Международная научно-практическая конференция
«Современные технологии кибербезопасности»

Современные аспекты развития классического антивируса

Виталий Бугаев
Технический директор
ТОО «Доктор Веб – Центральная Азия»

БАНК РОССИИ ФИНЦЕРТ

Объем несанкционированных операций в 2018 году:

- **платежные карты – 1,385 млрд. руб.**
- **системы ДБО – 1,469 млрд. руб.**

СБЕРБАНК

Убытки компаний от кибератак:
2018 - $1,5 трлн.
2019 - $2,5 трлн. (прогноз)

WORLD ECONOMIC FORUM

Сумма планетарного ущерба от кибератак к 2022 году вырастет **до $8 трлн**.

Современные вредоносные программы разрабатываются не просто вирусописателями-**профессионалами** — это **хорошо организованный криминальный бизнес:**

Организаторы

Участники

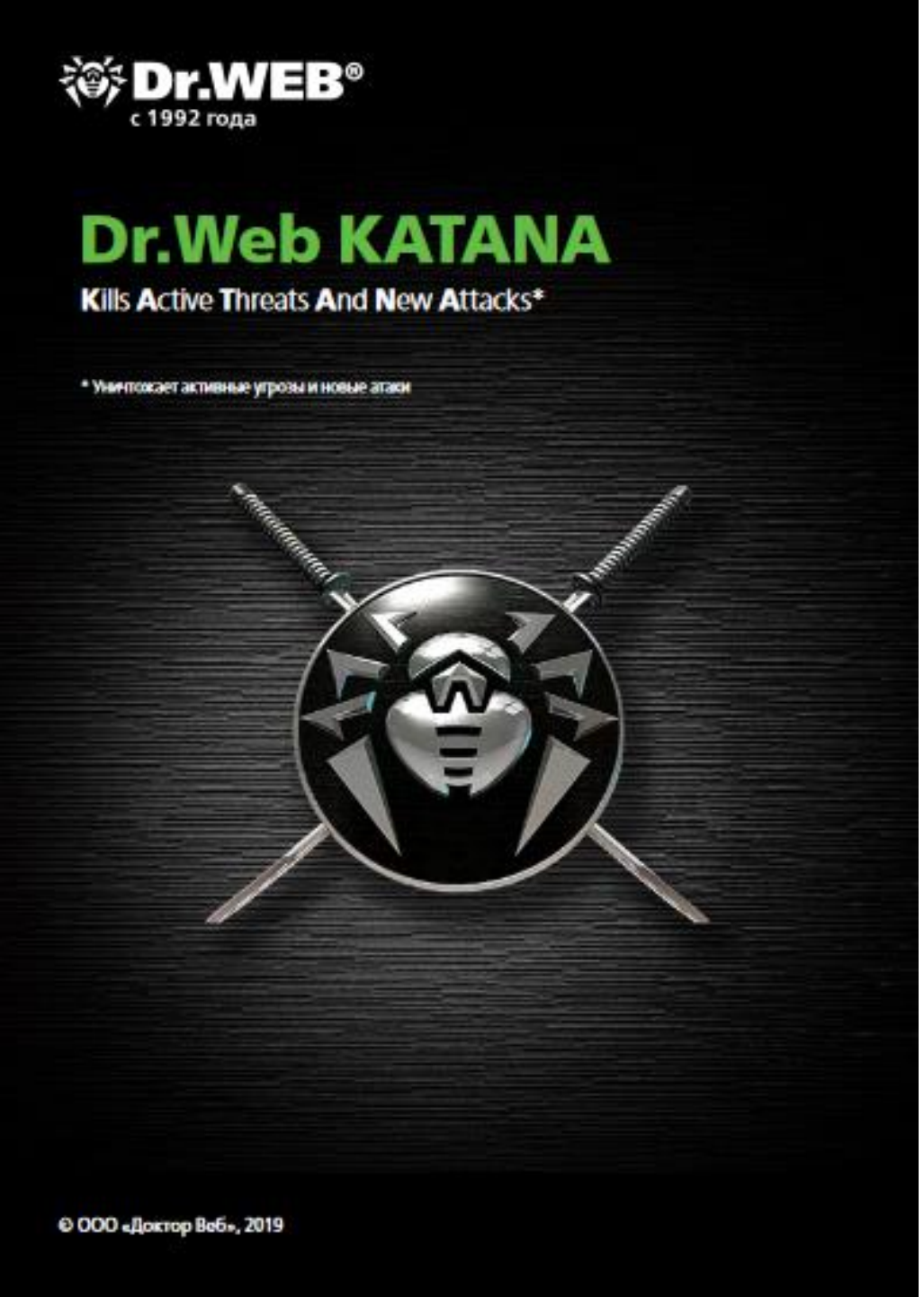
- ✓ Разработчики;
- ✓ Тестировщики;
- ✓ Исследователи уязвимостей;
- ✓ Специалисты по упаковщикам и шифрованию;
- ✓ Распространители, специалисты по социальной инженерии;
- ✓ Системные администраторы

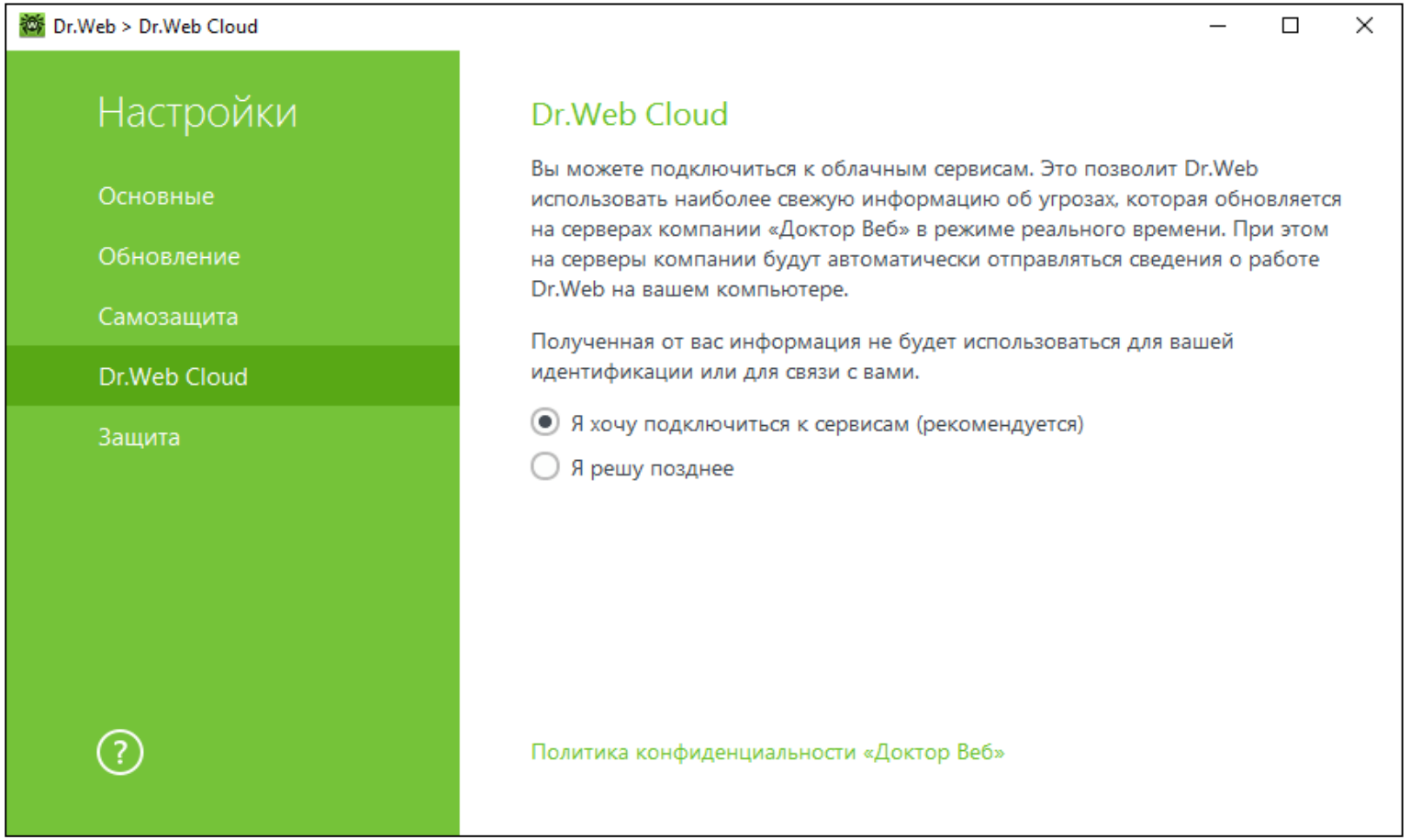
Антивирус действительно **не всегда может обнаружить** новейшую вредоносную программу в момент проникновения, рассчитанную на скрытое проникновение, - но **никакое другое программное обеспечение, кроме антивируса, не способно вылечить систему от уже проникшего и запущенного троянца**

Dr.Web KATANA

Kills **A**ctive **T**hreats **A**nd **N**ew **A**ttacks

Облачная защита





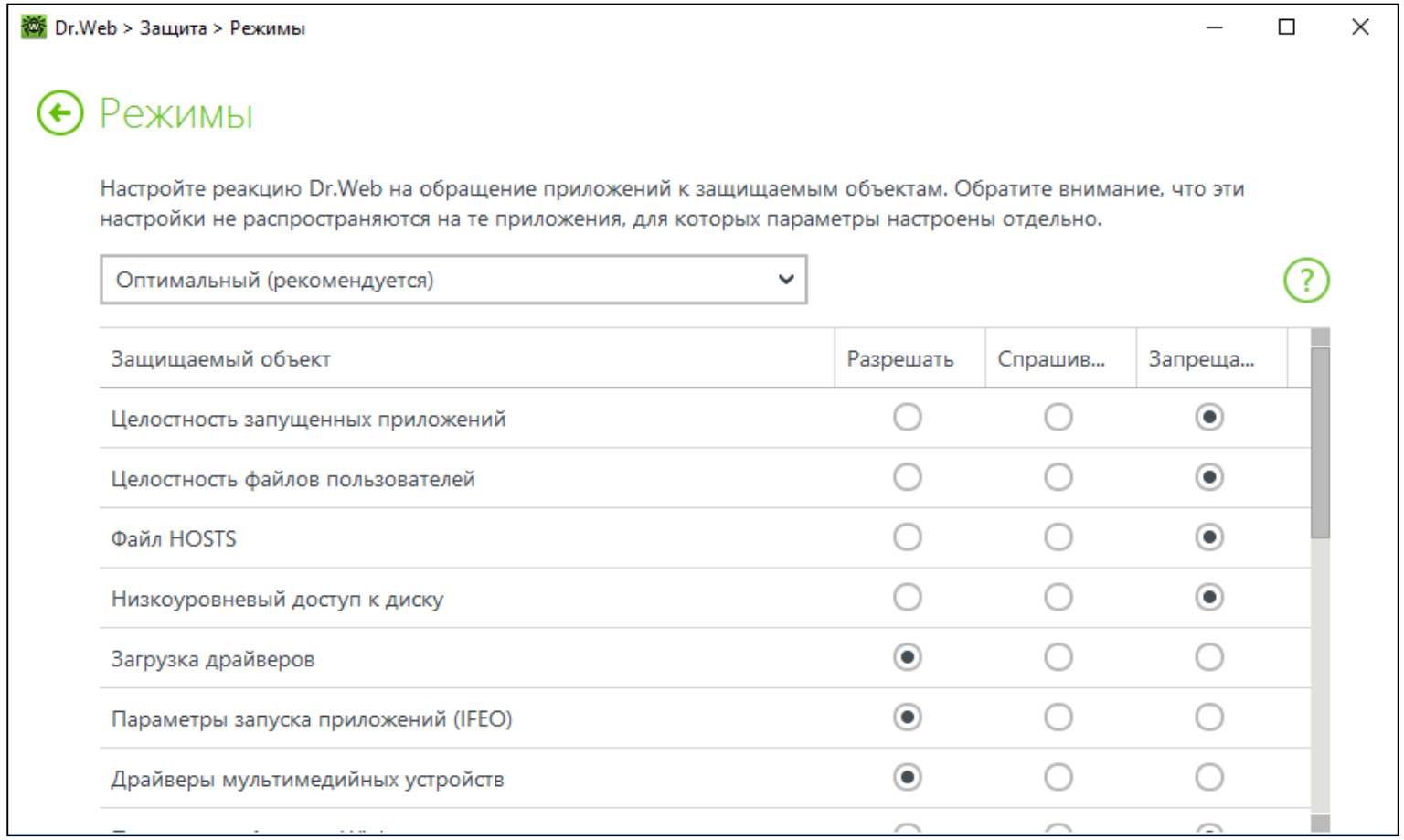
Dr.WEB®
с 1992 года

Dr.Web KATANA

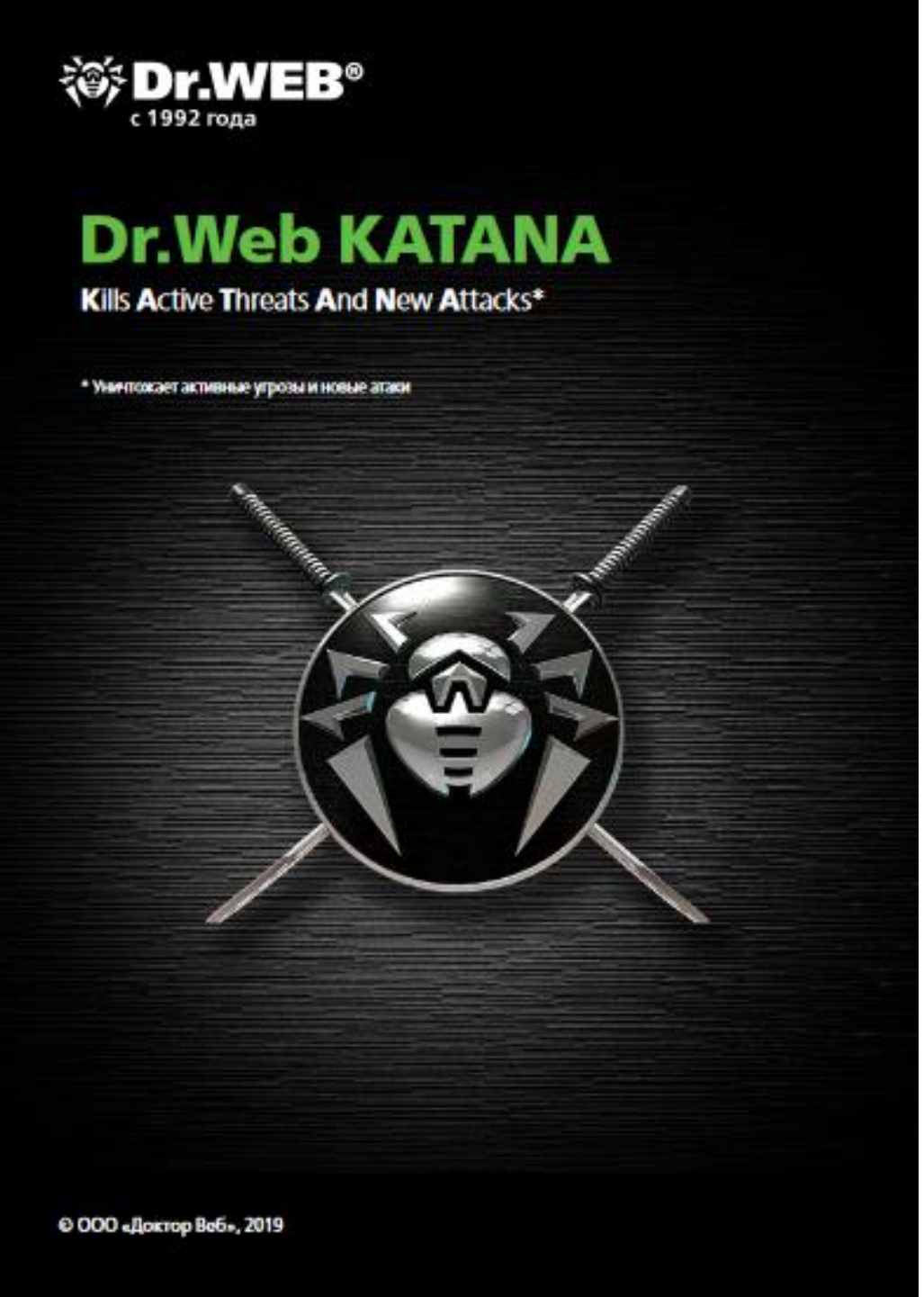
Kills Active Threats And New Attacks*

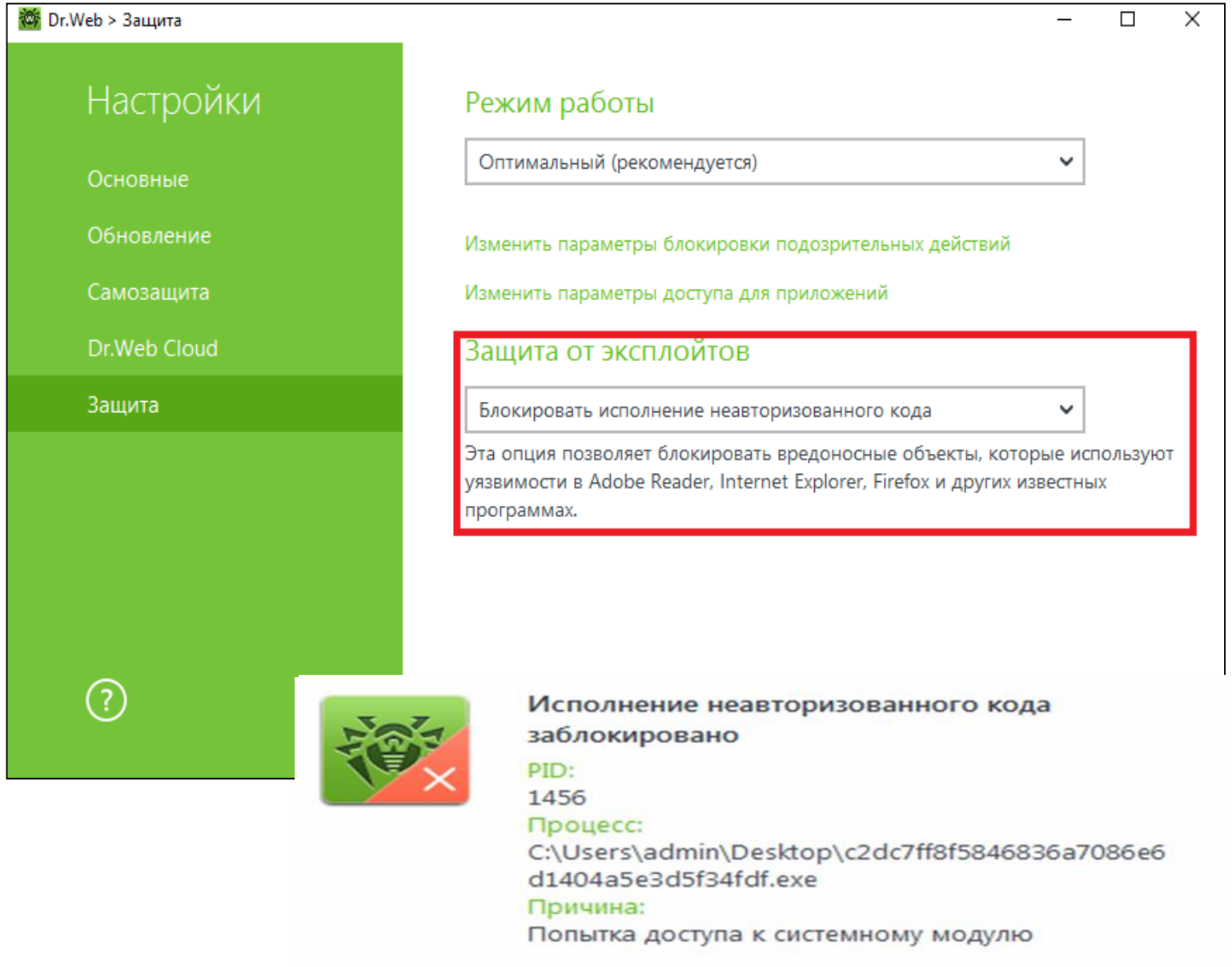
* Уничтожает активные угрозы и новые атаки

Поведенческий анализ

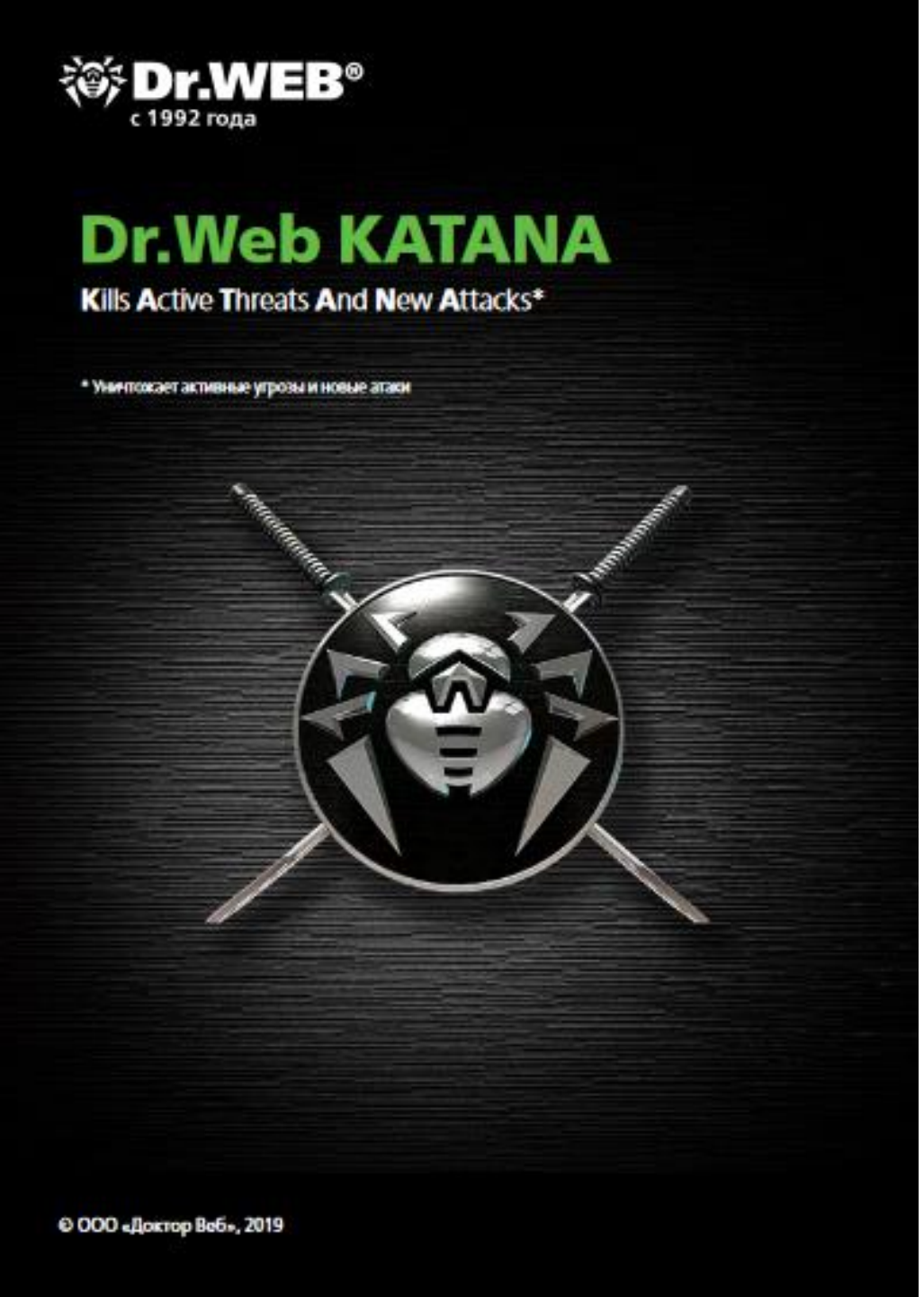


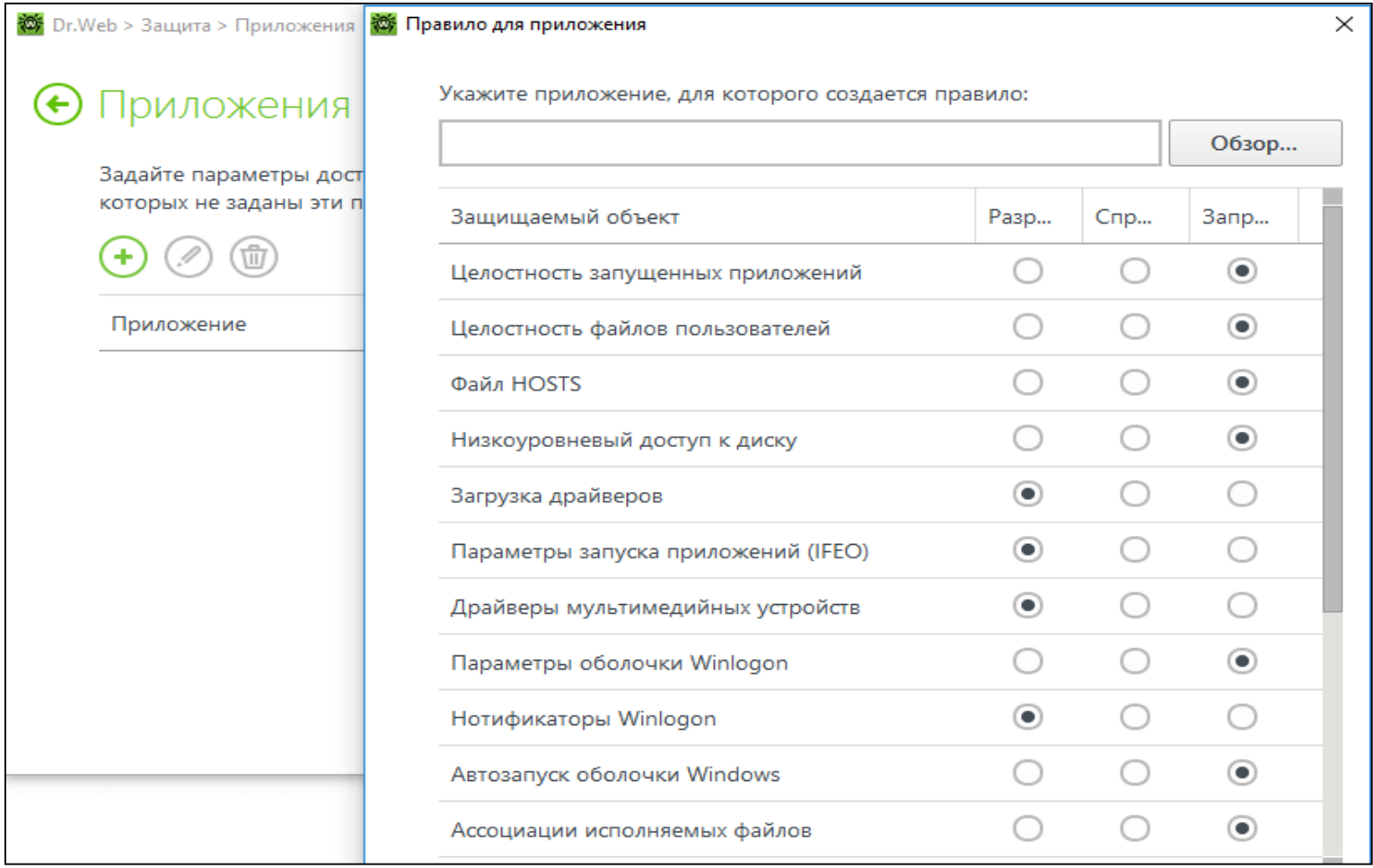
Защита от эксплойтов



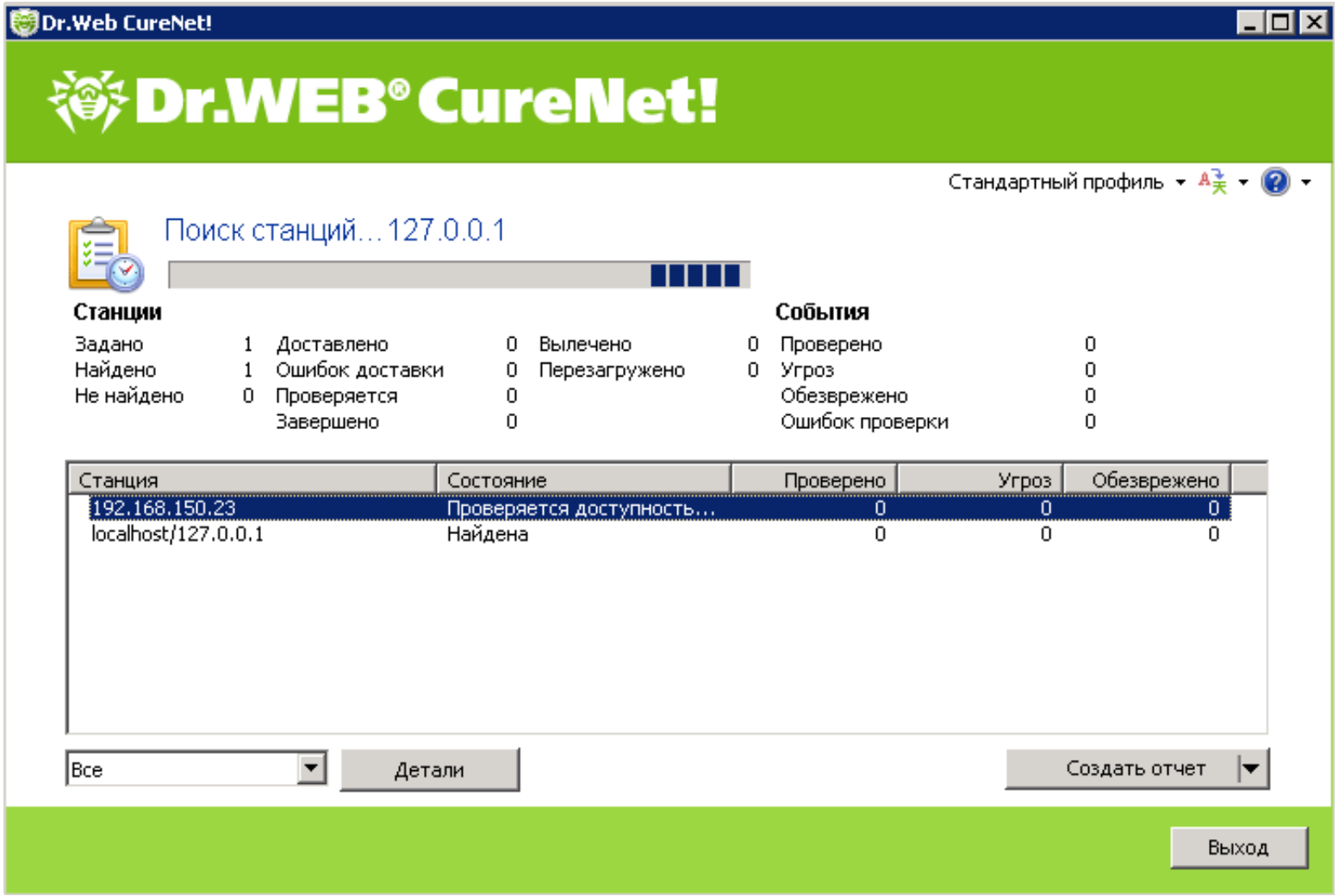


Защита приложений





Запуск проверки



Возможности проверки

Dr.WEB
CureNet!

«Доктор Веб» | Техническая поддержка

Выборочная

Начало: 23.06.2015 18:37
Конец: 23.06.2015 18:37

Распечатать

Станции

Задано	2	Доставлено	1	Вылечено	1
Найдено	1	Ошибок доставки	0	Перезагружено	0
Не найдено	1	Проверяется	0		
		Завершено	1		

События

Проверено	20
Угроз	16
Обезврежено	16
Ошибок проверки	0

192.168.150.23
localhost/127.0.0.1

Объекты

Инфицированные	16
Неизлечимые	0
Подозрительные	0
Рекламные программы	0
Программы дозвона	0
Программы-шутки	0
Потенциально опасные	0
Программы взлома	0

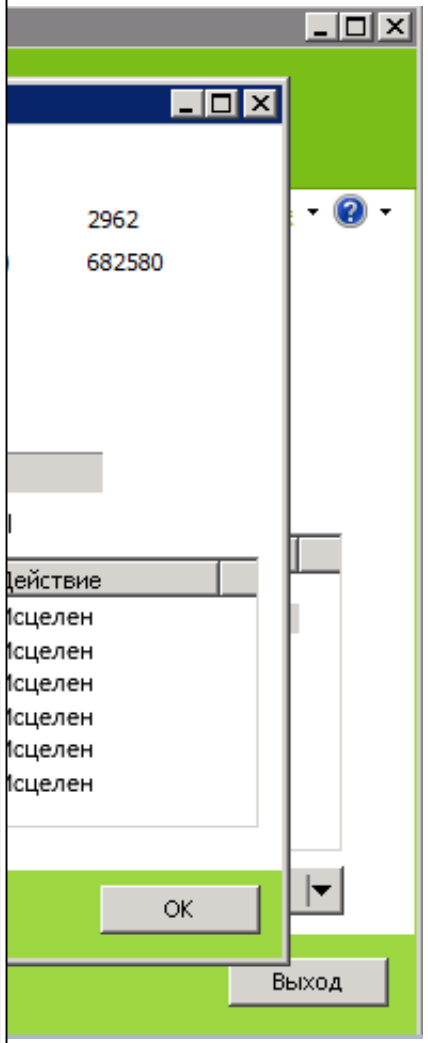
Действия

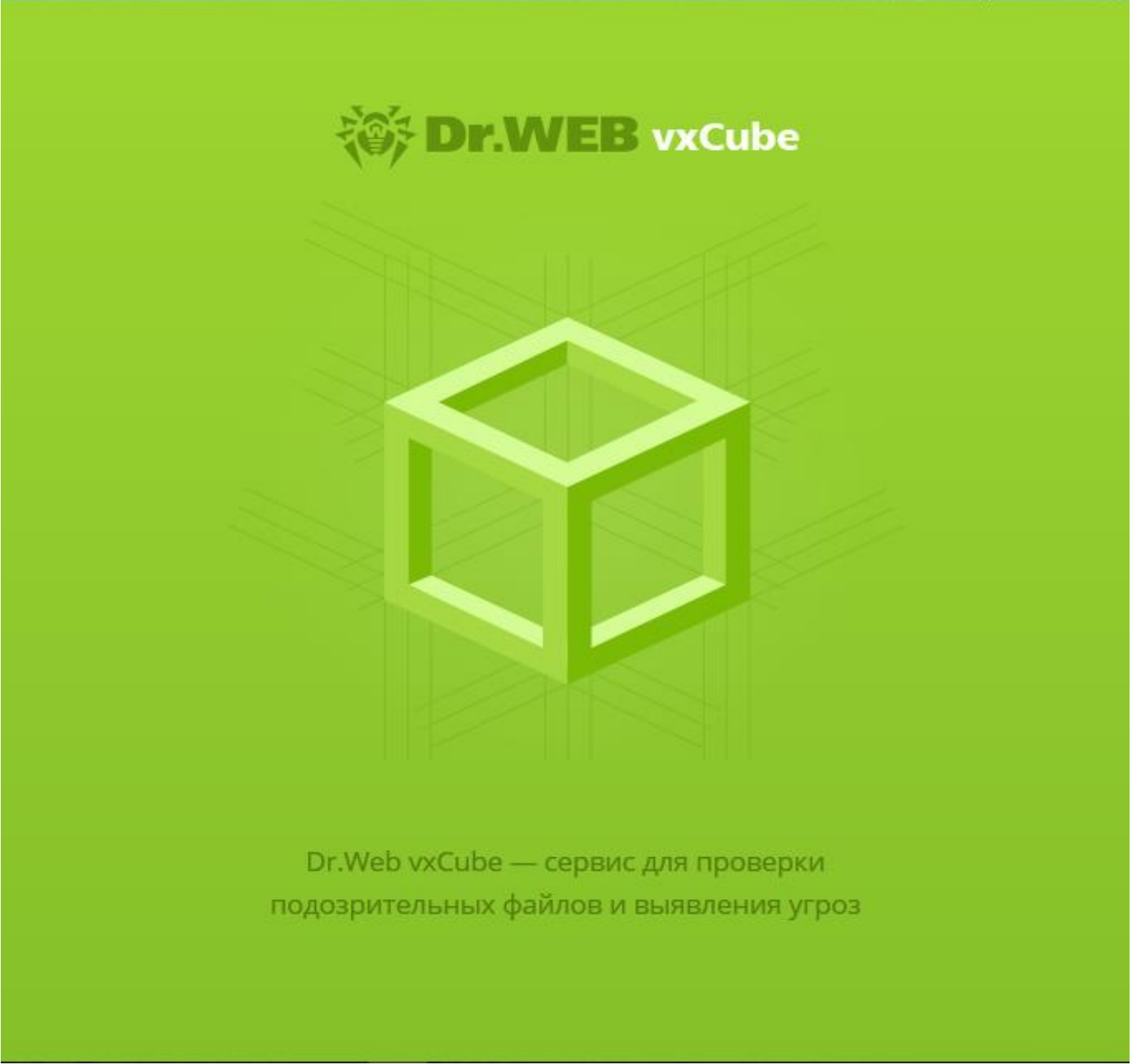
Вылечено	1
Удалено	13
Перемещен	2
Проигнорировано	0

Всего

Проверено	20
Объем данных (КБ)	3212
Время проверки	0000:00:08

Путь	Объекты	Действие
C:\new\1.js	Trojan.Browseban.based.2	Удалено
C:\new\22CC6C32.exe	Trojan.Winlock.3300	Удалено
C:\new\30.dat	Trojan.Carberp.30	Удалено
C:\new\514.zip	Trojan.Encoder.514	Перемещен
C:\new\647.exe	Trojan.Carberp.647	Удалено
C:\new\as.exe	Trojan.Winlock.4128	Удалено
C:\new\Builder.exe	MBRlock.Generator.1	Удалено
C:\new\calc[1].exe	Trojan.Winlock.4127	Удалено
C:\new\Download3.54521.zip	Trojan.DownLoad3.28161	Перемещен
C:\new\ibank.456.exe	Trojan.PWS.Ibank.456	Удалено
C:\new\igfxtray.#xe	Trojan.Carberp.10	Удалено
C:\new\KillAV.66.tmp	Trojan.KillAV.66	Удалено
C:\new\skype_05102012_image.exe	BackDoor.IRC.NgrBot.146	Удалено
C:\new\W97M.Siggen.1.xls	W97M.Siggen.1	Вылечено
C:\new\xxx_video.exe	Trojan.Winlock.2430	Удалено
C:\new\xxx_video_53239.avi.exe	Trojan.Winlock.2779	Удалено

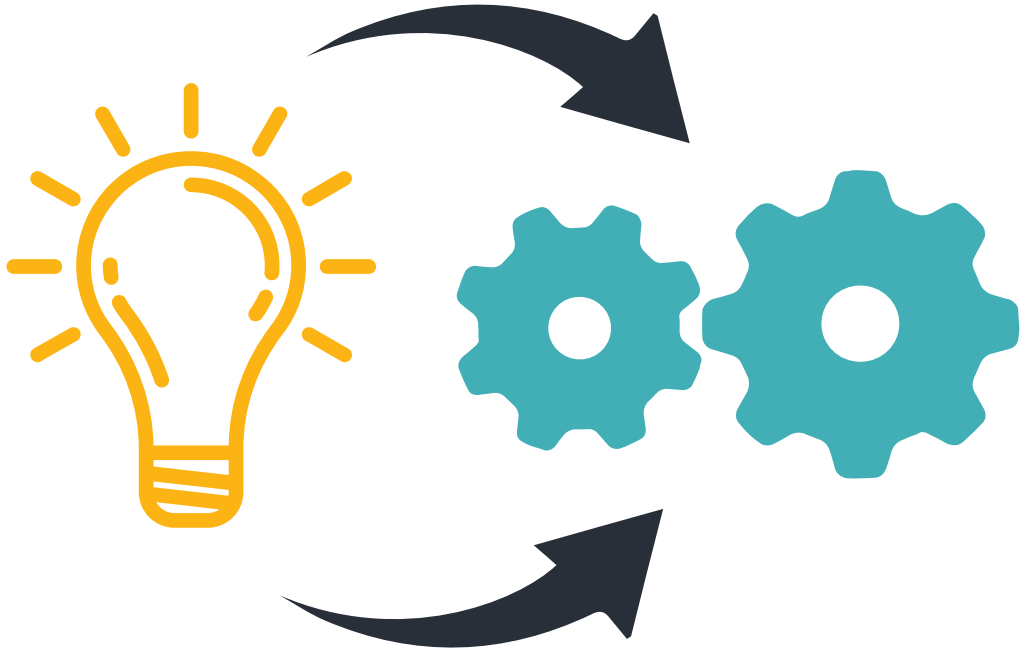




- Ежедневно на анализ поступает **до миллиона вредоносных файлов**.
- **Анализ** вредоносных файлов, сборка и тестирование обновлений, их выкладка на сервера обновлений **требует времени**.
- **Среднее время** появления информации в антивирусных базах на стороне пользователя **нулевым быть не может**.

Особенности

Dr.Web vxCube



01 Доступ VM в Интернет через прокси-сервер

02 Работа на уровне гипервизора

03 Журнал событий на уровне гипервизора - обнаружение анализатора невозможно

04 Возможность влиять на процесс анализа с помощью VNC-клиента

Windows XP x86

- Adobe Acrobat
- Adobe Flash 12.
- Microsoft Office
- JAVA 6u45
- Adobe Flash Sta
- Mozilla Firefox
- Opera 31.0.188
- Google Chrome
- ICQ 8.3 build 73
- QIP 2012 4.0.93
- Pidgin 2.10.11
- Mozilla Thunde
- Visual C++ Redis
- Visual C++ Redis
- Visual C++ Redis
- Visual C++ Redis
- Visual C++ Redis
- Visual C++ Redis
- .NET Framework
- .NET Framework
- .NET Framework
- .NET Framework
- .NET Framework
- .NET Framework
- Steam

Windows 7 x86

- Adobe Acrobat
- Adobe Flash 12.
- Adobe Flash Acti
- Microsoft Office
- JAVA 7u11
- Adobe Flash Star
- Mozilla Firefox 3
- Opera 33.0.1990
- Google Chrome
- ICQ 8.3 build 731
- QIP 2012 4.0.938
- Pidgin 2.10.11
- Mozilla Thunder
- Visual C++ Redis
- Visual C++ Redis
- Visual C++ Redis
- Visual C++ Redis
- Visual C++ Redis
- Visual C++ Redis
- .NET Framework
- .NET Framework
- .NET Framework
- Steam

Windows 7 x64

- Adobe Acrobat Reade
- Adobe Flash 18.0.0.2
- Adobe Flash ActiveX
- Microsoft Office 201
- JAVA 8u45 x64
- Adobe Flash Standalo
- K-Lite Mega Codec Pa
- Mozilla Firefox 37.0.2
- Opera 29.0.1795.47
- Google Chrome 42.0.
- ICQ 8.3 build 7317
- Mail.Ru Agent 6.4 bui
- QIP 2012 4.0.9380
- Pidgin 2.10.11
- Total Commander 8.5
- Mozilla Thunderbird
- Winamp 5.666
- Visual C++ Redistribu
- Visual C++ Redistribu
- Visual C++ Redistribu
- Visual C++ Redistribu
- Visual C++ redistribut
- Visual C++ Redistribu
- Visual C++ Redistribu
- Visual C++ Redistribu
- Visual C++ Redistribu
- Visual C++ Redistribu
- Visual C++ Redistribu
- Visual C++ Redistribu
- .NET Framework 1.1
- .NET Framework SDK
- .NET Framework 4.5.
- Steam

Windows 10 x64

- Adobe Acrobat Reader Document Cloud 2015.010.20060
- Adobe Flash 21.0.0.197
- Adobe Flash ActiveX 21.0.0.197
- Microsoft Office 2016
- JAVA 8u77 x64
- Adobe Flash Standalone 19.0.0.226 (%windir%\flash_sa.exe)
- Mozilla Firefox 45.0.1 x64
- Opera 36.0.2130.46
- Google Chrome 47.0.2526.80
- ICQ 8.3 build 7317
- QIP 2012 4.0.9380
- Pidgin 2.10.11
- Mozilla Thunderbird 38.7.1
- Visual C++ Redistributable 2005 x86
- Visual C++ Redistributable 2008 x86
- Visual C++ Redistributable 2010 x86
- Visual C++ Redistributable 2012 x86
- Visual C++ Redistributable 2013 x86
- Visual C++ Redistributable 2015 x86
- Visual C++ Redistributable 2005 x64
- Visual C++ Redistributable 2010 x64
- Visual C++ Redistributable 2012 x64
- Visual C++ Redistributable 2013 x64
- Visual C++ Redistributable 2015 x64
- .NET Framework 1.1
- .NET Framework SDK (msvcp70.dll, msvcr70.dll)
- .NET Framework 3.5
- Steam

Интерпретация результатов

1

Техническая информация

2

Файлы и дампы памяти

3

Журнал API

4

Карта сетевой активности

Журнал: все файлы

Имя файла	Формат	SHA1	Результаты анализа	Дата
payment0001.exe	EXE	8bc20b3adbbb486c3a5fdbc855653d463a2ae399	Win10 64-bit	15 мая
ООО Киа Моторс Россия и СНГ заказ.js	JS	f531c5cfdf65d214e9abffc92d47b9f1317f4436	Win10 64-bit	18 апр
Подробности заказа АО «Авиакомпания «РО...	JS	3528b93c40c1d3aed1c562ac6875dd8fe7abd83a	Win10 64-bit	27 мар
Подробности заказа.jse	JS	bea86236546da27967468be6177b63c3a18b4d...	Win10 64-bit	26 мар
Подробности заказа ПАО «Авиакомпания „...	JS	95ddcb93d0bbb777eb414c79bcee811fcdc2bc53	Win10 64-bit	24 мар
Подробности заказа ПАО «Авиакомпания „...	JS	c6e89abfc49935aecff14803200d1d8050c0dff1	Win10 64-bit	19 мар
details-20190319_175715.csv	XLSX	3d0d51ef49ce67ed99a0a33d482ac7240582a8f8	Win7 64-bit Win10 64-bit	19 мар
Пропуск.pdf.SAMBO	PDF	ef8c8b003b44abecf9346e1dcf432f6dc60310c4	Win10 64-bit	15 мар
Док-ты вторник.exe	EXE	063822a17c30594a2e4a01c5e2985583cb71d01d	Win10 64-bit	5 мар
MasVA.exe	EXE	83f298a2872fa40299ea2d0ec8fdaaac673bf0b6	Win10 64-bit	30 янв

1 2 3 4 5 Следующая страница →

Карта сетевой активности

менее 5 подключений | 5-10 подключений | более 10 подключений

TCP/IP	grupo-ocyr.com:80	HTTP GET http://www.grupo-ocyr.com/wp-content/themes/twentyseventeen/inc/hp.gf
TCP/IP	scottpatton.com:80	HTTP GET http://www.scottpatton.com/birthday/hp.gf
TCP/IP	194.109.206.212:443	{17,03,03,02,1a,84,2a,6a,e7,ef,e9,b1,67,78,8c,75,40,3f,7d,9d,31,8b,85,ec,97,fd,ae,77,ae,28,c3,65,70,cd,10,35,f0,7a,f7,1a,24,c4,05,c4,46,07,c9,1e,30,6d,2d,ae,f3,d7,65,8c,34,8a,94,62,f9,13,bb,e9,74,ec,77,57,f6,3e,7a,65,3d,0a,d1,a3,7a,55,7a,e0,fa,3a,24,c8,ef,ca,63,38,89,a2,38,0e,4b,ac,47,5b,a3,8b,b3,04,bb,8f,37,e8,04,13,97,17,07,81,e5,f4,8d,cb,e9,a7,73,6a,25,ae,f7,64,ba,4d,c6,3c,5f,5a,f4,60,06,e7,60,f3,c0,68,04,3d,5e,4a,40,53,21,43,e9,0a,1e,26,03,d8,45,0a,dc,46,60,2b,d0,0d,98,f5,12,97,e7,e1,cd,cc,d9,62,60,86,bf,dd,53,e3,d9,87,c9,e3,5d,05,2b,3c,82,b5,90,db,d0,98,3e,cd,57,22,4e,de,92,56,d2,a2,a9,76,d4,e1,d7,22,de,e3,d7,04,1e,8c,aa,72,d9,79,42,a0,b9,75,77,4d,10,a1,40,bf,67,dd,ae,38,ab,96,bb,d3,ef,c7,84,50,26,12,df,fe,b9,11,f3,d8,98,6c,5a,5b,35,9c,31,52,9a,11,88,50,0f,dd,f3,70,1d,2e,17,fc,3d,e0,70,b2,0f,b6,a4,25,fb,27,5a,b8,07,2e,d8,9c,69,4d,7e,a0,9c,5c,97,24,70,38,fe,58,58,5d,c1,3a,a4,60,bb,1b,84,ad,4a,b4,17,6d,4c,61,93,f6,0a,11,91,5e,b7,78,f9,e7,7b,c2,90,79,96,87,c0,b1,1b,24,3a,28,60,2c,74,9d,8a,77,a2,26,ee,ad,99,32,04,78,f2,41,a9,6b,0b,73,73,83,9c,67,5b,8a,ad,d7,ef,68,2c,2d,cb,35,1e,4c,0b,fd,4b,4e,20,c3,60,5c,fb,02,30,30,3d,8e,94,79,b9,5a,88,02,01,07,90,fc,6d,fd,a8,99,3a,81,4a,36,ce,1b,03,22,be,48,35,0f,09,c8,de,fa,87,84,e8,f8,c2,0c,46,13,e9,13,58,2b,73,d1,86,48,d9,3f,3f,6e,c6,9c,4f,5c,be,3e,f6,20,2f,70,34,ab,ed,72,1d,d4,1c,05,89,06,98,81,81,9c,6b,da,41,9d,3d,a2,9e,30,e9,73,d4,0e,05,30,15,e4,05,55,87,cf,b5,21,6c,cf,da,c6,26,a3,0e,a1,6a,d8,9d,f1,2e,78,82,6a,c6,67,57,aa,83,92,dd,e7,61,4c,0e,82,82,fa,d4,a3,ca,9a,4c,01,a7,8f,1c,7d,44,81,4f,a4,61,34,07,1c,97,0d,41,d1,4e,3a,5c,b1,0a,fc,30,72,06,7e,72,71,68,1c,65}
TCP/IP	131.188.40.189:443	{17,03,03,02,1a,14,07,3f,10,9b,4d,fa,6a,da,a8,76,cc,3f,d4,1f,be,89,c3,51,0d,7b,6f,f6,19,3b,73,29,c0,d5,4e,20,19,36,6d,63,8a,79,83,5f,4c,af,08,c2,4e,c4,ce,16,30,76,e9,50,15,6e,95,e8,9b,70,3a,bc,85,74,ca,14,7f,27,c7,c4,70,a8,06,3d,5c,3c,f6,59,17,f0,ea,94,a1,49,9b,91,d9,2f,af,02,d7,48,9d,89,a0,54,d0,0e,f5,72,51,98,de,00,e4,fd,62,95,6d,2e,bc,b3,b0,54,a2,66,81,3a,0a,ec,77,75,dd,b1,58,45,6d,a6,ac,a7,15,05,0c,0a,b7,e0,4e,59,8f,64,0e,96,fd,74,ed,e6,c6,3d,08,6c,83,6d,2d,47,b4,78,34,a4,e8,81,59,41,b2,91,2c,1a,17,b2,ed,7a,c5,49,bd,11,b2,e1,59,94,ed,7e,5a,8e,c5,4e,4f,4c,a1,93,c7,12,79,d4,7f,69,49,d1,c3,29,a5,c1,33,8d,0c,0b,1a,19,b0,9d,03,f2,fb,42,16,bf,38,f9,50,dc,88,0e,47,3f,ba,83,41,98,11,95,89,c1,54,88,f2,04,92,d1,5e,f0,a0,84,d7,04,87,93,63,b1,d0,5d,52,58,e5,61,49,69,88,0f,07,83,c7,5d,20,1e,05,cc,27,a7,a1,3b,3b,cb,00,bc,8b,40,82,fe,69,45,0c,54,86,6c,8b,5c,4e,6a,62,0e,22,c7,51,9d,b9,13,ee,76,20,86,05,1e,fa,4f,03,ec,d3,66,6e,61,a1,4f,5d,a3,9f,7e,eb,6e,6b,d5,9a,a8,0b,92,b9,ef,92,ca,7d,65,d7,11,eb,3c,88,46,d7,54,29,99,25,2d,7d,13,4d,d4,9d,c1,63,da,76,28,76,fd,47,cd,35,4f,4d,9f,ff,42,ab,74,7a,1d,95,e7,17,34,1e,35,ca,48,7e,e7,60,1b,c7,20,5d,5c,11,2a,25,bc,4f,6d,50,7f,b9,04,65,a3,01,87,db,be,28,35,9e,c6,96,9c,eb,f9,b6,51,14,bb,91,f2,e5,bc,97,e0,b1,6f,5b,ce,48,83,72,5e,03,d0,5a,73,8b,70,98,a7,3a,a8,8c,16,c2,b0,dd,d2,5d,5a,29,38,bb,1b,17,95,5c,f1,1b,7d,2e,d4,c9,7d,7f,f1,cf,70,18,d3,fa,c7,7e,ff,b6,a4,34,9d,c1,55,0f,d0,dc,6b,45,be,75,2e,af,86,2a,c8,cd,d4,69,34,d0,de,fd,af,e1,42,e6,8d,42,c1,bb,67,13,4a,d0,41,54,56,5e,53,c9,21,8d,da,5f,b5,e4,a2,56,f4,73,6c,dc,81,c6,b1,14,82,d4,b4,98,72,1d,66,b8,6a,cf,59,dc,49,92,f2,53,6e,9b}

- API 2.0
  - Объекты
    - Analysis
    - APIEvent
    - Call
    - Connection
    - Curelt
    - Dump
    - Drop
    - Format
    - Intent
    - License
    - Message
    - Platform
    - Sample
    - Session
    - Task
  - Эндпоинты
    - analyses
    - formats
    - license
    - login
    - platforms
    - samples
    - sessions
    - tasks
    - ws/progress

API 2.0 поддерживает формат JSON

- отправка файлов на анализ без участия человека;
- отправка файлов за меньшее количество времени;
- систематизация результатов программным путем

Dr.WEB®
с 1992 года

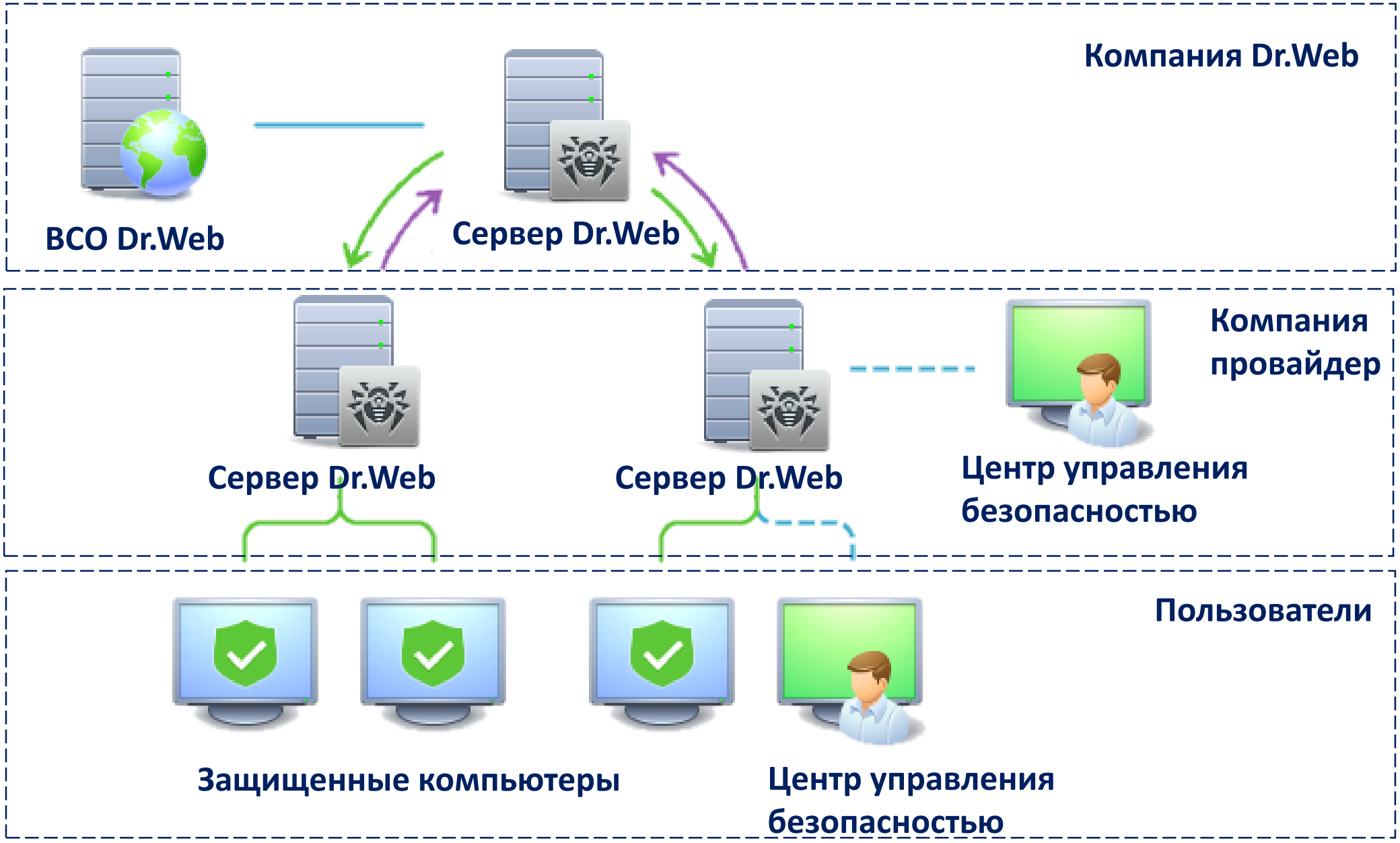
Интернет-сервис
Dr.Web® AV-Desk™

Безопасность как услуга

SaaS модель использования антивируса

Готовое программное обеспечение, полностью обслуживаемое провайдером

Как это работает?



Интернет-сервис
Dr.Web® AV-Desk™

Для дома и бизнеса

Для Windows/Server, macOS/Server, Linux, Android

Посуточная тарификация

Гибкое управление подпиской в личном кабинете

Услуга «Антивирус Dr.Web»

для

- **Разумная экономия**
- **Минимизация технических рисков**
- **Оптимизация труда персонала**
- **Экономия на серверном оборудовании**
- **Квалифицированное администрирование защиты**

Мгновенное подключение или отключение

Автоматическое продление- бесконечный антивирус

Расширение или сокращение защиты – когда угодно

Смена тарифа в любое время

Приостановка от 1 до 60 дней

Dr.WEB

Защити созданное

Спасибо за внимание

Вопросы?

+7 727 323 6 232
v.bugaev@drweb.kz
support@drweb.kz
www.drweb.ru
www.drweb.kz