левыкин.