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
Методы оценки безопасности компьютерных систем

Направление подготовки (специальности)
10.03.01 Информационная безопасность

Направленность (профиль)
«Безопасность компьютерных систем (в сфере информационных технологий)»

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

Целью освоения дисциплины «Методы оценки безопасности компьютерных систем» является изучение принципов и методов оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности в таких системах в рамках обеспечения безопасности информационных систем и технологий в целом, изучение математических основ моделирования процессов оценки безопасности компьютерных систем, получение профессиональных компетенций в области современных технологий оценки безопасности компьютерных систем.

Основные задачи дисциплины:

- обучение студентов базовым понятиям современных методов оценки безопасности компьютерных систем;
- обучение студентов базовым методам оценки безопасности компьютерных систем;
- овладение практическими навыками применения методов оценки безопасности компьютерных систем;
- раскрытие физической сущности построения и эксплуатации компьютерных систем с точки зрения определения актуальных угроз безопасности в таких системах с целью корректного решения задач по применению методов оценки безопасности компьютерных систем.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Методы оценки безопасности компьютерных систем» относится к обязательной части образовательной программы.

Для освоения данной дисциплиной обучающиеся должны облазать знаниями операционных систем, вычислительных сетей, баз данных, а также основных методов их защиты, иметь базовые навыки по администрированию вычислительных сетей и средств защиты информации.

Для успешного освоения дисциплины «Методы оценки безопасности компьютерных систем» ей должны предшествовать следующие дисциплины:

«Основы информационной безопасности»;
«Организационное и правовое обеспечение информационной безопасности»;
«Основы управления информационной безопасностью»;
«Программно-аппаратные средства защиты информации»;
«Безопасность операционных систем»;
«Системы управления базами данных»;
«Безопасность систем баз данных»;
«Компьютерные сети»;
«Сети и системы передачи информации»;
«Безопасность компьютерных сетей»;
«Комплексная защита объектов информатизации».

Дисциплина «Методы оценки безопасности компьютерных систем» 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
Профессиональные компетенции		
ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	И-ОПК-1.4_4 уметь организовывать и проводить контрольные проверки работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Знать: процессы проверки и оценки ИБ ИТ и СОИБ Уметь: осуществлять аудит ИБ и организовывать работы по его проведению Владеть: терминологией в области аудита ИБ
	И-ОПК-1.4_5 умеет проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей	Знать: критерии и стандарты в области аудита ИБ Уметь: формулировать выводы и заключение по результатам аудита ИБ Владеть: навыками использования инструментальных средств, автоматизированных процессов ИБ

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 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	Базовые сведения о проверке и оценке уровня безопасности компьютерных систем	8	4	4		1		10	
2	Оценка уровня безопасности компьютерных систем: общие понятия и определения	8	4	8		2		16	
3	Стандарты проведения оценки уровня безопасности компьютерных систем	8	8			2		16	
4	Методология оценки уровня безопасности компьютерных систем. Организация процесса оценки уровня безопасности компьютерных систем	8	8	8		2		16	
5	Инструментальные средства оценки уровня безопасности компьютерных систем	8	8	12		3		14	
						2	**0,5**	**33,5**	Экзамен
	ИТОГО		**32**	**32**		**10**	**0,5**	**105,5**	

Содержание разделов дисциплины

Тема № 1: Базовые сведения о проверке и оценке уровня безопасности компьютерных систем.

Проверки и оценки уровня ИБ организации. Оценка уязвимостей компьютерной системы. Разновидности проверок и оценок уровня ИБ организации. Рынок аналитических услуг в сфере ИБ. Место и роль аудита в модели обеспечения ИБ.

Тема № 2: Разновидности проверок и оценок уровня ИБ организации. Рынок аналитических услуг в сфере ИБ. Место и роль аудита в модели обеспечения ИБ.

Базовые определения. Принципы и формы аудита ИБ организации. Особенности автоматизированных информационных систем как объектов аудита ИБ. Исходная концептуальная схема (парадигма) проведения аудита ИБ.

Тема № 3: Стандарты проведения оценки уровня безопасности компьютерных систем.

Законодательная и нормативная база аудита ИБ. Структура международных стандартов по ИБ. Область применения. Процессная модель управления ИБ. Оценка зрелости системы управления ИБ. ISO 27001, ISO 27002. Стандарты ISO/IEC и ГОСТ ИСО/МЭК 27005, BS 7799-3. Анализ рисков ИБ. Общие критерии (ГОСТ Р ИСО/МЭК 15408). Руководящие

документы ФСТЭК России аудит в целях сертификации средств защиты и аттестации объектов информатизации. Стандарт Банка России СТО БР ИББС- 1.1. CoBit. Стандарт аудита PCI DSS. Соответствие и взаимодействие международного и российского подходов и методов аудита безопасности.

Тема № 4: Методология оценки уровня безопасности компьютерных систем. Организация процесса оценки уровня безопасности компьютерных систем.
Основные этапы и методы работ по проведению аудита ИБ. Программа аудита ИБ. Сбор свидетельств (исходной информации) для проведения аудита ИБ. Рекомендации по планированию аудита ИБ. Рекомендации по моделированию. Этапы проведения внутреннего и внешнего аудитов ИБ: общее и различия. Стадии аудита ИБ: планирование; подготовка; моделирование; тестирование; анализ; разработка предложений, документирование. Договор о проведении внешнего аудита ИБ. Порядок планирования аудита. Методы аудита: экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника. Методы сбора исходных данных: опрос, наблюдение, анализ. Методы анализа собранных свидетельств. Аудиторская группа: состав, права и обязанности, роли, привлечение технических специалистов. Обязанности проверяемой организации во время аудита ИБ.

Тема № 5: Инструментальные средства оценки уровня безопасности компьютерных систем.
Методы и инструментальные средства проведения аудита ИБ. Программные средства анализа и управления. Оценка уязвимостей компьютерной системы средствами Dallas Lock. Инструментарий базового уровня - справочные и методические материалы. Инструментарий для обеспечения повышенного уровня безопасности. ПО идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в сфере компьютерной и физической безопасности предприятия. СПВ, их применение и примеры систем. Сохранение доказательств вторжений. Стандарты в области обнаружения вторжений.

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.

Лекция-беседа или «диалог с аудиторией», является наиболее распространенной и сравнительно простой формой активного вовлечения студентов в учебный процесс. Эта лекция предполагает непосредственный контакт преподавателя с аудиторией. Преимущество лекции-беседы состоит в том, что она позволяет привлекать внимание студентов к наиболее

важным вопросам темы, определять содержание и темп изложения учебного материала с учетом особенностей студентов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

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:

- ПО "Dallas Lock 8.0-K";
- ПО "ViPNet Client 4.x (КС3)";
- Система защиты приложений от несанкционированного доступа Positive Technologies Application Firewal, конфигурация Education;
- MaxPatrol конфигурация Education;
- MaxPatrol Security Information and Event Management, конфигурация Education;
- XSpider, 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: 27.01.2022).

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. Меры защиты информации в государственных информационных системах, Методический документ. Утвержден ФСТЭК России от 11 февраля 2014 г.

4. Регламент включения информации об уязвимостях программного обеспечения ипрограммно-аппаратных средств банк данных угроз безопасности информации ФСТЭК России.

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

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

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 практических занятий, оснащенные средствами вычислительной техники, с установленным программным обеспечением ПО "Dallas Lock 8.0-K"; Система защиты приложений от несанкционированного доступа Positive Technologies Application Firewal, конфигурация Education; MaxPatrol конфигурация Education; MaxPatrol Security Information and Event Management, конфигурация Education; XSpider, 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
«Методы оценки безопасности компьютерных систем»

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

Задания для самостоятельной работы

- Установка и настройка ПО "Dallas Lock 8.0-K". Проведение аудита с помощью данного программного обеспечения.
- Установка и настройка системы защиты приложений от несанкционированного доступа Positive Technologies Application Firewal. Проведение аудита с помощью данного программного обеспечения.
- Установка и настройка MaxPatrol. Проведение аудита с помощью данного программного обеспечения.
- Установка и настройка MaxPatrol Security Information and Event Management. Проведение аудита с помощью данного программного обеспечения.
- Установка и настройка XSpider. Проведение аудита с помощью данного программного обеспечения.

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

Список вопросов к экзамену:

1. Оценка уязвимостей компьютерной системы. Разновидности проверок и оценок уровня ИБ организации. Место и роль аудита в модели обеспечения ИБ.
2. Принципы и формы аудита ИБ организации. Особенности автоматизированных информационных систем как объектов аудита ИБ. Исходная концептуальная схема (парадигма) проведения аудита ИБ.
3. Структура международных стандартов по ИБ. Область применения. Процессная модель управления ИБ. Оценка зрелости системы управления ИБ.
4. ISO 27001.
5. ISO 27002.
6. ISO 27005.
7. Анализ рисков ИБ. Общие критерии (ГОСТ Р ИСО/МЭК 15408).
8. Руководящие документы ФСТЭК России аудит в целях аттестации объектов информатизации.
9. Стандарт Банка России СТО БР ИББС- 1.1.
10. CoBit.
11. Стандарт аудита PCI DSS.
12. Соответствие и взаимодействие международного и российского подходов и методов аудита безопасности.
13. Основные этапы и методы работ по проведению аудита ИБ. Программа аудита ИБ.

14. Сбор свидетельств (исходной информации) для проведения аудита ИБ. Рекомендации по планированию аудита ИБ. Рекомендации по моделированию.
15. Этапы проведения внутреннего и внешнего аудитов ИБ: общее и различия. Стадии аудита ИБ: планирование; подготовка; моделирование; тестирование; анализ; разработка предложений, документирование. Договор о проведении внешнего аудита ИБ.
16. Порядок планирования аудита. Методы аудита: экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника.
17. Методы сбора исходных данных: опрос, наблюдение, анализ. Методы анализа собранных свидетельств.
18. Аудиторская группа: состав, права и обязанности, роли, привлечение технических специалистов. Обязанности проверяемой организации во время аудита ИБ.
19. Методы и инструментальные средства проведения аудита ИБ. Программные средства анализа и управления.
20. ПО идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в сфере компьютерной и физической безопасности предприятия.
21. Стандарты в области обнаружения вторжений.

Правила выставления оценки на экзамене.

В экзаменационный билет включаются два теоретических вопроса. На подготовку к ответу дается не менее 1 академического часа.

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Оценка «Отлично» выставляется студенту, который демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом в сфере защиты информации; умеет связывать теорию с практикой. Студент дает развернутые, полные и четкие ответы на вопросы экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует терминологию.

Оценка «Хорошо» выставляется студенту, ответ которого на экзамене в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.

Оценка «Удовлетворительно» выставляется студенту, который дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и дополнительные вопросы, но при этом демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. Ответы излагаются с использованием терминов в сфере защиты информации, но при этом допускаются ошибки в определениях некоторых основных понятий, формулировках положений, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» 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 сущности раскрываемых 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 «Неудовлетворительно» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

Приложение № 2 к рабочей программе дисциплины
«Методы оценки безопасности компьютерных систем»

Методические указания для студентов по освоению дисциплины

Учебным планом на изучение дисциплины «Методы оценки безопасности компьютерных систем» отводится один семестр. В конце семестра в качестве итогового контроля предусмотрен экзамен. В процессе изучения дисциплины проводятся лекционные и практические занятия, выполняются самостоятельные работы.

Основной формой изучения учебного материала по дисциплине «Методы оценки безопасности компьютерных систем» являются практические занятия. Это связано с тем, что основной задачей в рамках дисциплины является получение обучающимся практических навыков по аудиту (оценке) безопасности компьютерных систем.

Для успешного освоения дисциплины очень важно практическое освоение программных средств защиты информации, используемых при оценке безопасности компьютерных систем. Этому способствует изучение теоретического материала. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях и из учебной литературы.

Дополнительную роль при связи теории и практики играют задания для самостоятельной работы. В качестве заданий для самостоятельной работы обучающимся предлагаются задачи по настройке средств защиты информации.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы со средствами защиты информации, проводятся устные опросы обучающихся. Также проводятся консультации (при необходимости) по разбору трудных моментов заданий для самостоятельной работы.

По завершении изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса. На самостоятельную подготовку к экзамену выделяется 3 дня, во время подготовки к экзамену предусмотрена групповая консультация.

Опыт преподавания дисциплины «Методы оценки безопасности компьютерных систем» говорит о сложности ее самостоятельного изучения для обучающегося. Обучающиеся, вставшие на путь самоподготовки, часто неверно расставляют приоритеты при изучении данной дисциплины, что не позволяет им на высоком уровне овладеть изучаемым материалом. Это связано с насыщенностью изучаемого материала и большим числом практических занятий, необходимых для приобретения навыков практического использования средств защиты информации. Поэтому посещение всех аудиторных занятий является настоятельно рекомендуемым.