

	Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный колледж»
	Учебно-методический отдел
	Обучающая (учебная) и вспомогательная литература
	Рабочая тетрадь

РАБОЧАЯ ТЕТРАДЬ
МДК 04.02 ОБЕСПЕЧЕНИЕ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ
КОМПЬЮТЕРНЫХ СИСТЕМ

студента очной формы обучения
специальности 09.02.07 Информационные системы и программирование
группа № _____

(фамилия, имя, отчество)

Челябинск, 2025

2. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ

2.1. ВРЕДОНОСНЫЕ ПРОГРАММЫ

Задание 1. Сформулируйте определения следующим терминам:

Вредоносное программное обеспечение (ВПО)

Компьютерный вирус

Канал распространения вирусов

Задание 2. Каким образом распространяются вредоносные программы?

Задание 3. Перечислите признаки заражения вредоносной программой?

Задание 4. Какое наказание предусмотрено в УК РФ за распространение вредоносного программного обеспечения?

Задание 5. Что называют «полезной нагрузкой» в контексте вредоносного программного обеспечения?

Задание 6. Установите соответствие между методом обнаружения компьютерного вируса и его характеристикой

- | | | |
|----|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Просмотр | А. Обнаружение изменений в объектах компьютерной системы путем сравнения их вычисленных при проверке хэш-значений с эталонными или проверки ЭЦП для этих объектов. Недостатками является то, что не все изменения проверяемых объектов вызываются вирусным заражением, не может помочь при записи на жесткий диск компьютера пользователя уже зараженного файла. |
| 2. | Инспекция | Б. Постоянное присутствие в оперативной памяти компьютера с целью сканирования всех открываемых или получаемых извне файлов и контроля всех «подозрительных» действий других программ (например, обнаружение и блокирование потенциально опасных результатов web-поиска, ссылок на URL). Недостатками являются снижение эффективности работы системы и возможность выполнения контролируемых действий незараженными программами. |
| 3. | Эвристический анализ | В. Присоединение к защищаемому файлу специального модуля контроля, следящего за целостностью данного файла с помощью вычисления его хеш-значения и сравнения с эталоном. Недостатками являются возможность обхода вирусами-невидимками и неприменимость для защиты файлов документов. |
| 4. | Мониторинг | Г. Проверка системных областей памяти и файлов с целью обнаружения фрагментов исполнимого кода, характерного для компьютерных вирусов. Анализируются тысячи различных характеристик каждого файла. Недостатками являются длительность процедуры проверки и возможность ложных сообщений о найденных вирусах. |

5. Вакцинирование Д. Сканирование проверяемых объектов (системных областей дисковой и оперативной памяти, а также файлов заданных типов) в поиске сигнатур (уникальных последовательностей байтов) известных вирусов. Недостатками является необходимость постоянного обновления баз данных сигнатур известных вирусов, неспособность обнаружить новые компьютерные вирусы

Ответ: _____