МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины
Системы автоматизации деятельности центров обеспечения компьютерной безопасности

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Дисциплина «Системы автоматизации деятельности центров обеспечения компьютерной безопасности» имеет целью ознакомить обучающегося с порядком организации работ в центрах обеспечения компьютерной безопасности, а также позволяет приобрести основные навыки по работе с техническими средствами обнаружения и реагирования на инциденты информационной безопасности.

Дисциплина обеспечивает приобретение основных знаний, умений и навыков в области обеспечения информационной безопасности, способствует освоению принципов корректного применения современных средств и методов защиты информации, обнаружения и реагирования на компьютерные инциденты.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к обязательной части образовательной программы.

Для ее успешного освоения обучающиеся должны обладать знаниями операционных систем, вычислительных сетей, а также основных методов их защиты, иметь базовые навыки по администрированию вычислительных сетей и средств защиты информации, в том числе опытом администрирования систем журналирования.

Для успешного освоения дисциплины «Методы Системы автоматизации деятельности центров обеспечения компьютерной безопасности» ей должны предшествовать следующие дисциплины:

- «Основы информационной безопасности»;
- «Операционные системы»;
- «Безопасность операционных систем»;
- «Компьютерные сети»;
- «Сети и системы передачи информации»;
- «Безопасность компьютерных сетей».

Дисциплина «Системы автоматизации деятельности центров обеспечения компьютерной безопасности» является предшествующей для прохождения производственной и преддипломной практики и итоговой государственной аттестации.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Общепрофессиональные компетенции		
ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	И-ОПК-11.5 Способен разрабатывать политики управления информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	Знает: - терминологию в области защиты информации от несанкционированного доступа; - угрозы безопасности информации в информационных системах; - современные технологии защиты информации в области обнаружения и реагирования на инциденты информационной безопасности; Умеет: - разрабатывать политики управления информационными потоками в компьютерных системах.
	И-ОПК-11.6 Способен обеспечивать контроль информационных потоков в компьютерных системах	Умеет: - устанавливать, настраивать, тестировать и отлаживать программные и программно-аппаратные средства защиты информации в области обнаружения и реагирования на инциденты информационной безопасности.
ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	И- ОПК-16.4 Способен проводить анализ эффективности средств защиты информации в компьютерных системах и сетях	Знает: - требования к работоспособности и надежности систем защиты информации в области обнаружения и реагирования на инциденты информационной безопасности. Умеет: - проводить анализ эффективности средств защиты информации в компьютерных системах и сетях
	И-ОПК-16.5 Способен анализировать события информационной безопасности	Владеет: - навыками анализа событий информационной безопасности.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Введение. Процесс управления информационной безопасностью на предприятии. Система анализа защищенности и соответствия стандартам MaxPatrol 8: архитектура, схема лицензирования, режимы работы	А	2		2			1	Задания для самостоятельной работы
2	Способы выявления уязвимостей методом PenTest. Правила безопасного сканирования в режиме PenTest	А	2		2			2	Задания для самостоятельной работы
3	Выявление уязвимостей методом Audit. Определение сетевого транспорта. Привилегии учетной записи для сканирования. Аудит Windows, Unix, Cisco и СУБД	А	2		2			2	Задания для самостоятельной работы
4	Оценка соответствия требованиям стандартов. Адаптация MaxPatrol 8 к корпоративным требованиям. Управление стандартами и проверками	А	2		2			2	Задания для самостоятельной работы
5	Создание отчетов. Типы и параметры отчетов. Доставка отчетов. Применение отчетов. Оценка степени опасности уязвимостей	А	2		2			2	Задания для самостоятельной работы
6	Сканирование по расписанию. Сценарии запуска	А	2		2			2	Задания для самостоятельной работы
7	Упрощенное внедрение системы SIEM Maxpatrol. Назначение системы. Asset Managment, Vulnerability	А	2		2			2	Задания для самостоятельной работы

	Managment, SIEM. Компоненты системы, направления развития, потоки данных								
8	Asset&Vulnerability Management. Метрики CVSSv2, CVSSv3. Контекстные метрики. БДУ ФСТЭК РФ	А	4		4			2	Задания для самостоятельной работы
9	Пользователи и роли	А	2		2			2	Задания для самостоятельной работы
10	Сбор и работа с событиями. PDQL и таксономия события	А	4		4			2	Задания для самостоятельной работы
11	Корреляции. Обзор системных правил корреляции	А	2		2			2	Задания для самостоятельной работы
12	Инциденты и доставка уведомлений	А	2		2			2	Задания для самостоятельной работы
13	Статистика и отчеты	А	2		2			2	Задания для самостоятельной работы
14	Журналы и troubleshooting	А	2		2			2	Задания для самостоятельной работы
							0,3	10,7	Зачет
	ИТОГО		**32**		**32**		**0,3**	**37,7**	

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала. Проблемная лекция начинается с вопросов, с постановки проблемы, которую в ходе

изложения материала необходимо решить. В лекции сочетаются проблемные и информационные начала. При этом процесс познания студентов в сотрудничестве и диалоге с преподавателем приближается к поисковой, исследовательской деятельности. Содержание проблемы раскрывается путем организации поиска ее решения или суммирования и анализа традиционных и современных точек зрения.

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTex;
- Adobe Acrobat Reader;

при проведении практических занятий используется программное обеспечение:

- MaxPatrol конфигурация Education;
- MaxPatrol Security Information and Event Management, конфигурация Education.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

Для поиска учебной литературы библиотеки ЯрГУ используется автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php.

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин - М.: ДМК Пресс, 2012. - 592 с.

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277 (дата обращения: 06.02.2022).

б) дополнительная литература

1. Мельников В. П. Информационная безопасность и защита информации: учеб. пособие для вузов. / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова; УМО по университет. политехн. образованию – 4-е изд., стереотип. – М: Академия, 2009. – 331 с.

2. Методика оценки угроз безопасности информации. Методический документ. Утвержден ФСТЭК России от 5 февраля 2021 г.

3. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Руководящий документ. Приказ председателя Гостехкомиссии России от 19 июня 2002 г. № 187.

4. Серия стандартов ИСО 27000 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности».

в) ресурсы сети «Интернет» (при необходимости)

https://bdu.fstec.ru/ – содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов.

https://attack.mitre.org/ – это общедоступная база знаний о тактиках и методах (техниках) противника, основанная на анализе реальных атак. База знаний ATT&CK используется в качестве основы для разработки моделей угроз и методологий в коммерческом секторе, в органах государственной власти, а также при разработке продуктов и услуг по защите информации.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения лабораторных работ, оснащенные средствами вычислительной техники, с установленным программным обеспечением MaxPatrol конфигурация Education; MaxPatrol Security Information and Event Management, конфигурация Education;
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Доцент кафедры КБиММОИ, канд. физ.-мат. наук Д.М. Мурин

Приложение № 1 к рабочей программе дисциплины
«Системы автоматизации деятельности центров обеспечения компьютерной безопасности»

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Лабораторные работы

1. Установка системы MaxPatrol 8.
2. Сканирование в режиме PenTest.
3. Сканирование в режиме Audit.
4. Оценка соответствия требованиям стандартов.
5. Генерация отчетов.
6. Создание расписания.
7. Инсталляция SIEM системы, первичная настройка компонент.
8. Задачи/профили/активы: Обнаружение узлов в сети, журналы агента. Группы активов. Аудит Windows и Linux. Назначение контекстных метрик группам. Топология.
9. Пользователи и роли, инфраструктуры.
10. Сбор событий: WinEventLog, WMInotification. File via SSH. PDQL. Группировка событий. FileMonitor SMB. Сбор событий по протоколу Syslog.
11. Корреляции и генераторы.
12. Работа с инцидентами и почтовыми уведомлениями: Работа с автоматически созданным инцидентом. Самостоятельное создание инцидента.
13. Статистика и отчеты: Статистика. Построение отчетов.
14. Troubleshooting. Журнальные файлы. Клиент к базе данных elasticsearch.

Задания для самостоятельной работы

Задания для самостоятельной работы состоят в самостоятельном повторении изученного материала и в доработке лабораторных работ, выполнение которых начинается в аудитории.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к зачету:

1. Процесс управления ИБ на предприятии.
2. Система анализа защищенности и соответствия стандартам MaxPatrol 8: архитектура.
3. Система анализа защищенности и соответствия стандартам MaxPatrol 8: режимы работы.

4. Способы выявления уязвимостей методом PenTest.
5. Правила безопасного сканирования в режиме PenTest.
6. Выявление уязвимостей методом Audit. Определение сетевого транспорта. Привилегии учетной записи для сканирования.
7. Аудит Windows, Unix, Cisco и СУБД.
8. Оценка соответствия требованиям стандартов. Управление стандартами и проверками.
9. Адаптация MaxPatrol 8 к корпоративным требованиям.
10. Создание отчетов. Типы и параметры отчетов. Доставка отчетов. Применение отчетов. Оценка степени опасности уязвимостей.
11. Сканирование по расписанию. Сценарии запуска.
12. Упрощенное внедрение системы SIEM Maxpatrol.
13. Назначение системы SIEM Maxpatrol. Asset Managment, Vulnerability Managment, SIEM.
14. Компоненты системы, направления развития, потоки данных.
15. Asset&Vulnerability Management. Метрики CVSSv2, CVSSv3.
16. Asset&Vulnerability Management. Контекстные метрики. БДУ ФСТЭК РФ.
17. Пользователи и роли
18. Сбор и работа с событиями. PDQL и таксономия события.
19. Корреляции. Обзор системных правил корреляции.
20. Инциденты и доставка уведомлений.
21. Статистика и отчеты.
22. Журналы и troubleshooting.

Правила выставления оценки на зачете.

В процессе зачета требуется ответить на один из приведенных выше вопросов. На подготовку к ответу дается не менее 1 академического часа.

По итогам зачета выставляется одна из оценок: «зачтено», «не зачтено».

Оценка «Зачтено» выставляется студенту, который демонстрирует **в**ладение содержанием материала; умеет связывать теорию с практикой. В ответе могут допускаться отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора. На часть дополнительных вопросов студент может не дать ответ или дать неверный ответ. Обязательным условием для выставления оценки «Зачтено» является успешная защита всех лабораторных работ.

Оценка «Не зачтено» выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой; допускает грубые ошибки при определении понятий, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Не зачтено» выставляется также студенту, который взял билет, но отказался дать на него ответ.

Приложение № 2 к рабочей программе дисциплины
«Системы автоматизации деятельности центров обеспечения компьютерной безопасности»

Методические указания для студентов по освоению дисциплины

Учебным планом на изучение дисциплины «Системы автоматизации деятельности центров обеспечения компьютерной безопасности» отводится один семестр, по завершении которого в качестве итогового контроля предусмотрен зачет. В процессе изучения дисциплины проводятся лекционные занятия и выполняются лабораторные работы.

Для успешного освоения дисциплины важно, чтобы обучающийся уделил особенное внимание выполнению лабораторных работ. Теоретические основы, необходимые для выполнения этих работ, подробно разбираются на лекционных занятиях. Основная цель выполнения лабораторных работ – дать обучающимся представление о применении современных средств обнаружения и реагирования на инциденты информационной безопасности на практике. Для успешного выполнения лабораторных работ необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала, чему способствуют регулярные задания для самостоятельной работы. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, лабораторных занятиях и из учебной литературы.

В качестве заданий для самостоятельной работы дома обучающимся предлагается доработать задания лабораторных работ, выполнение которых начинается в аудитории.

По окончанию семестра изучения дисциплины обучающиеся сдают зачет. Зачет принимается по билетам, каждый из которых включает в себя один теоретический вопрос. На самостоятельную подготовку к зачету выделяется 2 дня.

Опыт преподавания дисциплины «Системы автоматизации деятельности центров обеспечения компьютерной безопасности» говорит о высокой сложности ее самостоятельного изучения для обучающегося в первую очередь ввиду достаточно узкого выбора учебной литературы на русском языке, а также ввиду того, что дисциплина является достаточно новой. Излагаемый на лекциях материал часто является нетривиальным и отражает результаты практических разработок последних трех-пяти лет. Поэтому посещение всех аудиторных занятий является обязательным.