МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Инструментальные средства анализа защищённости и управления уязвимостями»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

Преподаватель  /Г.Ф. Шипулин/

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность»,  А.Ю. Гневшев

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

Целью преподавания дисциплины является формирование у студентов знаний в области инструментальных средств анализа защищенности и управления уязвимостями.
Задачи преподавания дисциплины:

- изучение методы и средства контроля эффективности технической защиты информации;
- освоение способов выбора и обоснования критериев эффективности функционирования защищенных информационных систем;
- освоение способов и средств участия в экспертизе состояния защищенности информации на объекте защиты;
- освоение средств контроля эффективности принятых мер по реализации частных политик информационной безопасности информационных систем.

В результате освоения дисциплины «Анализ защищенности систем» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:
знать:
- методы и средства контроля эффективности технической защиты информации;
уметь:
- контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем;
владеть:
- навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем, навыками участия в экспертизе состояния защищенности информации на объекте защиты.

Обучение по дисциплине «Анализ защищенности систем» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;	ИПК-3.1. Знает методы и средства контроля эффективности технической защиты информации; ИПК-3.2. Умеет контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; ИПК-3.3. Владеет навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем, навыками участия в экспертизе состояния защищенности информации на объекте защиты.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Инструментальные средства анализа защищённости и управления уязвимостями» относится к числу профессиональных учебных дисциплин части, формируемой участниками образовательных отношений (Б1.2) основной образовательной программы (Б1.2.2).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы проектирования информационных систем», «Введение в аналитику информационной безопасности», «Анализ защищенности систем».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, т.е. 216 часов (лекции – 36 часов, лабораторные занятия – 72 часа, самостоятельная работа - 108 часов, форма контроля – экзамен) в 6 семестре.
Структура и содержание дисциплины «Инструментальные средства анализа защищённости и управления уязвимостями» по срокам и видам работы отражены в п. 3.2.

3.1Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			6	
1	**Аудиторные занятия**	**108**	108	
	В том числе:			
1.1	Лекции	36	36	
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	72	
2	**Самостоятельная работа**	**108**	108	
	В том числе:			
2.1	…			
3	**Промежуточная аттестация**			
	Зачет/диф.зачет/экзамен		Экзамен	
	Итого	**216**		

3.1.2 Очно-заочная форма обучения
Не предусмотрена

3.1.3 Заочная форма обучения
Не предусмотрена

3.2 Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	

1	Раздел 1.						
1.1	Тема 1. Основные концепции, техники и инструменты для проведения анализа защищенности и управления уязвимости.	56	12		16		28
1.2	Тема 2. Анализ защищенности и тестирование на проникновение Windows систем.	124	18		44		62
1.3	Тема 3. Анализ защищенности и тестирование на проникновение Linux систем.	20	4		6		10
1.4	Тема 4. Цифровые сертификаты безопасности.	16	2		6		8
	Итого	**216**	**36**		**72**		**108**

3.2.2 Очно-заочная форма обучения
Не предусмотрена.

3.2.2 Заочная форма обучения
Не предусмотрена

3.3. Содержание дисциплины

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Раздел 1	
1.1	Основные концепции, техники и инструменты для проведения анализа защищенности и управления уязвимости.	Введение в тестирование на проникновение и анализ защищенности. Инструментарий для проведения анализа защищенности информационных систем. Классификация сетевых атак. Пассивные сетевые атаки. Анализ сетевого трафика. Активные сетевые атаки: ARP, DNS, DHCP-spoofing. Активные сетевые атаки: bruteforce, DoS, DDoS. Metasploit Framework: структура, команды. Metasploit Framework: полезная нагрузка, управление модулями, получение удаленного доступа. Metasploit Framework: способы внедрения, модификации и детектирования вредоносного кода в файлах. Механизмы аутентификации ОС, способы их обхода и восстановления паролей. Автоматизированные средства поиска уязвимостей: OpenVas, nmap nse.
1.2	Анализ защищенности и тестирование на проникновение Windows систем.	PowerShell: область применения, команды и переменные, объекты. PowerShell: структуры данных, условные операторы и циклы. PowerShell: функции, работа с модулями. PowerShell: способы локального и удаленного запуска сценариев. Анализ структур PE-файла и процесса, основные элементы исполняющей подсистемы. Разграничение доступа к ресурсам, сбор информации о системе и пользователях. Этапы тестирования на

		проникновение систем под управлением Windows AD. Классификация атак на AD: проблемы делегирования, использование GPO. Классификация атак на AD: уязвимости протоколов.
1.3	Анализ защищенности и тестирование на проникновение Linux систем.	Методы и способы сбора учетных данных в Linux. Способы эксплуатации уязвимостей ядра и служб в Linux, методы защиты. Способы эксплуатации уязвимостей типа security misconfiguration, методы защиты. Уязвимость библиотеки журналирования log4j: способы эксплуатации и ее закрытия. Настройка расширения системы мониторинга zabbix, ее использование в качестве системы управления уязвимости.
1.4	Цифровые сертификаты безопасности.	PKI: понятие, структура, жизненный цикл сертификата. PKI: создание УЦ, выпуск, отзыв, проверка подлинности сертификатов.

3.4Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

№	Наименование лабораторной работы	Объем, час.
1	Выполнение лабораторной работы №1	16
2	Выполнение лабораторной работы №2	14
3	Выполнение лабораторной работы №3	14
4	Выполнение лабораторной работы №4	16
5	Выполнение лабораторной работы №5	6
6	Выполнение лабораторной работы №6	6
Итого		72

3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по данной дисциплине учебным планом не запланировано.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров 10.05.03 «Информационная безопасность».

4.2 Основная литература

1. «Основы управления информационной безопасностью» (Мошак, Н. Н. Основы управления информационной безопасностью : учебное пособие / Н. Н. Мошак ; под редакцией В. В. Овчинникова. — Санкт-Петербург : ГУАП, 2022. — ISBN 978-5-8088-1711-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/340967
2. «Разработка защищенных программных средств информатизации производственных процессов предприятия» (Бабушкин, В. М. Разработка защищенных программных средств информатизации производственных процессов предприятия : учебное пособие / В. М. Бабушкин. — Казань : КНИТУ-КАИ, 2020. — ISBN 978-5-7579-2463-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/193486
3. «Основы технической эксплуатации защищенных телекоммуникационных систем» (Крыжановский, А. В. Основы технической эксплуатации защищенных телекоммуникационных систем : методические указания / А. В. Крыжановский. — Самара : ПГУТИ, 2021. — 50 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/301133

4.3 Дополнительная литература

1. «Базовые принципы информационной безопасности вычислительных систем» (Базовые принципы информационной безопасности вычислительных систем : учебное пособие / А. А. Гладких, Д. В. Ганин, С. В. Кривоногов [и др.]. — Нижний Новгород : НГИЭУ, 2015. — ISBN 978-5-91592-067-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/330293
2. Колегов, Д. Н. Лабораторный практикум по основам построения защищенных компьютерных сетей : учебное пособие / Д. Н. Колегов. — Томск : ТГУ, 2013. — 140 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/44913

4.4 Электронные образовательные ресурсы

1. ЭОР «Инструментальные средства анализа защищённости и управления уязвимостями» [Электронный ресурс] — URL: https://online.mospolytech.ru/course/view.php?id=10268 (дата обращения: 18.02.2023).

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Virtual Box
2. Виртуальная машина Metasploitable3
3. Дистрибутив ОС Kali Linux
4. Дистрибутив ОС Windows Server 2012/2016

5. Дистрибутив ОС Windows 7, 10

4.6 Современные профессиональные базы данных и информационные справочные системы

1. БДУ ФСТЭК [Электронный ресурс] — URL: https://bdu.fstec.ru/ (дата обращения: 18.02.2023).
2. CVE [Электронный ресурс] — URL: https://www.cve.org/ (дата обращения: 18.02.2023).

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6 Методические рекомендации

6.1Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.
2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической и практической подготовки студентов являются лекции и лабораторные работы.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

7 Фонд оценочных средств

7.1Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

7.2Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.
По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Текущий контроль
Оценочные средства для текущей аттестации
- Защита отчетов о выполнении лабораторных работ

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации
- Экзамен

Список вопрос для проведения экзамена по дисциплине:
1 Введение в тестирование на проникновение и анализ защищенности.
2. Инструментарий для проведения анализа защищенности информационных систем.
3. Классификация сетевых атак. Пассивные сетевые атаки.
4. Анализ сетевого трафика.
5. Активные сетевые атаки: ARP, DNS, DHCP-spoofing.
6. Активные сетевые атаки: bruteforce, DoS, DDoS.
7. Metasploit Framework: структура, команды.
8. Metasploit Framework: полезная нагрузка, управление модулями, получение удаленного доступа.
9. Metasploit Framework: способы внедрения, модификации и детектирования вредоносного кода в файлах.
10. Механизмы аутентификации ОС, способы их обхода и восстановления паролей.
11. Автоматизированные средства поиска уязвимостей: OpenVas, nmap nse.
12. PowerShell: область применения, команды и переменные, объекты.
13. PowerShell: структуры данных, условные операторы и циклы.
14. PowerShell: функции, работа с модулями.
15. PowerShell: способы локального и удаленного запуска сценариев.
16. Анализ структур PE-файла и процесса, основные элементы исполняющей подсистемы. Разграничение доступа к ресурсам, сбор информации о системе и пользователях.
17. Этапы тестирования на проникновение систем под управлением Windows AD.
18. Классификация атак на AD: проблемы делегирования, использование GPO.
19. Классификация атак на AD: уязвимости протоколов.
20. Методы и способы сбора учетных данных в Linux.
21. Способы эксплуатации уязвимостей ядра и служб в Linux, методы защиты.
22. Способы эксплуатации уязвимостей типа security misconfiguration, методы защиты.
23. Уязвимость библиотеки журналирования log4j: способы эксплуатации и ее закрытия.
24. Настройка расширения системы мониторинга zabbix, ее использование в качестве системы управления уязвимости.
25. PKI: понятие, структура, жизненный цикл сертификата.
26. PKI: создание УЦ, выпуск, отзыв, проверка подлинности сертификатов.

Пример билета.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий
Кафедра: Информационная безопасность
Дисциплина: Инструментальные средства анализа защищённости и управления уязвимостями
Бакалавры. Курс 3, семестр 2

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. PKI: понятие, структура, жизненный цикл сертификата.
2. Активные сетевые атаки: ARP, DNS, DHCP-spoofing.

Преподаватель _____ / Шипулин Г.Ф. /