

МИНОБРНАУКИ РОССИИ

Ярославский государственный университет им. П.Г. Демидова

Кафедра интеллектуальных информационных радиофизических систем

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины

Защита от вредоносного программного обеспечения

Направление подготовки (специальности)

10.04.01 Информационная безопасность

Направленность (профиль)

«Управление информационной безопасностью»

Форма обучения очная

Программа рассмотрена

на заседании кафедры

от 29 марта 2024 г., протокол № 6

Программа одобрена НМК

физического факультета

протокол № 5 от 30 апреля 2024 г.

1. Цели освоения дисциплины

Целью преподавания дисциплины является изучение основных видов вредоносного программного обеспечения для наиболее распространенных операционных систем, включая мобильные платформы Android, IOS.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина является факультативной.

При изучении данной дисциплины студенты имеют возможность расширить свои знания, полученные при изучении таких дисциплин как «Защита Web-приложений» и «Разработка защищенных приложений». Большинство рассматриваемых в курсе вопросов основывается на знании архитектуры микропроцессорной системы и низкоуровневого программирования на языке ассемблера. Знания и навыки, полученные при изучении данной дисциплины, могут быть использованы обучающимися для выполнения выпускной квалификационной работы, а также в последующей профессиональной деятельности.

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		
ПК-2 Способен анализировать математические модели систем обеспечения информационной безопасности, а также проводить тестирование средств защиты информации на соответствие этим моделям	И-ПК-2.6 Способен применять сканеры и мониторы для изучения принципов работы программ И-ПК-2.7 Способен применять инструменты сигнатурного анализа для выявления вредоносного ПО И-ПК-2.8 Способен проводить тестирование механизмов безопасности ПО на соответствие моделям обеспечения информационной безопасности	Знать: - архитектуру процессора; - основные принципы управления ресурсами в ЭВМ и организации доступа к этим ресурсам; - классификацию компьютерных вирусов; - стандартные средства борьбы с вирусами. Уметь: - разрабатывать программное обеспечение на языке ассемблера; - разрабатывать программы на высокоуровневых языках с использованием ассемблерных вставок; - противодействовать вредоносному программному обеспечению с помощью стандартных антивирусных средств; - внедрять патчи и заплатки для устранения угроз безопасности в современных операционных системах Владеть навыками: - отладки программ на языке ассемблера; - использования hex-редакторов, дизассемблеров, отладчиков;

		- работы с эксплоитами; - разработки программ для выявления и устранения вредоносного ПО.
--	--	--

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единиц, 72 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	Вводная лекция	3		1				2	
2	Архитектура ЭВМ и программирование на языке ассемблера	3		2		1		8	Устный опрос
3	Алгоритмы и особенности работы вирусов	3		2				8	
4	Маскировка вирусов	3		2		1		8	
5	Принципы разработки антивирусных программ	3		2				8	
6	Фишинговые атаки, руткиты и буткиты	3		2				8	Тестирование
7	Особенности реализации вирусов в мобильных ОС	3		2				8	
							0,3	6,7	Зачет
	ИТОГО			13		2	0,3	56,7	

Содержание дисциплины

Тема 1: Вводная лекция

Предмет и задачи дисциплины. Её связь с другими дисциплинами. Рекомендуемая литература. Вредоносное программное обеспечение, основные признаки, классификация. Примеры работы вирусов и их воздействия на аппаратную и программную составляющую ЭВМ.

Тема 2: Архитектура ЭВМ. и программирование на языке ассемблера

История развития архитектуры ЭВМ и ОС. Организация взаимодействия микропроцессора, оперативной памяти и портов ввода-вывода. Схемы адресации. Регистры данных, сегментов, указателей и индексов. Указатели команд, флаги. Система прерываний. Защищенный режим работы процессора. Введение в программирование на языке ассемблера.

Тема 3: Алгоритмы и особенности работы вирусов

Структура исполнимого файла, присоединение к нему вируса. Резидентная программа. Внедрение вируса в исполнимые файлы и команды перехода на тело вируса. Алгоритм работы файлового вируса. Внедрение вируса в загрузочный сектор.

Тема 4: Маскировка вирусов

Скрытие вирусов в файловой системе. Обход антивирусных программ. Структура «вируса-невидимки». Уход вируса из зараженного файла, при его открытии программой и его возвращение на место при закрытии файла.

Тема 5: Принципы разработки антивирусных программ

Загрузочная запись исполнимого файла, переход на тело вируса. Выделение вируса в карантин. Выделение вируса из зараженного файла или загрузочной области диска. Поиск и удаление вируса в теле файла. Реализация поиска зараженных файлов на диске.

Тема 6: Фишинговые атаки, руткиты и буткиты

Определение, классификация и обнаружение фишинговых атак. Обзор угроз онлайн банкинга, примеры атак, методы защиты. Обзор ядра ОС Windows, понятие руткитов, эволюция руткитов. Понятие буткитов и их эволюция.

Тема 7: Особенности реализации вирусов в мобильных ОС

Классификация основных видов угроз IOS. Вирусы и уязвимости AppleIOS. Средства защиты. Обзор архитектуры Android. Примеры программ. Патчи, эксплойты.

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, история развития науки и практики, достижения в этой сфере, имена известных ученых, 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.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по 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 по дисциплине 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

- Microsoft Visual Studio;
- MikTeX (свободно распространяемое ПО).

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

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

- Электронная библиотечная система «Лань» <https://e.lanbook.com>

- Электронная библиотечная система «Юрайт» <https://urait.ru>

- Электронная библиотечная система «Консультант студента»

<https://www.studentlibrary.ru>

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

а) основная литература

1. Н. Б. Федотов Практикум на ЭВМ. Ассемблер: метод. указания - Ярославль: ЯрГУ, 2011. <http://www.lib.uniyar.ac.ru/edocs/iuni/20110205.pdf>

2. Дейл Н., Уимз Ч., Хедингтон М. Программирование на C++ - Москва: ДМК Пресс, 2007. <https://www.studentlibrary.ru/ru/book/ISBN5937000080.html>

3. Вирусы и средства борьбы с ними - Москва: Национальный Открытый Университет "ИНТУИТ", 2016. https://www.studentlibrary.ru/ru/book/intuit_098.html

4. Климентьев К. Е. Компьютерные вирусы и антивирусы: взгляд программиста - Москва: ДМК Пресс, 2013.

<https://www.studentlibrary.ru/ru/book/ISBN9785940748854.html>

б) дополнительная литература

1. Секаев В. Г. Основы программирования на Ассемблере — Новосибирск: НГТУ, 2010. <https://www.studentlibrary.ru/ru/book/ISBN9785778214736.html>

2. Лагутина Н. С. C++. Примеры и задачи: практикум. - Ярославль: ЯрГУ, 2011. <http://www.lib.uniyar.ac.ru/edocs/iuni/20110401.pdf>

в) ресурсы сети «Интернет»:

1. Система справочной онлайн-информации Microsoft: <https://msdn.microsoft.com/ru-ru/>

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 Microsoft Visual Studio;
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля;
- 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
«Защита от вредоносного программного обеспечения»**

**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**

**Контрольные задания и иные материалы,
используемые в процессе текущей аттестации**

1) Вопросы устного опроса №1:

1. Основные этапы развития архитектуры ЭВМ и ОС.
2. Шинная организация взаимодействия микропроцессора, оперативной памяти и портов ввода-вывода.
3. Схемы адресации.
4. Регистры данных, сегментов, указателей и индексов.
5. Указатели команд, флаги.
6. Система прерываний.
7. Определения, типы и классификация прерываний. Вектор прерываний
8. Защищенный режим работы процессора.
9. Типы данных в языке ассемблера.
10. Директивы определения данных.
11. Сегментация программ на ассемблере и способы определения сегментов.
12. Состав и структура машинной команды.
13. Модели памяти и способы их определения.

2) Вопросы устного опроса №2:

1. Структура исполнимого файла PE.
2. Внедрение вируса в исполнимые файлы, команды перехода на тело вируса.
3. Общий алгоритм работы файлового вируса.
4. Внедрение вируса в загрузочный сектор.
5. Скрытие вирусов в файловой системе.
6. Обход антивирусных программ.
7. Структура «вируса-невидимки».
8. Загрузочная запись исполнимого файла, переход на тело вируса.
9. Выделение вируса в карантин.
10. Выделение вируса из зараженного файла или загрузочной области диска.
11. Поиск и удаление вируса в теле файла.
12. Реализация поиска зараженных файлов на диске.
13. Определение и классификация фишинговых атак.
14. Понятие руткитов и их эволюция.
15. Понятие буткитов и их эволюция.
16. Классификация основных видов угроз iOS.
17. Классификация основных видов угроз Android.
18. Патчи, эксплойты.

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

Зачет выставляется по итогам текущей аттестации.

3. 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 владение содержанием материала и понятийным аппаратом теории псевдослучайных генераторов; 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
«Защита от вредоносного программного обеспечения»**

Методические указания для студентов по освоению дисциплины

Студенту достаточно сложно самостоятельно освоить вопросы дисциплины «Защита от вредоносного программного обеспечения». Посещение всех предусмотренных аудиторных занятий является совершенно необходимым. Без упорных и регулярных самостоятельных занятий в течение семестра сдать зачет практически невозможно. Изучение дисциплины предполагает уверенное владение компьютером, знание основ программирования и основных функций операционной системы.