



**«Доктор Веб»:  
обзор вирусной активности  
в феврале 2024 года**

## «Доктор Веб»: обзор вирусной активности в феврале 2024 года

Анализ статистики детектирований антивируса Dr.Web в феврале 2024 года показал рост общего числа обнаруженных угроз на 1,26% по сравнению с январем. При этом число уникальных угроз снизилось на 0,78%. Лидирующие позиции по количеству детектирований вновь заняли различные рекламные трояны и нежелательные рекламные программы. Кроме того, высокую активность сохранили вредоносные приложения, которые распространяются в составе других угроз и затрудняют их обнаружение. В почтовом трафике чаще всего выявлялись вредоносные скрипты, фишинговые документы, а также программы, которые эксплуатируют уязвимости документов Microsoft Office.

Число обращений пользователей за расшифровкой файлов снизилось на 7,02% по сравнению с предыдущим месяцем. Наиболее часто виновниками атак становились трояны-шифровальщики [Trojan.Encoder.3953](#) (18,27% инцидентов), [Trojan.Encoder.37369](#) (9,14% инцидентов) и [Trojan.Encoder.26996](#) (8,12% инцидентов).

На Android-устройствах наиболее часто вновь детектировались рекламные трояны семейства [Android.HiddenAds](#), активность которых значительно возросла.

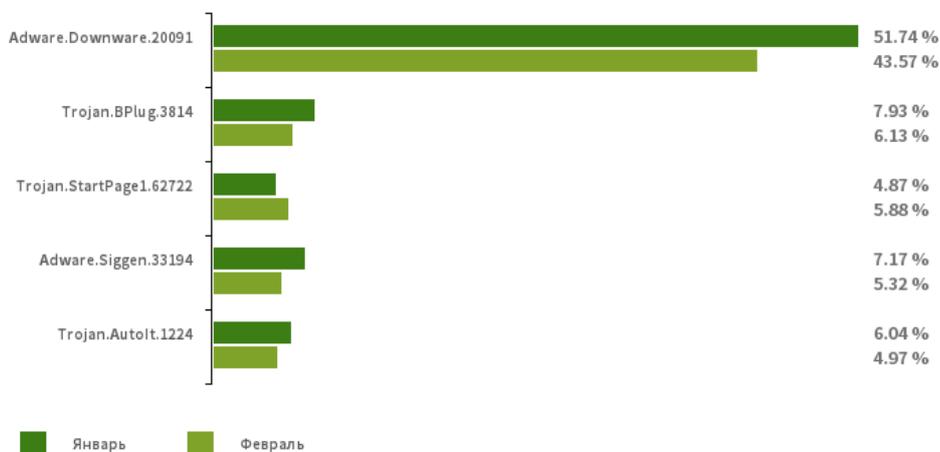
### Главные тенденции февраля

- Рост общего числа обнаруженных угроз
- Преобладание вредоносных скриптов и фишинговых документов во вредоносном почтовом трафике
- Снижение числа обращений пользователей за расшифровкой файлов, затронутых шифровальщиками
- Рост числа детектирований рекламных троянских приложений [Android.HiddenAds](#) на защищаемых устройствах

# «Доктор Веб»: обзор вирусной активности в феврале 2024 года

## По данным сервиса статистики «Доктор Веб»

Наиболее распространенное рекламное и вредоносное ПО в феврале 2024 года согласно данным сервиса статистики «Доктор Веб»



### Adware.Downware.20091

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

### Trojan.BPlug.3814

Детектирование вредоносного компонента браузерного расширения WinSafe. Этот компонент представляет собой сценарий JavaScript, который демонстрирует навязчивую рекламу в браузерах.

### Trojan.StartPage1.62722

Вредоносная программа, подменяющая стартовую страницу в настройках браузера.

### Adware.Siggen.33194

Детектирование созданного с использованием платформы Electron бесплатного браузера со встроенным рекламным компонентом. Этот браузер распространяется через различные сайты и загружается на компьютеры при попытке скачивания торрент-файлов.

### Trojan.AutoIt.1224

Детектирование упакованной версии троянской программы [Trojan.AutoIt.289](#), написанной на скриптовом языке AutoIt. Она распространяется в составе группы из нескольких вредоносных приложений — майнера, бэкдора и модуля для самостоятельного распространения. [Trojan.AutoIt.289](#) выполняет различные вредоносные действия, затрудняющие обнаружение основной полезной нагрузки.

# «Доктор Веб»: обзор вирусной активности в феврале 2024 года

## Статистика вредоносных программ в почтовом трафике



### JS.Inject

Семейство вредоносных сценариев, написанных на языке JavaScript. Они встраивают вредоносный скрипт в HTML-код веб-страниц.

### HTML.FishForm.365

Веб-страница, распространяющаяся посредством фишинговых рассылок. Представляет собой фиктивную форму ввода учетных данных, которая имитирует авторизацию на известных сайтах. Введенные пользователем данные отправляются злоумышленникам.

### Trojan.PackedNET.2511

Вредоносное ПО, написанное на VB.NET и защищенное программным упаковщиком.

### Exploit.CVE-2018-0798.4

Эксплойты для использования уязвимостей в ПО Microsoft Office, позволяющие выполнить произвольный код.

### W97M.DownLoader.2938

Семейство троянов-загрузчиков, использующих уязвимости документов Microsoft Office. Они предназначены для загрузки других вредоносных программ на атакуемый компьютер.

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

## «Доктор Веб»: обзор вирусной активности в феврале 2024 года

### Шифровальщики

В феврале 2024 года число запросов на расшифровку файлов, затронутых троянскими программами-шифровальщиками, снизилось на 7,02% по сравнению с январем.

Количество запросов на расшифровку, поступивших в службу технической поддержки «Доктор Веб»



Наиболее распространенные энкодеры февраля:

- Trojan.Encoder.3953 — 18.27%
- Trojan.Encoder.35534 — 9.14%
- Trojan.Encoder.26996 — 8.12%
- Trojan.Encoder.29750 — 0.51%
- Trojan.Encoder.37400 — 0.51%

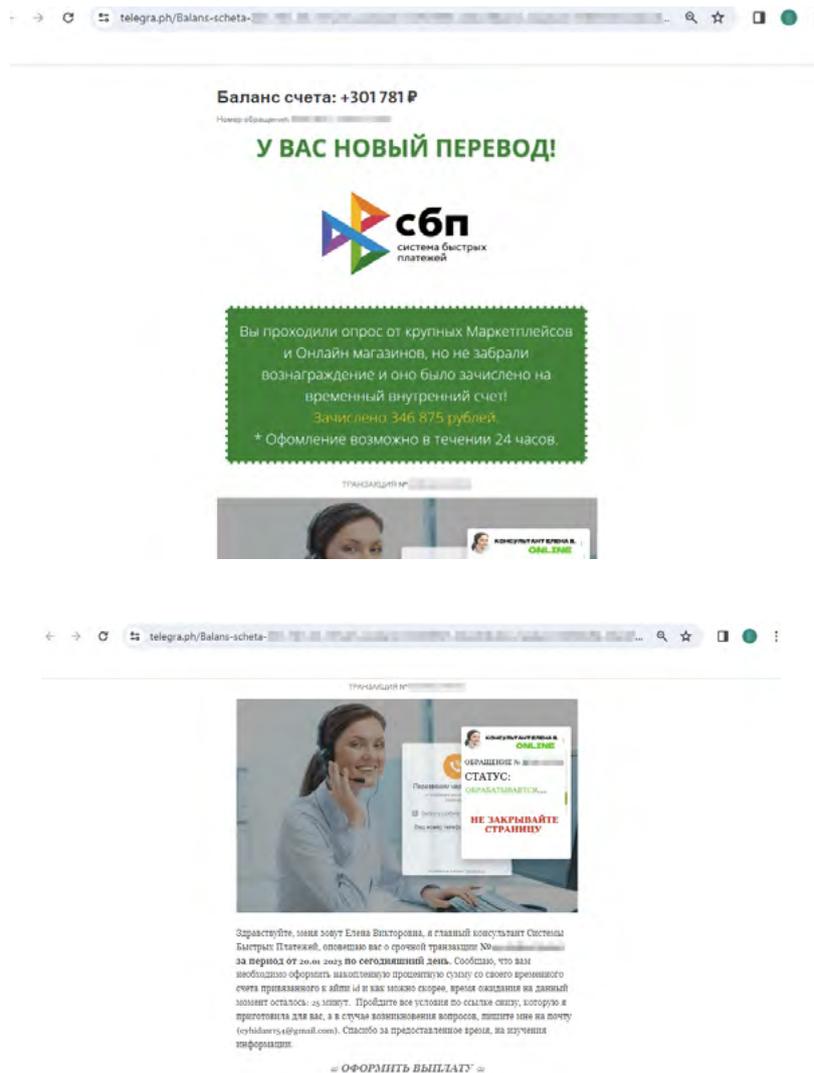
Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

# «Доктор Веб»: обзор вирусной активности в феврале 2024 года

## Опасные сайты

В феврале 2024 года интернет-аналитики компании «Доктор Веб» продолжили выявлять нежелательные сайты различной тематики. Так, популярностью среди злоумышленников стали пользоваться сайты, информирующие потенциальных жертв о доступности для них неких денежных переводов. Для «получения» этих средств пользователи должны заплатить «комиссию» за межбанковский перевод. Ссылки на подобные сайты распространяются в том числе через блог-платформу Telegraph.

Ниже представлен пример такой публикации. Потенциальным жертвам предлагается в течение 24 часов «забрать» вознаграждение, якобы полученное после участия в опросе интернет-магазинов:



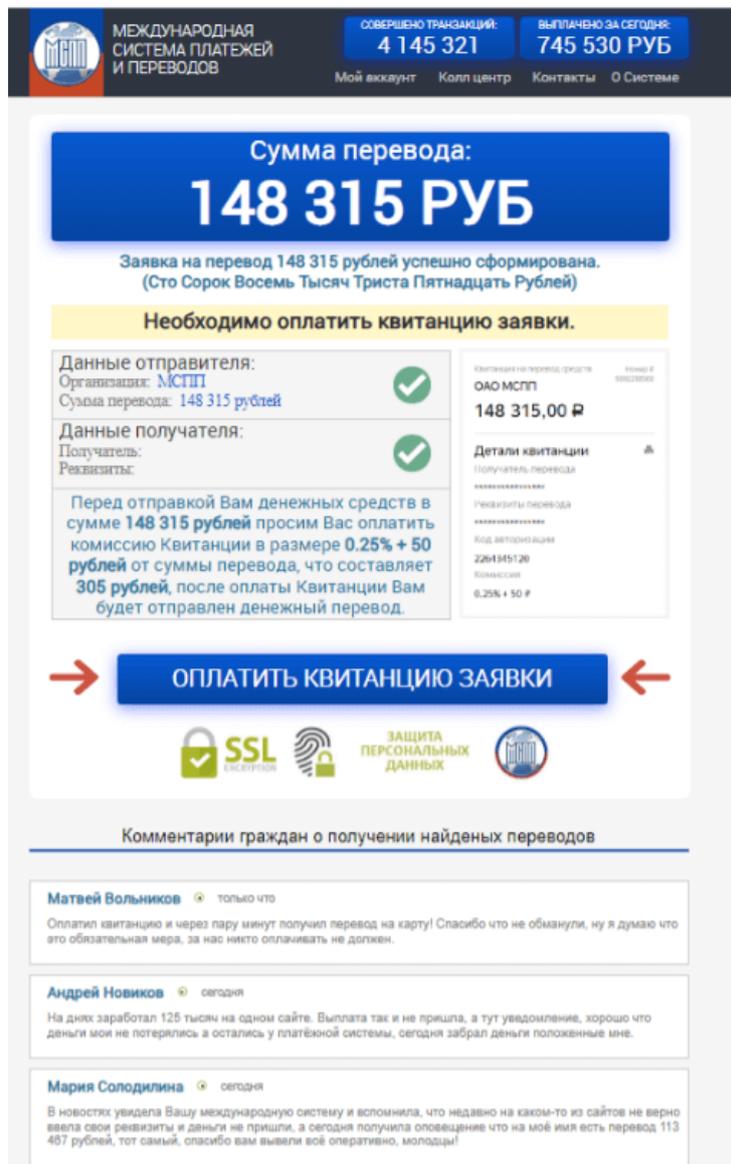
Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

## «Доктор Веб»: обзор вирусной активности в феврале 2024 года

### Опасные сайты

При нажатии на ссылку «ОФОРМИТЬ ВЫПЛАТУ» пользователь перенаправляется на мошеннический сайт некой «Международной Системы Платежей и Переводов», где ему якобы доступно получение обещанной выплаты:



The screenshot shows a website for "МЕЖДУНАРОДНАЯ СИСТЕМА ПЛАТЕЖЕЙ И ПЕРЕВОДОВ" (International Payment and Transfer System). The header includes a logo, the company name, and statistics: "ОСОВЕРШЕНО ТРАНЗАКЦИЙ: 4 145 321" and "ВЫПЛАЧЕНО ЗА СЕГОДНЯ: 745 530 РУБ". Navigation links include "Мой аккаунт", "Колл центр", "Контакты", and "О Системе".

The main content area displays "Сумма перевода: 148 315 РУБ" and states: "Заявка на перевод 148 315 рублей успешно сформирована. (Сто Сорок Восемь Тысяч Триста Пятнадцать Рублей)". A yellow banner reads "Необходимо оплатить квитанцию заявки." (It is necessary to pay the invoice for the application).

There are two columns of information:

- Данные отправителя:** Организация: МСПП, Сумма перевода: 148 315 рублей. Status: ✓
- Данные получателя:** Получатель, Реквизиты. Status: ✓

A text box explains: "Перед отправкой Вам денежных средств в сумме 148 315 рублей просим Вас оплатить комиссию Квитанции в размере 0.25% + 50 рублей от суммы перевода, что составляет 305 рублей, после оплаты Квитанции Вам будет отправлен денежный перевод." (Before sending you money in the amount of 148,315 rubles, we ask you to pay the invoice commission in the amount of 0.25% + 50 rubles from the sum of the transfer, which amounts to 305 rubles, after paying the invoice you will be sent a money transfer).

Below this is a table for "Детали квитанции" (Invoice details):

Квитанция на перевод средств	Имя и телефон
ОАО МСПП	
148 315,00 Р	
Детали квитанции	
Получатель перевода	*****
Реквизиты перевода	*****
Код авторизации	
2261345120	
Комиссия	0.25% + 50 Р

A large blue button with red arrows says "ОПЛАТИТЬ КВИТАНЦИЮ ЗАЯВКИ" (PAY INVOICE FOR APPLICATION). Below it are security logos: SSL, ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ, and a globe icon.

At the bottom, there is a section "Комментарии граждан о получении найденных переводов" (Comments from citizens about receiving found transfers). It contains three testimonials:

- Матвей Вольников** (only today): "Оплатил квитанцию и через пару минут получил перевод на карту! Спасибо что не обманули, ну я думаю что это обязательная мера, за нас никто оплачивать не должен." (Paid the invoice and after a few minutes I received the transfer to the card! Thank you that you didn't cheat, I think that this is a necessary measure, no one should pay for us.)
- Андрей Новиков** (today): "На днях заработал 125 тысяч на одном сайте. Выплата так и не пришла, а тут уведомление, хорошо что деньги мои не потерялись а остались у платёжной системы, сегодня забрал деньги положенные мне." (A few days ago I earned 125 thousand on one site. The payment didn't come, but here is a notification, good that my money wasn't lost and remained in the payment system, today I took the money I deserved.)
- Мария Солодилина** (today): "В новостях увидела Вашу международную систему и вспомнила, что недавно на каком-то из сайтов не верно ввела свои реквизиты и деньги не пришли, а сегодня получила оповещение что на моё имя есть перевод 113 487 рублей, тот самый, спасибо вам вывели всё оперативно, молодцы!" (I saw your international system in the news and remembered that recently on one of the sites I entered my details incorrectly and the money didn't come, and today I received a notification that there is a transfer of 113,487 rubles in my name, that's the one, thank you for everything, you did it quickly, well done!)

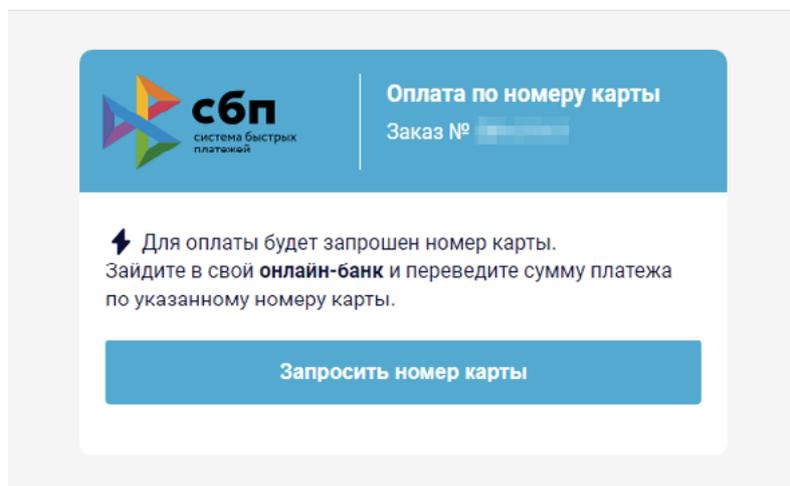
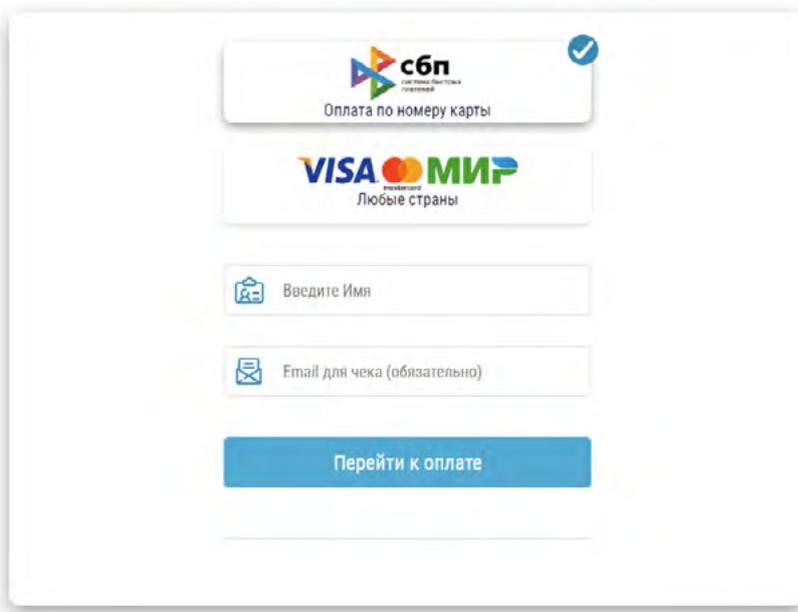
Для «получения» денег пользователь вначале должен указать персональные данные — имя и адрес электронной почты, а затем заплатить «комиссию» через Систему быстрых платежей (СБП) за «перевод» ему несуществующего вознаграждения. При этом в качестве способа оплаты «комиссии» мошенники указывают перевод денег по номеру банковской карты через

## «Доктор Веб»: обзор вирусной активности в феврале 2024 года

онлайн-банк, в то время как СБП предусматривает переводы только по номеру мобильного телефона. В данном случае злоумышленники могут целенаправленно спекулировать на набирающем в России популярность способе перевода денег в расчете на низкую финансовую грамотность пользователей. Если жертва согласится заплатить «комиссию», она переведет собственные деньги на подконтрольную мошенникам банковскую карту. В то же время нельзя исключать, что в попытке украсть у пользователей деньги злоумышленники в будущем действительно станут использовать СБП.

### Оплата квитанции

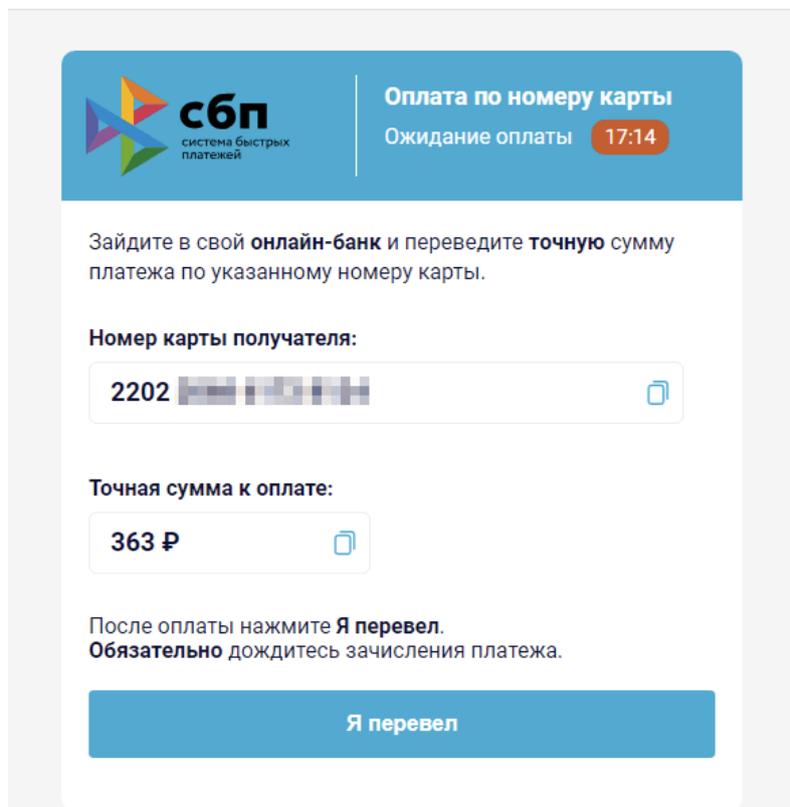
- Заказ № [REDACTED]
- К оплате 305 Р + комиссия



Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

## «Доктор Веб»: обзор вирусной активности в феврале 2024 года



The screenshot shows a payment interface for 'сбп система быстрых платежей' (SBP). The header includes the logo and the text 'Оплата по номеру карты' (Payment by card number) with a timer 'Ожидание оплаты 17:14'. The main text instructs the user to go to their online bank and transfer the exact amount. There are two input fields: one for the card number (starting with 2202) and one for the amount (363 RUB). A 'Я перевел' (I transferred) button is at the bottom. A warning message states: 'После оплаты нажмите Я перевел. Обязательно дождитесь зачисления платежа.' (After payment, click I transferred. You must wait for the payment to be credited.)

Узнайте больше о нерекомендуемых Dr.Web сайтах

## «Доктор Веб»: обзор вирусной активности в феврале 2024 года

### Вредоносное и нежелательное ПО для мобильных устройств

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в феврале 2024 года на защищаемых устройствах наиболее часто вновь выявлялись троянские программы [Android.HiddenAds](#), демонстрирующие нежелательную рекламу. Их активность по сравнению с январем возросла на 73,26%. При этом рекламные троянские программы другого семейства, [Android.MobiDash](#), атаковали пользователей на 58,85% реже.

Число детектирований шпионских троянов [Android.Spy](#) снизилось на 27,33%, а банковских троянов — на 18,77%. В то же время вредоносные программы-вымогатели [Android.Locker](#) выявлялись на 29,85% чаще.

Наиболее заметные события, связанные с «мобильной» безопасностью в феврале:

- значительный рост активности рекламных троянских программ [Android.HiddenAds](#),
- снижение числа атак банковских троянов и шпионских троянских приложений,
- рост числа атак вредоносных программ-вымогателей.

Более подробно о вирусной обстановке для мобильных устройств в феврале читайте в нашем [обзоре](#).

## «Доктор Веб»: обзор вирусной активности в феврале 2024 года

### О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

### Полезные ресурсы

[Центр противодействия кибер-мошенничеству](#)

### Пресс-центр

[Официальная информация](#) | [Контакты для прессы](#) | [Брошюры](#) | [Галерея](#)

### Контакты

Центральный офис

125124 Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

[www.антивирус.рф](http://www.антивирус.рф) | [www.drweb.ru](http://www.drweb.ru)

[«Доктор Веб» в других странах](#)



© ООО «Доктор Веб»,  
2003

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)