




## Результаты теста антивирусов/антируткитов на обнаружение и удаление современных руткитов (Тест №2 от 12.2007)

**Таблица 1а: Лучшие антивирусы/антируткиты по результатам теста**

Название антивируса/антируткита	Награда	Получено баллов		
		Вредоносные программы (6 max)	Концепты (2 max)	Всего (max 8)
Rootkit Unhooker 3.7.300	 <b>Gold Anti-Rootkit Protection Award</b>	5.5	2	7.5
GMER 1.0.13		5.5	1.5	7
Kaspersky Anti-Virus 7.0		4.5	2	6.5
Avira Rootkit Detection 1.0		5	1.5	6.5
AVG Anti-Rootkit 1.1	 <b>Silver Anti-Rootkit Protection Award</b>	4	1.5	5.5
Panda AntiRootkit version 1.08		4	1.5	5.5
Sophos Anti-Rootkit 1.3.1		4.5	1	5.5
Dr.Web 4.44		5	0	5
TrendMicro RootkitBuster 1.6		4	1	5
Symantec Anti-Virus 2008	 <b>Bronze Anti-Rootkit Protection Award</b>	4	0.5	4.5
F-Secure Anti-Virus 2008		2.5	1.5	4
McAfee Rootkit Detective 1.1		3	0.5	3.5
BitDefender Antivirus 2008	<b>Провалили тест</b>	3	0	3
McAfee VirusScan Plus 2008		1.5	0	1.5
Eset Nod32 Anti-Virus 3.0		1	0	1
Trend Micro Antivirus plus Antispyware 2008		1	0	1

**Таблица 1б: Лучшие антивирусы по результатам теста**

Название антивируса	Вредоносные программы (6 max)	Концепты (2 max)	Всего баллов
Kaspersky Anti-Virus 7.0	4.5	2	6.5
Dr.Web 4.44	5	0	5
Symantec Anti-Virus 2008	4	0.5	4.5
F-Secure Anti-Virus 2008	2.5	1.5	4
BitDefender Antivirus 2008	3	0	3
McAfee VirusScan Plus 2008	1.5	0	1.5
Eset Nod32 Anti-Virus 3.0	1	0	1
Trend Micro Antivirus plus Antispyware 2008	1	0	1

**Таблица 1в: Лучшие антируткиты по результатам теста**

Название антируткита	Вредоносные программы (6 max)	Концепты (2 max)	Всего баллов
Rootkit Unhooker 3.7.300	5.5	2	7.5
GMER 1.0.13	5.5	1.5	7
Avira Rootkit Detection 1.0	5	1.5	6.5
AVG Anti-Rootkit 1.1	4	1.5	5.5
Panda AntiRootkit version 1.08	4	1.5	5.5
Sophos Anti-Rootkit 1.3.1	4.5	1	5.5
TrendMicro RootkitBuster 1.6	4	1	5
McAfee Rootkit Detective 1.1	3	0.5	3.5

**Таблица 2: Результаты теста антивирусов/антируткитов на обнаружение вредоносных программ, использующих руткит-технологии**

Антивирус \ Вредоносная программа	Trojan-Spy.Win32. Goldun.hn	Trojan-Proxy. Win32.Wopla.ag	SpamTool. Win32.Mailbot.bd	Monitor.Win32. EliteKeylogger.21	Rootkit.Win32. Agent.ea	Rootkit.Win32. Podnuha.a	Всего баллов
BitDefender Antivirus 2008	++	++	-/	++	-/	-/	3
Dr.Web 4.44	++	++	++	-/	++	++	5
F-Secure Anti-Virus 2008	++	+/-	+/-	+/-	-/	-/	2.5
Kaspersky Anti-Virus 7.0	++	++	++	++	+/-	-/	4.5
Eset Nod32 Anti-Virus 3.0	++	-/	-/	-/	-/	-/	1
McAfee VirusScan Plus 2008	++	-/	+/-	-/	-/	-/	1.5
Symantec Anti-Virus 2008	++	++	++	++	-/	-/	4
Trend Micro Antivirus plus Antispyware 2008	++	-/	-/	-/	-/	-/	1
<b>Антируткит</b>							
AVG Anti-Rootkit 1.1	++	++	++	++	-/	-/	4
Avira Rootkit Detection 1.0	++	++	++	++	++	-/	5
GMER 1.0.13	+/-	++	++	++	++	++	5.5
McAfee Rootkit Detective 1.1	++	++	+/-	+/-	-/	-/	3
Panda AntiRootkit version 1.08	++	++	+/-	++	+/-	-/	4
Rootkit Unhooker 3.7.300	++	++	++	++	++	+/-	5.5
Sophos Anti-Rootkit 1.3.1	++	++	++	++	+/-	-/	4.5
TrendMicro RootkitBuster 1.6	++	+/-	++	++	+/-	-/	4

**Таблица 3: Результаты теста антивирусов/антируткитов на обнаружение концептуальных руткитов**

Антивирус \ Концептуальный руткит	Unreal A 1.0.1	RkDemo v1.2	FuTo	HideToolz	Всего баллов
BitDefender Antivirus 2008	-	-	-	-	0
Dr.Web 4.44	-	-	-	-	0
F-Secure Anti-Virus 2008	-	+	+	+	1.5
Kaspersky Anti-Virus 7.0	+	+	+	+	2
Eset Nod32 Anti-Virus 3.0	-	-	-	-	0
McAfee VirusScan Plus 2008	-	-	-	-	0
Symantec Anti-Virus 2008	+	-	-	-	0.5
Trend Micro Antivirus plus Antispyware 2008	-	-	-	-	0
<b>Антируткит</b>					
AVG Anti-Rootkit 1.1	-	+	+	+	1.5
Avira Rootkit Detection 1.0	-	+	+	+	1.5
GMER 1.0.13	-	+	+	+	1.5
McAfee Rootkit Detective 1.1	-	-	-	+	0.5
Panda AntiRootkit version 1.08	+	+	-	+	1.5
Rootkit Unhooker 3.7.300	+	+	+	+	2
Sophos Anti-Rootkit 1.3.1	-	-	+	+	1
TrendMicro RootkitBuster 1.6	-	-	+	+	1

+/+	- руткит успешно обнаружен в системе (будь то файл, процесс или перехват функций) и удален
+/-	- руткит успешно обнаружен в системе, но не удален
-	- руткит не обнаружен в системе

**За каждый плюс (обнаружение или удаление руткита) начисляется 0.5 балла**