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

Кафедра интеллектуальных информационных радиофизических систем

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 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 17 апреля 2023 г., протокол № 8

Программа одобрена НМК
физического факультета
протокол № 5 от 25 апреля 2023 г.

Ярославль

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 ОП магистратуры

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 ОП магистратуры

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

Код компетенции	Формулировка компетенции	Перечень планируемых результатов обучения
Общепрофессиональные компетенции		
ОПК-1	*способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности*	*Знать:* – *архитектуру процессора;* – *основные принципы управления ресурсами в ЭВМ и организации доступа к этим ресурсам.* *Уметь:* – *разрабатывать программное обеспечение на языке ассемблера;* – *разрабатывать программы на высокоуровневых языках с использованием ассемблерных вставок.* *Владеть навыками:* – *отладки программ на языке ассемблера;* – *использования hex-редакторов, дизассемблеров, отладчиков.*

Профессиональные компетенции		
ПК-4	*способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности*	*Знать:* − *классификацию компьютерных вирусов;* − *стандартные средства борьбы с вирусами.* *Уметь:* − *противодействовать вредоносному программному обеспечению с помощью стандартных антивирусных средств;* − *внедрять патчи и заплатки для устранения угроз безопасности в современных операционных системах.* *Владеть навыками:* − *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	Введение	3		1				6	
2	Архитектура ЭВМ. и программирование на языке ассемблера	3		2				8	Устный опрос
3	Алгоритмы и особенности работы вирусов	3		2				6	
4	Маскировка вирусов	3		2				6	
5	Принципы разработки антивирусных программ	3		2				6	
6	Фишинговые атаки, руткиты и буткиты	3		2				6	Тестирование
7	Особенности реализации вирусов в мобильных ОС	3		2				8	
		3					**0,3**	**10,7**	**зачет**
	Всего			**13**		**2**		**57**	

Тема №1: Введение
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, эксплоиты.

5. 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 по предложенному алгоритму.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).
В образовательном процессе используется
-программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов:

- Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery);
- Microsoft OfficeSTD 2013;
- MikTeX (свободно распространяемое ПО).
-Microsoft Visual Studio 2013/2015/2017 (в составе Microsoft Imagine Premium Electronic Software Delivery).

Информационные справочные системы:

система справочной информации Microsoft: https://msdn.microsoft.com/ru-ru/;

7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература

1. Кирнос В. Н. Введение в вычислительную технику : основы организации ЭВМ и программирование на Ассемблере: учебное пособие Томск: Эль Контент, 2011. 172 стр. [Электр. ресурс] http:// https://biblioclub.ru/index.php?page=book_view_red&book_id=208651
2. Слабнов В. Д. Программирование на С++: лекции Казань: Познание, 2012. 136 стр. [Электр. ресурс] http://biblioclub.ru/index.php?page=book_red&id=364222&sr=1
3. Холмогоров В. PRO вирусы. -Издательство: Страта, 2017.- 162 с. https://biblioclub.ru/index.php?page=book_view_red&book_id=477964
4. Сердюк В. А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. - Издательство: Издательский дом Высшей школы экономики, 2015. https://biblioclub.ru/index.php?page=book_view_red&book_id=440285

б) дополнительная литература

1. Секаев В.Г. Основы программирования на Ассемблере [Электронный ресурс] : учебное пособие / В.Г. Секаев. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2010. — 100 с. — 978-5-7782-1473-6. — Режим доступа: http://www.iprbookshop.ru/44986.html
2. Практикум на ЭВМ. Ассемблер: метод. указания / Н.Б. Федотов; Яросл. гос. ун-т им. П. Г. Демидова, Науч.-метод. совет ун-та. - Ярославль: ЯрГУ, 2011. – 66 с.
3. Лагутина Н. С. С++. Примеры и задачи: практикум. / Н. С. Лагутина; Яросл. гос. ун-т им. П. Г. Демидова, Науч.-метод. совет ун-та - Ярославль: ЯрГУ, 2011. - 47 с.

в) ресурсы сети «Интернет»:

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

.

8. 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 (семинаров);

- лаборатория информационных технологий;

- 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.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, хранящиеся на электронных носителях и обеспечивающие тематические иллюстрации, соответствующие рабочим программам дисциплин.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы) :

Доцент, к.т.н Тараканов А.Н.

Приложение №1 к рабочей программе дисциплины
«Вредоносное программное обеспечение»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 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, эксплоиты.

1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации

Зачет выставляется по итогам текущей аттестации.

2. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

2.1 Шкала оценивания сформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дисциплины осуществляется по следующей трехуровневой шкале:

Пороговый уровень - предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков, полученных студентом в результате освоения дисциплины. Пороговый уровень является обязательным уровнем для студента к моменту завершения им освоения данной дисциплины.

Продвинутый уровень - предполагает способность студента использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутый уровень превосходит пороговый уровень по нескольким существенным признакам.

Высокий уровень - предполагает способность студента использовать потенциал интегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профессиональных задач и самостоятельного поиска новых подходов в их решении путем комбинирования и использования известных способов решения применительно к конкретным условиям. Высокий уровень превосходит пороговый уровень по всем существенным признакам.

2.2 Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования

Код компе-тенции	Форма контроля	Этапы форми-рования (№ темы (раздела)	Показатели оценивания	Шкала и критерии оценивания компетенций на различных этапах их формирования		
				Пороговый уровень	Продвинутый уровень	Высокий уровень
Общепрофессиональные компетенции						
ОПК-1	Устный опрос	1-2	Знать: архитектуру процессора; основные принципы управления ресурсами в ЭВМ и организации доступа к этим ресурсам. Уметь: разрабатывать программное обеспечение на языке ассемблера;	Знать: архитектуру процессора; основные принципы управления ресурсами в ЭВМ и организации доступа к этим ресурсам.	Знать: архитектуру процессора; основные принципы управления ресурсами в ЭВМ и организации доступа к этим ресурсам. Уметь: разрабатывать программное обеспечение на языке ассемблера; разрабатывать программы на	Знать: архитектуру процессора; основные принципы управления ресурсами в ЭВМ и организации доступа к этим ресурсам. Уметь: разрабатывать программное обеспечение на языке ассемблера; разрабатывать программы на

			разрабатывать программы на высокоуровневых языках с использованием ассемблерных вставок. Владеть навыками: отладки программ на языке ассемблера; использования hex-редакторов, дизассемблеров, отладчиков.		высокоуровневых языках с использованием ассемблерных вставок.	высокоуровневых языках с использованием ассемблерных вставок. Владеть навыками: отладки программ на языке ассемблера; использования hex-редакторов, дизассемблеров, отладчиков.
Профессиональные компетенции						
ПК-4	Устный опрос	З-7	Знать: классификацию компьютерных вирусов; стандартные средства борьбы с вирусами. Уметь: противодействовать вредоносному программному обеспечению с помощью стандартных антивирусных средств; внедрять патчи и заплатки для устранения угроз безопасности в современных операционных системах. Владеть навыками: работы с эксплоитами; разработки программ для выявления и устранения вредоносного ПО.	Знать: классификацию компьютерных вирусов; стандартные средства борьбы с вирусами.	Знать: классификацию компьютерных вирусов; стандартные средства борьбы с вирусами. Уметь: противодействовать вредоносному программному обеспечению с помощью стандартных антивирусных средств; внедрять патчи и заплатки для устранения угроз безопасности в современных операционных системах.	Знать: классификацию компьютерных вирусов; стандартные средства борьбы с вирусами. Уметь: противодействовать вредоносному программному обеспечению с помощью стандартных антивирусных средств; внедрять патчи и заплатки для устранения угроз безопасности в современных операционных системах. Владеть навыками: работы с эксплоитами; разработки программ для выявления и устранения вредоносного ПО.

3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.1 Критерии оценивания степени овладения знаниями, умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):
- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):
- достаточно полные и систематизированные знания в объёме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):
- систематизированные, глубокие и полные знания по всем разделам дисциплины;
- точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;

- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

3.2 Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка. Вид оценки: «зачтено», «незачтено».

Оценка «зачет» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «незачтено» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Приложение №2 к рабочей программе дисциплины
«Вредоносное программное обеспечение»

Методические указания для студентов по освоению дисциплины

Студенту достаточно сложно самостоятельно освоить вопросы дисциплины «**Вредоносное программное обеспечение**». 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.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы рекомендуется использовать учебную литературу и интернет-источники, указанные в разделе 7 данной программы.