

Настрой-ка Dr.Web от **майнеров**

© ООО «Доктор Веб», 2018



В целях максимальной защиты от современных программ — в том числе вредоносных программмайнеров — сразу после установки необходимо произвести следующие настройки антивирусной защиты.

Проверьте, чтобы используемая вами версия антивируса была актуальной, а лицензия — действующей

Внимание! Статистика работы службы технической поддержки компании «Доктор Веб» показывает, что значительное число заражений происходит вследствие того, что антивирус был отключен или длительное время не обновлялся.

Для того чтобы проверить актуальность лицензии, щелкните на значок 🗃. Напротив пункта **Лицензия** будет показано количество дней до истечения текущей лицензии.

Ð	Мой Dr.Web	
8	Лицензия	Осталось 493 дн.
	Инструменты	
	Компоненты з	ащиты
0	Требуется обн	овление
Q	Сканер	

Для того чтобы узнать используемую версию продукта, щелкните на значок Ш, выберите пункт Инструменты и в открывшемся окне — Поддержка.



Внимание! Текущая версия антивируса Dr.Web Security Suite — 11.5. Использование неактуальных версий антивирусных программ увеличивает риск заражения в связи с отсутствием в них <u>новейших</u> <u>технологий детектирования.</u>



2. Все компоненты антивирусной защиты на момент заражения должны быть включены

В том числе модули Превентивной защиты, Dr.Web SpIDer Gate, Антиспам Dr.Web и Брандмауэр Dr.Web.

Лишних компонентов в антивирусе Dr.Web нет! В качестве примера можно привести Антиспам Dr.Web. Тестирование данного модуля показало, что он отфильтровывает более 90% неизвестных вредоносных программ, рассылаемых злоумышленниками, по признакам распространения мошеннических писем. И это без использования технологий антивирусного ядра.

Об отключении одного или нескольких компонентов свидетельствует вид значка **SpiDer Agent'a** в системном трее: *****, а само меню агента будет выглядеть так:

-	Мой Dr.Web	
Q	Лицензия	Осталось 493 дн.
A	Инструменты	
0-	Компоненты защи	ты
2	Загрузка файлов	0%
Q	Сканер	

Отсутствие значка агента может означать, что антивирус выгружен и компьютер остался без антивирусной защиты.

Узнать, какие компоненты отключены, можно, кликнув на значок агента и далее на пункт Компоненты защиты.

Компоненты защиты	
SpIDer Guard	
SpIDer Gate	
SpIDer Mail	
Родительский контроль	
Брандмауэр	
Превентивная защита	
.00.	(2)
	Компоненты защиты SpIDer Guard SpIDer Gate SpIDer Mail Родительский контроль Брандмауэр Превентивная защита



3. Все обновления антивируса должны быть установлены, включая обновления, требующие перезагрузки в целях установки новых драйверов перехвата и исправления потенциальных уязвимостей защиты.

Ежедневно злоумышленниками создаются сотни новых майнеров (не считая других вредоносных программ). Если антивирус отключен или долго не обновлялся — каждый из этих майнеров может беспрепятственно установиться на вашем компьютере или устройстве.

Чтобы проверить статус обновлений, кликните на значок 🗃. Статус обновлений будет показан в открывшемся меню.



Чтобы проверить периодичность получения обновлений, кликните на значок 👹 в системном меню, затем в открывшемся меню последовательно нажмите на 🛍 и появившийся значок 🙆.





Сеть Самозацита Дополнительно Сеть Самозацита Дополнительные настройии

В открывшемся окне **Настройки** выберите **Основные — Обновление**.

Не рекомендуется увеличивать период между обновлениями более 1 часа.

4. Должен быть включен компонент Dr.Web Cloud, обеспечивающий мгновенную реакцию на появление новых угроз — до получения обновления.

Проверить использование облачного контроля можно, нажав значок 🛍 (значок изменит вид на 🛅), нажав на появившийся значок 🙆 и выбрав в меню **Настройки** пункт **Основные.**



5. Действия антивируса Dr.Web Security Space по отношению к вредоносным программам-майнерам должны включать перемещение их в карантин

В случае повторных заражений, целевых атак, а также в случаях, когда нужно выявить путь заражения, наличие тела вредоносной программы может быть критически важным. Поэтому по отношению к вредоносным программам рекомендуется использовать действие **Перемещать в карантин.**

Кликните на значок в системном меню, затем в открывшемся меню последовательно нажмите на (Режим администратора) и появившийся значок 🔅 (Настройки). В открывшемся окне Настройки выберите пункт Компоненты защиты и далее SpiDer Guard. Настройте действия для групп Инфицированные и Потенциально опасные.



🌃 Dr. Web > Компоненты защиты > SplDe	r Guard	
Компоненты зашиты	Опции проверки Проверять объекты на съемных носителях	
SplDer Guard	Блокировать автозалуск со сменных носителей	
SplDer Gate	Вкл.	
SplDer Mail	Пействия	
Сканер	Инфицированные	
Превентивная защита	Лечить, перемещать в карантин неизлечимые (рекомендуе 🗸	
	Лечить, перемещать в карантин неизлечимые (рекомендуется) Лечить, удалять неизлечимые Перемещать в карантин Удалять Перемещать в карантин (рекомендуется)	
0	Программы дозвона Перемещать в карантин (рекомендуется) ✓ Программы-шутки	

Аналогичные настройки необходимо использовать и для иных модулей антивируса — в частности, Антивирусного модуля, модуля Dr.Web SpIDer Gate.

👹 Dr. V	/eb > Компоненты защиты > Сканер		
€	Компоненты зашиты	Режим проверки Прерывать проверку при переходе на питание от аккумулятора	
	SplDer Guard	откл. Использовать звуковые оповещения	
	SplDer Gate	Откл.	
	SplDer Mail	Использование ресурсов компьютера	
	Сканер	Оптимальное (рекомендуется) 🗸 🗸	25
	Превентивная защита	Действия инфицированные	
		Лечить, перемещать в карантин неизлечимые (рекомендуе 🗸	
		Лечить, перемещать в карантин неизлечимые (рекомендуется) Лечить, удалять неизлечимые Перемещать в карантин Удалять	
	?	Перемещать в карантин (рекомендуется) Порграммы дозвона 	

Внимание! Майнеры — это общее название вредоносных программ В частности, они могут распознаваться как троянские программы (Trojan.BtcMine), Java-скрипты (JS.BtcMine), утилиты (Tool.BtcMine). Настройки Dr.Web Security Space позволяют выбрать действия по умолчанию применительно ко всем этим типам майнеров.

Так, для обнаружения вредоносных программ-майнеров, относящихся к типу Tool, рекомендуется установить действие **Потенциально опасные** в **Перемещать в карантин.**



6. Правила исключения из антивирусной проверки должны использоваться крайне осторожно. В случае необходимости использования исключений необходимо указывать конкретные файлы.

Зачастую вредоносные программы используют для майнинга легальные программы. Такие программы распознаются средствами защиты как потенциально опасные. Если вы уверены, что установленный вами майнер не является вредоносным, вы можете разрешить его использование, используя **Исключения.**

Для того чтобы добавить используемый вами майнер в исключения антивирусной проверки, нажмите значок 🛍 (значок изменит вид на 🛅) и, нажав на появившийся значок 🕸, войдите в меню Настройки в пункт Исключения.

👹 Dr.Web > Настройки > Исключения > Файль	ы и папки		<u></u>		×
Исключения	Вы можете исключить из пр	оверки определенные файлы и г	папки.		
Веб-сайты					
Файлы и папки	Объект	SpIDer Guard	Скане	р	
Приложения	C:\Temp	Исключен			
Антиспам					

Внимание! Исключения по маскам типа *.exe или *.dll будут служить причиной того, что никакие объекты, подходящие под такую маску, не будут и будут пропущены. В случае маски *.exe будут пропущены все исполняемые файлы.

Внимание! Не рекомендуется исключать проверку трафика для используемых программ — в таком случае никакое вредоносное ПО, загруженное данными программами, проверяться не будет.

👹 Dr.Web > Настройки > Исключени	ия > Приложения			_		×
Исключения	Вы можете исклк возможно, увели	очить из проверки оп чит скорость проверк	ределенные програм и, но безопасность к	имы и проце сомпьютера	ессы. Эт может	0,
Веб-сайты		n.				
Файлы и папки		.				
Приложения	Объект	SpIDer Guard	SpIDer Gate	SpIDer	Mail	
Антиспам	C:\Program .		Исключен			

7. Должна использоваться система обнаружения вредоносных скриптов

Используемая в Dr.Web технология ScriptHeuristic предотвращает исполнение вредоносных скриптов (в том числе майнеров) в браузере, не нарушая при этом функциональности легитимных скриптов. Дополнительно к данной технологии для противодействия использованию вирусописателями скриптовых языков JScript, JavaScript, VBScript и PowerShell используется модуль защиты Dr.Web Amsiclient, обеспечивающий проверку выполняемых скриптов, написанных на данных языках.



Включение антивирусной проверки модуля Dr.Web Amsi-client производится в разделе настроек **SpiDer Guard.** По умолчанию проверка включена. Для того чтобы проверить состояние модуля, кликните на значок в системном меню, затем в открывшемся меню последовательно нажмите на **администратора**) и появившийся значок (Hacтройки). В открывшемся окне Hacтройки выберите пункт **Компоненты защиты** → **SpiDer Guard** и кликните на пункт **Дополнительные настройки.** Пункт **Проверять скрипты**... должен быть включен.



Внимание! Установка и удаление модуля Dr.Web Amsi-client производится совместно с модулем Dr.Web SpIDer Guard. Модуль доступен при использовании Антивируса Dr.Web и Dr.Web Security Suite в операционных системах начиная с Windows 10 (x86, x64), а также Windows Server 2016.

8. Должен быть настроен Офисный/Родительский контроль

Троянец-майнер может проникнуть в локальную сеть или на отдельный компьютер через спам (как правило, сообщение содержит вредоносное вложение или специально сформированную ссылку), с помощью сообщения мессенджера (также содержащего ссылку), путем загрузки файла (например, Java-скрипта) пользователем с зараженного сайта или на зараженной флешке.

Для настройки режима доступа к ресурсам сети Интернет, а также ограничения доступа к файлам и папкам, последовательно кликните на значки 🗃 и 💼. Затем нажмите на появившийся значок 🔅 и в окне **Настройки** перейдите к пункту меню **Родительский контроль**.





В открывшемся окне выберите пользователя, для которого необходимо настроить ограничения и сделать необходимые настройки.

Dr.Web > Родите	льский контроль > Админис	тратор > Интернет	
🕤 🚺 A	дминистр	Режим работы	
		Блокировать по категориям	~
Интернет		Без ограничений	
		Блокировать по категориям	
เป็นผู้สุดปาก เห	20104	Блокировать все, кроме сайтов	из белого списка
		🖌 Азартные игры	🗌 Почта
		🖌 Наркотики	🔲 Социальные сети
		E a se di anno di anno di	
		велый и черный списки	
		Автоматически включать функци	ию резопасного поиска в поисковых системах
0			
r.Web > Родите	льский контроль > Админис	тратор > Файлы и папки	
			×

Объект	Доступ	
C.\Temp	Read-only	~
	Blocked	
	Read-only	



По умолчанию ограничения отключены.

Для настройки ограничений к сменным носителям в окне **Настройки** выберите **Основные** → **Устройства.**



В данном окне выберите **Ограничивать доступ к сменным носителям.** Далее нажмите на **Изменить** для классов устройств и выберите необходимые классы устройств.

Объект	Заблокировать
Sensor (Sensors)	
AudioEndpoint (Audio inputs and outputs)	
WCEUSBS (Mobile devices)	
Dot4 (IEEE 1284.4 devices)	
CDROM (DVD/CD-ROM drives)	
DiskDrive (Disk drives)	
Keyboard (Keyboards)	
ОК Отмениять	(

После этого появится возможность настройки для раздела **Белый список устройств.** Если необходимо использовать только разрешенные сменные носители, нажмите на **Изменить** — 💮 .



	Обзор	льные
+		(i) (?
Пользователь	Правило	
Everyone	Разрешать все 🛛 👻	
		5
	(+) ()) Пользователь Everyone	(+) (()) Пользователь Правило Everyone Разрешать все ~

В открывшемся окне нажмите Обзор и выберите необходимое устройство.

Устройства Состояни > Print queues > Universal Serial Bus controllers	ie
 Print queues Universal Serial Bus controllers 	
Universal Serial Bus controllers	
DVD/CD-ROM drives	
NECVMWar VMware IDE CDR10 ATA Devi Включено	D
P Disk drives	
VMware, VMware Virtual S SCSI Disk Device Включено	D
Display adapters	
Floppy drive controllers	
Standard floppy disk controller Включено	D
IDE ATA/ATAPI controllers	

Подтвердите выбор, нажав ОК.



standard hoppy disk contr	oller	Обзор
+		
Пользователь	Правило	
Everyone	Разрешать все	~
Everyone	Разрешать все	~

Если необходимо разрешить использование данного носителя только для определенных пользователей компьютера, нажмите 🕙 и выберите необходимого пользователя.

🔯 Dr.Web > Основные > Устройства	Выбор: Пользователи или Группы	2 🗙
Белый с Устройства Выбор: Пользователи или Группы	Выберите тип объекта: Пользователи, Группы, или Встроенные участники безопасности Типы объектое. В следующем месте: USER-7DDE5FA70F Размещение	
Выберите тип объекта: Пользователи, Группы, или Встроенные участники безопасности В следующем месте: USER-7DDE5FA70F Введите умена выбираемых объектов (примеры): Пополнительно	Общие запросы Имя: начинается Понск Описание: начинается Понск Описание: начинается Понск Отключенные учетные записи Отключенные учетные записи Отключенные учетные записи Отключенные осоком действия Число дней со времени последнего входа в систему:	
ОК Отмените	OK Отмен Имя (RDN) В папке INETWORK SERVICE INETWORK SERVICE REMOTE INTERACTIVE L SUPPORT_388945a0 USER-7DDE5F INETWORK SERVICE Apaseseterparop USER-7DDE5F Apaseseterparop USER-7DDE5F Apaseseterparop USER-7DDE5F Apageseterparop USER-7DDE5F	

Укажите права по использованию данного устройства.



Multiple Card Reade	er USB Device	Обзор
+		
Пользователь	Правило	
Everyone	Разрешать все	~
	Разрешать все	
	Только чтение	

Подтвердите выбор.

🐻 Dr. We	b > Oc	новные » Устройства	
•	Бел	ый список устройств	
i	Задайт индиви	ге правила доступа к устройствам. Для некоторых типов устройств поддерживаются идуальные настройки для каждого пользователя.	
(•	2 1	?
	44	Устройства	
	0	ADATA USB Flash Drive USB Device	

9. **Доступ используемых программ в сеть Интернет должен быть ограничен** — это можно сделать с помощью компонента **Брандмауэр.**

Для настройки параметров работы **Брандмауэра** щелкните кнопкой мыши значок **В** системном трее, разблокируйте возможность изменения настроек путем нажатия значка (сзначок изменит вид на (с), нажав на появившийся значок ⁽, выберите в меню **Компоненты защиты** пункт **Брандмауэр.**



Компоненты защиты Интерактивный режим	~
SpiDer Guard Разрешать локальные соединения SpiDer Gate Вкл. SpiDer Mail Изменить доступ к сети для приложений Сканер Изменить параметры работы для известных сетей	
Брандмауэр Превентивная защита	

Фильтрация на уровне приложений позволяет контролировать доступ конкретных программ и процессов к сетевым ресурсам.

Для каждой программы может быть не более одного набора правил фильтрации.

web > пастроики > компоненты защить	гэ брандмаузр эттрилол	кения			-
) Приложения					
	α.				
Фильтрация на уровне приложен сетевым ресурсам, а также разре	ний позволяет контро ешать или запрещать	лироватн этим при	» доступ иложени	і конкретных программ и процессов к іям запуск других процессов.	
					0
000					0
Приложение	õ	¢+		Путь	
svchost.exe	0	0	0	C:\Windows\System32\svchost.exe	
SYSTEM	0	0	0	SYSTEM	
🔝 wininit.exe	۲	۲	۲	C:\Windows\System32\wininit.exe	
🕽 explorer.exe	0	۲	۲	C:\Windows\explorer.exe	
💷 userinit.exe	0	۲	0	C:\Windows\System32\userinit.exe	
🥑 firefox.exe	0	0	0	C:\Program Files\Mozilla Firefox\firefox.exe	
🚊 winlogon.exe	0	۲	0	C:\Windows\System32\winlogon.exe	
V <u>112</u> 327		120	1.41		

Для доступа к этому окну в настройках **Брандмауэра** нажмите **Изменить доступ к сети для приложений** и нажмите кнопку 🕙 или выберите приложение и нажмите кнопку 🖉.

Для формирования набора правил выполните одно из следующий действий.

- Чтобы создать набор правил для новой программы, нажмите кнопку 🕙 (Создать).
- Чтобы отредактировать существующий набор правил, выберите его в списке и нажмите кнопку (Изменить).



- Чтобы добавить копию существующего набора правил, выберите Копировать в контекстном меню. Копия добавляется под выбранным набором.
- Чтобы удалить все правила для программы, выберите соответствующий набор в списке и нажмите кнопку ((Удалить).

Приложе	ение	õ	\$ *		Путь
💷 svcho	ost.exe	0	0	0	C:\Windows\System32\svchost.exe
SYSTE	EM	0	0	0	SYSTEM
💽 winin	it ava		0	٥	C:\Windows\System32\wininit.exe
ز exp	изменить Копировать		0	0	C:\Windows\explorer.exe
💷 use	Добавить		0	0	C:\Windows\System32\userinit.exe
ire	Удалить		0	0	C\Program Files\Mozilla Firefox\firefox exe
- In c	Удалить неиспользуемые правила		-	-	ert regram rice to send in crowfin crowiese

В окне **Новый набор правил для приложения** (или **Редактирование набора правил**) отображается тип правила для конкретного приложения или процесса, а также список правил. Вы можете изменять тип правила, формировать список, добавляя новые или редактируя существующие правила фильтрации, а также изменяя порядок их выполнения. Правила применяются последовательно, согласно очередности в списке.

noop n	in a second the second second		
/кажите файл	или процесс, для которог	о создается правило:	
			Обзор
7.0			
🖌 запрашив	ать подтверждение при из	менении ооъекта (рекоменд	уется)
н Запуск сет	евых приложений:		
Не задан	0	~	
	0700 01 000 000		
в доступ к с	етевым ресурсам:		
Разреша	ть все	~	
OK	Отменить		2

Вы можете создать правило при помощи окна настроек **Брандмауэра.** При работе в режиме обучения вы можете инициировать создание правила непосредственно из окна оповещения о попытке несанкционированного подключения.



STEM				
Запрашиват Запуск сетев	ъ подтвержден вых приложени	ние при измене й:	ении объекта (р	рекомендуется)
Разрешать			~	
Доступ к сет	евым ресурсам	и:		
Пользоват	ельский		~	
()	0			
Включено	Действие	Имя прави	Тип соеди	Описание
\checkmark	Разрешать	udp4://*	Исходящее	Auto-rule
\checkmark	Разрешать	udp4://*	Исходящее	Auto-rule
\checkmark	Разрешать	tcp4://*	Исходящее	Auto-rule
\checkmark	Разрешать	tcp4://* <	Входящее	Auto-rule
	Разрешать	udp4://* <	Входящее	Auto-rule
	STEM Запрашиват Запуск сетев Разрешать Доступ к сет Пользоват Пользоват Включено Включено Г	STEM Запрашивать подтвержден Запуск сетевых приложени Разрешать Доступ к сетевым ресурсам Пользовательский () () () () () Включено Действие Включено Действие () Разрешать () Разрешать () Разрешать	STEM Запрашивать подтверждение при измене Запуск сетевых приложений: Разрешать Доступ к сетевым ресурсам: Пользовательский Ф ОО ОО ОО Включено Действие Имя прави Включено Действие Имя прави № Разрешать udp4://* № Разрешать tcp4://* № Разрешать tcp4://*	STEM Запрашивать подтверждение при изменении объекта (Запуск сетевых приложений: Разрешать Г Доступ к сетевым ресурсам: Пользовательский ✓ Ф СОСТУП к сетевым ресурсам: Пользовательский ✓ Включено Действие Имя прави Тип соеди Включено Действие Имя прави Тип соеди P азрешать udp4://* Исходящее P азрешать tcp4://* Исходящее P азрешать tcp4://* < Входящее

10. Должна быть включена проверка зашифрованного трафика. На данный момент до половины трафика сети Интернет зашифровано, чем могут воспользоваться злоумышленники.

Как правило, майнеры действуют в составе ботнетов — групп зараженных компьютеров. Это позволяет им существенно увеличить вероятность заработка на криптовалютах. Кроме того, сами по себе майнеры бесполезны для злоумышленников без наличия связи с сетью Интернет.

Включите проверку зашифрованного трафика (функционал доступен для Dr.Web Security Space) —

кликните на значок 🗃 в системном меню, затем в открывшемся меню последовательно нажмите на 间 (Режим администратора) и появившийся значок 🍄 (Настройки). В открывшемся окне Настройки выберите пункт Основные и далее Сеть. Переключатель Безопасные соединения должен быть включен.





1

11. Настройки Dr.Web Process Heuristic не должны позволять внедрение майнерами эксплойтов в работающие приложения

Проверить настройки можно, нажав значок 🛍 (значок изменит вид на 🛅), нажав на появившийся значок 🕸 и выбрав в меню Настройки пункт Компоненты защиты и далее Изменить параметры блокировки подозрительных действий.

👹 Dr.Web > Настройки > Компоненты защит	ы > Превентивная защита	° - °		×
🔶 Компоненты	Режим работы			
защиты	Оптимальный (рекомендуется)	~		
SplDer Guard	Изменить параметры блокировки подозрительных действий			
SplDer Gate	Изменить параметры доступа для приложений			
SplDer Mail				
Сканер	Защита от эксплоитов			
Брандмауэр	Блокировать исполнение неавторизованного кода	~		
Превентивная защита	эта опция позволяет олокировать вредоносные объекты, котор уязвимости в Adobe Reader, Internet Explorer, Firefox и других из программах.	вестны:	ользую х	т

Режимы				
Настройте реакцию Dr.Web на обращение приложен настройки не распространяются на те приложения, д	ний к защищаемым объект иля которых параметры на	гам. Обратите вни строены отдельно	мание, что эти ,	
Оптимальный (рекомендуется)	· (•)	Ì		?
Защищаемый объект	Разрешать	Спрашивать	Запрещать	
Целостность запущенных приложений	0	0	۲	
Целостность файлов пользователей	0	0	۲	
Файл HOSTS	0	0	۲	
Низкоуровневый доступ к диску	0	0	۲	
Загрузка драйверов	۲	0	0	
Параметры запуска приложений (IFEO)	۲	0	0	
n		0	0	

Статус **Разрешить** разрешает внесение изменений в соответствующие ресурсы пользователям и злоумышленникам.



12. Установка пароля позволит гарантировать невозможность отключения защиты злоумышленниками — в том числе в случае взлома вашего компьютера.

Вредоносные программы, в том числе майнеры, стремятся отключить антивирус. Не стоит способствовать им в этом желании.

Для установки пароля доступа нажмите значок (акачок изменит вид на) и, нажав на появившийся значок (), выберите в меню **Настройки** пункт **Основные.** Нажмите на переключатель и далее на кнопку **Изменить пароль.**

🔯 Dr.Web > Основные > Настройки		<u>- 🗆 ×</u>
Настройки	Пароль	
Основные	Защищать паролем настройки Dr.Web	
Родительский контроль	Изменить пароль	
Исключения		
Компоненты защиты	Управление настройками	
	Вы можете сохранить настройки продукта на жесткий диск в виде файла, импортировать их из файла или восстановить настройки по умолчанию.	
	Изменить 🗸	
\bigcirc		

Внимание! Не рекомендуется устанавливать пароль, совпадающий с паролем доступа к компьютеру или устройству.

Мы также рекомендуем:

1. Включите и настройте компонент Защита от потери данных.

Далеко не все майнеры безобидны. В качестве примера можно привести <u>Trojan.BtcMine.1978.</u> При попытке завершить его вручную Windows аварийно прекращает работу и демонстрирует «синий экран смерти» (BSOD).

Не нужно забывать также о том, что далеко не все вирусописатели являются профессионалами в программировании и их «творения» могут повредить данные, находящиеся на вашем компьютере.

Для настройки параметров **Защиты от потери данных** кликните на значок 🕮 в системном меню, затем в открывшемся меню нажмите на 间 и выберите пункт **Инструменты.**

Dr.Web — российский антивирус

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Это один из первых антивирусов в мире. «Доктор Веб» — один из немногих антивирусных вендоров, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ.

<u>Технологии Dr.Web | История разработки | Наши клиенты</u>

<u> Продукты Dr.Web внесены в Реестр отечественного ПО</u>

Лицензии и сертификаты

- Сертификаты ФСТЭК России
- Сертификаты МО России
- Сертификаты ФСБ России
- Все сертификаты и товарные знаки

Демо бесплатно

На 30 дней на все продукты комплекса Dr.Web Enterprise Security Suite:

https://download.drweb.ru/demoreg/biz/v2

Проверить качество работы наших решений вы также можете как с помощью бесплатных лечащих утилит <u>Dr.Web CureNet!</u> и <u>Dr.Web Curelt!</u>, так и с помощью сервиса тестирования наших решений — <u>Dr.Web LiveDemo.</u>

Контакты

Центральный офис ООО «Доктор Веб» 125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а

<u>Телефоны</u> <u>Схема проезда</u> <u>Контакты для прессы</u> <u>Офисы за пределами России</u>

антивирус.pф | www.drweb.ru | free.drweb.ru | www.av-desk.ru | curenet.drweb.ru



© ООО «Доктор Веб», 2003-2018