Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б4.Ч.05**
Трудоемкость в зачетных единицах:	**6 семестр - 2;**
Часов (всего) по учебному плану:	**72 часа**
Лекции	**6 семестр - 14 часов;**
Практические занятия	**6 семестр - 14 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**6 семестр - 43,7 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Контрольная работа**	
Промежуточная аттестация:	
Зачет	**6 семестр - 0,3 часа;**

Москва 2021

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: получение знаний и навыков в области выбора и применения технологий обнаружения уязвимостей в автоматизированных системах хозяйствующего субъекта

Задачи дисциплины

- сформировать представление о существующих подходах к обнаружению уязвимостей в операционных системах и прикладных программных продуктах, установленных в автоматизированных системах;
- определить критерии выбора технологии обнаружения уязвимостей для типовых автоматизированных систем.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ОПК-2 способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ИД-2$_{ОПК-2}$ Применяет программно-аппаратные средства и средства системного назначения, инструментальные средства, в том числе отечественного производства для решения профессиональных задач	знать: - типовые уязвимости операционных систем и прикладных программных продуктов; - критерии выбора и порядок применений технологий обнаружения уязвимостей в автоматизированных системах.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам основной профессиональной образовательной программе Безопасность компьютерных систем (продвинутый уровень) (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Подготовительный этап исследования автоматизированной системы на наличие уязвимостей информационной безопасности	34	6	7	-	7	-	-	-	-	-	20	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Подготовительный этап исследования автоматизированной системы на наличие уязвимостей информационной безопасности" ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Подготовительный этап исследования автоматизированной системы на наличие уязвимостей информационной безопасности" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Подготовительный этап исследования автоматизированной системы на наличие уязвимостей информационной безопасности" ***Изучение материалов литературных***
1.1	Порядок сбора данных об уязвимостях автоматизированных систем и создания триаж-копий	4		1	-	1	-	-	-	-	-	2	-	
1.2	Анализ артефактов журналов событий, реестра и файловой системы	4		1	-	1	-	-	-	-	-	2	-	
1.3	Подходы к анализу вредоносного кода в процессе обратной разработки	4		1	-	1	-	-	-	-	-	2	-	
1.4	Динамический и статический анализ вредоносного кода, используемый специалистами по информационной безопасности	4		1	-	1	-	-	-	-	-	2	-	

1.5	Особенности анализа и толкования информации из открытых источников с целью формулирования гипотез и выявления деятельность злоумышленников	6		1	-	1	-	-	-	-	-	4	-	***источников:*** [1], 33-62 [2], 249-529
1.6	Порядок идентификации следов инцидентов ИБ в журналах событий Windows.	6		1	-	1	-	-	-	-	-	4	-	
1.7	Обзор средств защиты ядра Linux	6		1	-	1	-	-	-	-	-	4	-	
2	Порядок обнаружения уязвимостей в автоматизированных системах и подходы к их устранению	37.7		7	-	7	-	-	-	-	-	23.7	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Порядок обнаружения уязвимостей в автоматизированных системах и подходы к их устранению" ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка к контрольной работе:*** Изучение материалов по разделу Порядок обнаружения уязвимостей в автоматизированных системах и подходы к их устранению и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Порядок обнаружения уязвимостей в
2.1	Оценка уровня защищенности наиболее распространённых операционных систем	4		1	-	1	-	-	-	-	-	2	-	
2.2	Общая характеристика уязвимостей системного программного обеспечения операционных систем	4		1	-	1	-	-	-	-	-	2	-	
2.3	Программные решения для обнаружения уязвимостей в операционных системах	5		1	-	1	-	-	-	-	-	3	-	

2.4	Перечень наиболее опасных слабых мест программного обеспечения по данным CWE	6		1	-	1	-	-	-	-	-	4	-	автоматизированных системах и подходы к их устранению" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Порядок обнаружения уязвимостей в автоматизированных системах и подходы к их устранению" ***Изучение материалов литературных источников:*** [1], 15-31
2.5	Изучение подхода к эксплуатации уязвимостей Stack Buffer Overflow и UAF.	6		1	-	1	-	-	-	-	-	4	-	
2.6	Методы и алгоритмы управления задачами, процессами, памятью и внешними устройствами	6		1	-	1	-	-	-	-	-	4	-	
2.7	Комплексный подход к выбору технологий обнаружения уязвимостей в автоматизированных системах	6.7		1	-	1	-	-	-	-	-	4.7	-	
	Зачет	0.3		-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	**72.0**		**14**	**-**	**14**	**-**	**-**	**-**	**-**	**0.3**	**43.7**	**-**	
	Итого за семестр	**72.0**		**14**	**-**	**14**	**-**		**-**		**0.3**	**43.7**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Подготовительный этап исследования автоматизированной системы на наличие уязвимостей информационной безопасности

1.1. Порядок сбора данных об уязвимостях автоматизированных систем и создания триаж-копий

Понятие триаж-копии. Классификация этапов сбора данных об уязвимостях. Программные продукты для автоматизации части процессов сбора исходных данных для анализа уязвимостей.

1.2. Анализ артефактов журналов событий, реестра и файловой системы

Порядок выборки данных из различных источников с использованием встроенных в операционную систему инструментов. Платные и самописные программные решения для анализа исходных данных об уязвимости.

1.3. Подходы к анализу вредоносного кода в процессе обратной разработки

Понятие "обратной разработки". Принципы реверс инжиниринга программного обеспечения.

1.4. Динамический и статический анализ вредоносного кода, используемый специалистами по информационной безопасности

Отличия динамического и статистического анализа кода. Программные продукты, используемые для динамического и статистического анализа кода.

1.5. Особенности анализа и толкования информации из открытых источников с целью формулирования гипотез и выявления деятельность злоумышленников

Понятие "гипотезы" в сфере проведения расследования инцидента информационной безопасности и обнаружения уязвимостей в автоматизированных системах.

1.6. Порядок идентификации следов инцидентов ИБ в журналах событий Windows.

Работа с встроенными в ОС Windows инструментами для анализа уязвимостей в автоматизированных системах.

1.7. Обзор средств защиты ядра Linux

Работа с встроенными в ОС Linux инструментами для анализа уязвимостей в автоматизированных системах.

2. Порядок обнаружения уязвимостей в автоматизированных системах и подходы к их устранению

2.1. Оценка уровня защищенности наиболее распространённых операционных систем

Анализ статистических данных по уязвимостям, обнаруженным в операционных системах, в базах данных CWE и CVE.

2.2. Общая характеристика уязвимостей системного программного обеспечения операционных систем

Различие структуры и особенностей написания системных и прикладных программных продуктов. Классификация типовых уязвимостей для каждого из видов программного обеспечения.

2.3. Программные решения для обнаружения уязвимостей в операционных системах

Краткая характеристика платных, бесплатных и самописных программных решений для обнаружения уязвимостей в автоматизированных системах.

2.4. Перечень наиболее опасных слабых мест программного обеспечения по данным CWE

Структура базы данных CWE. Анализ уязвимых компонентов программного обеспечения на основе годовых отчётов CWE.

2.5. Изучение подхода к эксплуатации уязвимостей Stack Buffer Overflow и UAF.

Разбор порядка анализа уязвимостей в программном продукте на примере UAF.

2.6. Методы и алгоритмы управления задачами, процессами, памятью и внешними устройствами

Взаимосвязь уязвимостей в программном коде прикладных программных продуктов и системного программного обеспечения нижних уровней операционной системы.

2.7. Комплексный подход к выбору технологий обнаружения уязвимостей в автоматизированных системах

Структурирование программных решений, применяемых для обнаружения уязвимостей в автоматизированных системах, по виду операционной системы и критерию эффективности.

3.3. Темы практических занятий

1. Принципы использования IoC для создания YARA-правил в рамках мероприятий по реагированию на инциденты ИБ;
2. Реконструкция действий атакующего и набор индикаторов компрометации для типовой автоматизированной системы;
3. Базовое представление о языке ассемблер и порядок чтения исполняемого кода;
4. Работа с песочницами и базовая детонация вредоносного кода в виртуальных машинах. инструменты, используемые для статического анализа и обратной разработки, в частности IDA Pro;
5. Тестирование гипотез в рамках threat hunting с использованием матрицы MITRE ATT&CK;
6. Обзор LOLBAS и Sysmon для организации процесса журналирования в процессе охоты за угрозами;
7. Построение Linux Kernel Defence Map для систематизации уязвимостей ОС;
8. Расчёт вероятности появления отказов и сбоев в работе операционной системы;
9. Использование сканеров безопасности для обнаружения уязвимостей в операционных системах;
10. Подходы к использованию NGFW, SIEM, NTA, EDR, NDR, Threat Intelligence и Threat hunting для обнаружения уязвимостей ОС;
11. Проблемы безопасной разработки программного обеспечения на различных языках программирования.;
12. Особенности уязвимости типа UAF и понятие уязвимого приложения;
13. Безопасность операционной системы на примере Astra Linux Special Edition;
14. Характеристика направлений развития специалиста в области анализа уязвиостей операционных систем.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Подготовительный этап исследования автоматизированной системы на наличие уязвимостей информационной безопасности"
2. Обсуждение материалов по кейсам раздела "Порядок обнаружения уязвимостей в автоматизированных системах и подходы к их устранению"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Подготовительный этап исследования автоматизированной системы на наличие уязвимостей информационной безопасности"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Порядок обнаружения уязвимостей в автоматизированных системах и подходы к их устранению"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)		Оценочное средство (тип и наименование)
		1	2	
Знать:				
критерии выбора и порядок применений технологий обнаружения уязвимостей в автоматизированных системах	ИД-2$_{ОПК-2}$	+		Контрольная работа/Контрольное мероприятие № 1 Контрольная работа/Контрольное мероприятие № 2
типовые уязвимости операционных систем и прикладных программных продуктов	ИД-2$_{ОПК-2}$		+	Контрольная работа/Контрольное мероприятие № 3

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

6 семестр

Форма реализации: Письменная работа

1. Контрольное мероприятие № 1 (Контрольная работа)
2. Контрольное мероприятие № 2 (Контрольная работа)
3. Контрольное мероприятие № 3 (Контрольная работа)
4. Контрольное мероприятие № 3 (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет (Семестр №6)

Оценка проставляется по результатам ответа на вопрос билета. Результаты контрольных мероприятий № 1, 2, 3, 4 учитываются.

В диплом выставляется оценка за 6 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Управление событиями информационной безопасности : учебное пособие / А. С. Минзов, О. Р. Баронов, С. А. Минзов, П. А. Осипов, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ" ; ред. А. Ю. Невский . – Москва : ВНИИгеосистем, 2020 . – 110 с. - Для студентов бакалавриата, магистратуры, аспирантов и преподавателей, занимающихся вопросами создания эффективных систем управления кибербезопасностью . - ISBN 978-5-8481-0244-4 .;
2. Диогенес Ю., Озкайя Э.- "Кибербезопасность. стратегия атак и обороны", Издательство: "ДМК Пресс", Москва, 2020 - (326 с.)
https://e.lanbook.com/book/131717.

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции;
5. Windows Server / Серверная операционная система семейства Linux;
6. Kali Linux.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. **ЭБС Лань** - https://e.lanbook.com/

2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **Электронные ресурсы издательства Springer** - https://link.springer.com/
5. **База данных Web of Science** - http://webofscience.com/
6. **База данных Scopus** - http://www.scopus.com
7. **Национальная электронная библиотека** - https://rusneb.ru/
8. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
9. **Журнал Science** - https://www.sciencemag.org/
10. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
11. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
12. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
13. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
14. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
15. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	М-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная	стол преподавателя, стол

	лаборатория "Информационно-аналитические технологии"	компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Технологии обнаружения уязвимостей в автоматизированных системах

(название дисциплины)

6 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 Контрольное мероприятие № 1 (Контрольная работа)
КМ-2 Контрольное мероприятие № 2 (Контрольная работа)
КМ-3 Контрольное мероприятие № 3 (Контрольная работа)
КМ-4 Контрольное мероприятие № 3 (Контрольная работа)

Вид промежуточной аттестации – Зачет.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	14
1	Подготовительный этап исследования автоматизированной системы на наличие уязвимостей информационной безопасности					
1.1	Порядок сбора данных об уязвимостях автоматизированных систем и создания триаж-копий		+	+		
1.2	Анализ артефактов журналов событий, реестра и файловой системы		+	+		
1.3	Подходы к анализу вредоносного кода в процессе обратной разработки		+	+		
1.4	Динамический и статический анализ вредоносного кода, используемый специалистами по информационной безопасности		+	+		
1.5	Особенности анализа и толкования информации из открытых источников с целью формулирования гипотез и выявления деятельность злоумышленников		+	+		
1.6	Порядок идентификации следов инцидентов ИБ в журналах событий Windows.		+	+		
1.7	Обзор средств защиты ядра Linux		+	+		
2	Порядок обнаружения уязвимостей в автоматизированных системах и подходы к их устранению					
2.1	Оценка уровня защищенности наиболее распространённых операционных систем				+	+
2.2	Общая характеристика уязвимостей системного программного обеспечения операционных систем				+	+
2.3	Программные решения для обнаружения уязвимостей в операционных системах				+	+
2.4	Перечень наиболее опасных слабых мест программного обеспечения по данным CWE				+	+

2.5	Изучение подхода к эксплуатации уязвимостей Stack Buffer Overflow и UAF.			+	+
2.6	Методы и алгоритмы управления задачами, процессами, памятью и внешними устройствами			+	+
2.7	Комплексный подход к выбору технологий обнаружения уязвимостей в автоматизированных системах			+	+
	Вес КМ, %:	25	25	25	25