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
Дополнительные вопросы защищенности компьютерных систем

Направление подготовки (специальности)
10.03.01 Информационная безопасность

Направленность (профиль)
«Безопасность компьютерных систем»

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 «Дополнительные вопросы защищенности компьютерных систем» является теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных компьютерных систем, а также углубленное изучение принципов и методов основных видов атак и защиты от них.

Задачи дисциплины:

- изучение типовых угроз безопасности в компьютерных системах;
- изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных системах;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных системах;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных системах.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина является факультативной дисциплиной. (ФТД.В.02)

Для освоения данной дисциплиной обучающиеся должны владеть навыками работы с операционными системами и вычислительными сетями, обладать базовыми навыками программирования, знать основные подходы к обеспечению информационной безопасности.

Для успешного освоения дисциплины «Дополнительные вопросы защищенности компьютерных систем» ей должны предшествовать следующие дисциплины:

«Информатика»;
«Языки программирования»;
«Основы информационной безопасности»;
«Операционные системы»;
«Защита в операционных системах»;
«Сети и системы передачи информации»;
«Криптографические методы защиты информации»;
«Компьютерные сети».

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-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	И-ОПК-1.4_1 знает источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению	Знать: - содержание отечественных и зарубежных стандартов в области компьютерной безопасности; - детали анализа безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.
	И-ОПК-1.4_4 уметь организовывать и проводить контрольные проверки работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Уметь: - проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.
	И- ОПК-1.4_5 умеет проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей	Владеть: - навыками проведения анализа безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 1 зачетных единиц, 36 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	Операционная система	7		2				1	Опрос по заданиям

	Linux								для самостоятельной работы
2	Криптография и криптоанализ на практике. Аспекты практического применения	7		4				1	Опрос по заданиям для самостоятельной работы
3	Стеганография. Аспекты практического применения	7		4				1	Опрос по заданиям для самостоятельной работы
4	Форензика. Основы расследования компьютерных преступлений	7		4				2	Опрос по заданиям для самостоятельной работы
5	Уязвимости web-приложений	7		4				2	Опрос по заданиям для самостоятельной работы
							0,3	10,7	Зачет
	ИТОГО			**18**			**0,3**	**17,7**	

Содержание разделов дисциплины

Тема № 1. Основы Linux

1.1. История возникновения Linux.
1.2. Архитектура Linux.
1.3. Дистрибутивы Linux.
1.4. Приемы практического использования Linux.

Тема № 2. Криптография и криптоанализ на практике. Аспекты практического применения

2.1. Обзор истории криптографии.
2.2. Отечественные криптоалгоритмы и их криптоанализ.
2.3. Зарубежные криптоалгоритмы и их криптоанализ.

Тема № 3. Стеганография. Аспекты практического применения.

3.1. Основные понятия стеганографии.
3.2. Использование методов стеганографии для скрытия информации.
3.3. Практические приемы обнаружения фактов использования стеганографии.

Тема № 4. Форензика. Основы расследования компьютерных преступлений.

4.1. Основные понятия форензики.
4.2. Анализ дампов сетевого трафика с использованием методов форензики.
4.3. Анализ дампов памяти с использованием методов форензики.
4.4. Анализ образов жестких дисков с использованием методов форензики.

Тема № 5. Уязвимости web-приложений.

5.1. Понятие web-приложения. Типичные архитектуры web-приложения.
5.2. Классификация рисков web-приложений OWASP Top 10.
5.3. XSS-атаки и методы защиты от них.
5.4. SQL-инъекции и методы защиты от них.

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:

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

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

- IDA (бесплатная версия ПО);
- Microsoft Debugging Tools (свободно распространяемое ПО);
- Virtual Box (GNU GPL v.2).
- GDB (GNU GPL v.2).
- BurpSuite (бесплатная версия ПО);
- OpenSSL (свободно распространяемое ПО);
- Linux (GNU GPL v.3).

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. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. : ил.
2. Олифер В.Г. Основы сетей передачи данных [Электронный ресурс] / В.Г. Олифер, Н.А. Олифер. — 2-е изд. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 219 c. — 2227-8397.
3. Таненбаум Э., Современные операционные системы. – СПб.: Питер, 2013., 2014– 1115 с.

б) дополнительная литература

1. Касперски Крис Фундаментальные основы хакерства. Искусство дизассемблирования [Электронный ресурс] / Крис Касперски. — Электрон. текстовые данные. — М. : СОЛОН-ПРЕСС, 2010. — 446 c. — 5-93455-175-2.

в) ресурсы сети «Интернет» (при необходимости)

1. Электронно-библиотечная система «Лань» http://e.lanbook.com/
2. Новейшие данные об угрозах работы с подключением к сети Интернет российской компании «Лаборатория Касперского»:http://www.kaspersky.ru/internet-security-center.

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 практических занятий, оснащенные средствами вычислительной техники, с установленным программным обеспечением;
- 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
«Дополнительные вопросы защищенности 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:

1. Самостоятельно найти в открытых источниках примеры уязвимостей и эксплойтов для ядра Linux.
2. Самостоятельно найти в открытых источниках самые популярные дистрибутивы Linux.
3. Самостоятельно найти в открытых источниках уязвимости криптоалгоритма AES.
4. Самостоятельно найти в открытых источниках уязвимости криптоалгоритма DES.
5. Самостоятельно найти в открытых источниках примеры атак на блочные шифры.
6. Самостоятельно найти в открытых источниках атаки на криптосистему RSA.
7. Самостоятельно найти в открытых источниках утилиты для применения стеганографических методов при скрытии информации в звуковых файлах.
8. Самостоятельно найти в открытых источниках описание стеганографического алгоритма LSB.
9. Самостоятельно, после знакомства с учебной литературой, объяснить назначение, архитектуру и принципы работы фреймворка Volatility.
10. Самостоятельно, после знакомства с учебной литературой, объясните суть протокола аутентификации Kerberos.
11. Самостоятельно, после знакомства с учебной литературой, объясните принципы работы IPSEC.
12. Самостоятельно, после знакомства с учебной литературой, проведите сравнение отечественных и зарубежных алгоритмов шифрования.
13. Самостоятельно, после знакомства с учебной литературой, объясните принципы работы протокола HTTP.
14. Самостоятельно, после знакомства с учебной литературой, приведите примеры уязвимостей библиотеки OpenSSL.

Перечень вопросов для практических занятий:

1. Установка и настройка операционной системы Linux.
2. Линейный криптоанализ шифра DES.
3. Использование утилиты stegsolve.
4. Использование фреймворка Volatility.
5. Эксплуатация SQL-инъекции в уязвимом сайте.

Список вопросов к экзамену:

1. История возникновения Linux.

2. Архитектура Linux.
3. Дистрибутивы Linux.
4. Приемы практического использования Linux.
5. Обзор истории криптографии.
6. Отечественные криптоалгоритмы и их криптоанализ.
7. Зарубежные криптоалгоритмы и их криптоанализ.
8. Основные понятия стеганографии.
9. Использование методов стеганографии для скрытия информации.
10. Практические приемы обнаружения фактов использования стеганографии.
11. Основные понятия форензики.
12. Анализ дампов сетевого трафика с использованием методов форензики.
13. Анализ дампов памяти с использованием методов форензики.
14. Анализ образов жестких дисков с использованием методов форензики.
15. Понятие web-приложения. Типичные архитектуры web-приложений.
16. Классификация рисков web-приложений OWASP Top 10.
17. XSS-атаки и методы защиты от них.
18. SQL-инъекции и методы защиты от них.

Правила выставления оценки на экзамене.

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 владение содержанием материала и понятийным аппаратом практической информационной безопасности; 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.

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 экзаменационный билет, но отказался дать на него ответ.

Приложение № 2 к рабочей программе дисциплины
«Дополнительные вопросы защищенности компьютерных систем»

Методические указания для студентов по освоению дисциплины

Формой изложения учебного материала по дисциплине «Дополнительные вопросы защищенности компьютерных систем» являются практические занятия. Это связано с тем, что данная дисциплина находится на стыке между дисциплинами «Операционные системы» и «Защита в операционных системах» в части аппаратного обеспечения защиты вычислительных процессов и использования памяти, методов хранения данных, и дисциплиной «Основы построения защищенных баз данных». Кроме того, очевидно, что данные о методах обеспечения безопасности постоянно совершенствуются.

Для успешного освоения дисциплины важно углубленное самостоятельное изучение ее разделов, в том числе выполнение домашних заданий. Основная цель самостоятельных работ – помочь не только усвоить теоретические основы и практические методы защиты в операционных системах, но и развить свои умения и навыки до полных и системных.

Для проверки и контроля усвоения материала, приобретенных практических навыков в течение обучения проводятся мероприятия текущей аттестации в виде ряда самостоятельных работ в домашних условиях. Варианты заданий выдаются учащимся на первом занятии по каждой изучаемой теме. Оценка и обсуждение выполненных студентами заданий для самостоятельной работы производится на последнем учебном часе практических занятий по каждой изучаемой теме и учитывается, на ряду с результатами практических занятий, при оценке текущей успеваемости.

В конце семестра изучения дисциплины студенты сдают зачет. Зачет принимается по билетам, каждый из которых включает в себя один теоретический и один практический вопрос.

Освоить вопросы, излагаемые в процессе изучения дисциплины «Дополнительные вопросы защищенности компьютерных систем» самостоятельно студенту крайне сложно. Это связано со сложностью изучаемого материала и необходимостью отработки практических навыков. Поэтому посещение всех аудиторных занятий является совершенно необходимым.