

# Практическая работа

## Работа с онлайн-сервисами для проверки сайтов на вирусы

Заражение сайта вирусами — риск, который есть практически у каждого ресурса, что может привести к серьёзным последствиям: сбоям в работе сайта, краже данных пользователей или блокировке страницы.

И, если сегодня вы сделали всё возможное, чтобы обезопасить сайт, это не значит, что завтра ваш сайт не попробуют атаковать новыми методами или новым вредоносным кодом. Что делать в этом случае и как проверить свой ресурс? На помощь приходят веб-сканеры, которые выполняют анализ сайта. Сегодня расскажем о том, как понять, что ваш ресурс заражён, и сервисах, где можно проверить сайт на вирусы самостоятельно.

Согласно [исследованию](#) компании Acunetix, более 87% сайтов имеют уязвимости среднего уровня, а 46% веб-ресурсов имеют высокий риск заражения вирусами. Это значит, что регулярная проверка на вирусы актуальна для любого сайта.

Проверка сайта на вирусы делится на два основных типа:

1. **Проверка контента.** Самый простой способ, которым злоумышленники могут заразить сайт — через контент. Представим, что на вашем ресурсе есть поля для комментариев. Именно через них хакер может разместить вирусный файл.
2. **Проверка кода.** В этом случае проверяется все элементы сайта. Это может быть долго, но подождать определённо стоит. Особенно, когда ваш сайт используется в коммерческих целях и принимает денежные платежи.

## Как понять, что сайт заражён

Даже когда кажется, что всё в порядке, вы сможете заметить «звоночки», говорящие о заражении веб-ресурса. Вот некоторые из них:

- Аномальное увеличение нагрузки исходящего трафика.

- Появление в поисковой выдаче при ссылке на сайт пометки о том, что данный ресурс может угрожать вашему компьютеру.
- Предупреждения от вашего антивируса о небезопасности сайта.
- Появление подозрительных перенаправлений на сторонние ресурсы.
- Заметное «торможение» в работе сайта и прочие неполадки.
- Появление новых файлов и папок, изменение даты файлов и так далее.
- Вам приходят тревожные предупреждения со стороны хостинг-провайдера.

При появлении одного или нескольких тревожных сигналов, обязательно нужно проверить сайт в специальных сервисах.

## Сервисы для проверки сайта

Чтобы воспользоваться ими, вам не нужно устанавливать что-либо на компьютер или сайт, достаточно указать URL и нажать «Проверить».

### Проверка сайта на вирусы с помощью поисковых систем

Первым делом стоит проверить свой сайт в популярных поисковиках — Google и Яндекс. Оба поисковика ведут «чёрные» списки и проверяют сайты на предмет заражения, сразу блокируя опасное содержимое. Единственное, что не могут гарантировать эти поисковые системы — диагностику отсутствия вирусов или троянов в файлах веб-ресурса.

[Yandex Site status check](#)

Yandex

## Site status check

Thanks to Safe Browsing technology, Yandex checks millions of URLs every day and detects thousands of unsecured web resources, many of which were not created by hackers but have since been hacked. For such sites you will see a warning from Yandex in search results or in the browser. You can check whether it is dangerous to visit a particular site.

Check URL

Check

[Google безопасный просмотр](#)

# Безопасный просмотр: статус сайта

С помощью Безопасного просмотра мы ежедневно проверяем миллиарды URL и находим тысячи вредоносных веб-ресурсов, многие из которых создавались отнюдь не злоумышленниками, но потом были взломаны. Для таких сайтов Google показывает предупреждения в результатах поиска в браузере, чтобы защитить пользователей.

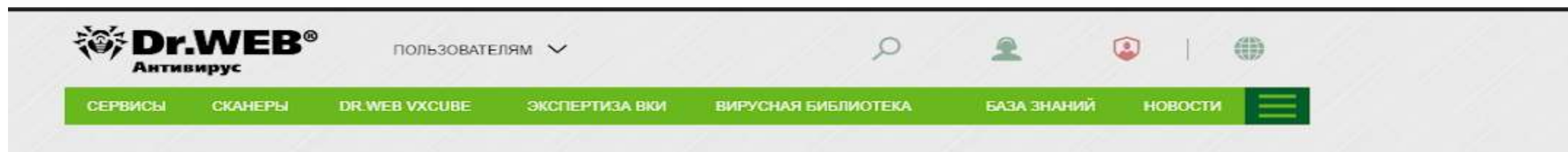
Проверить сайт

Укажите URL

После этой проверки можно переходить к наиболее популярным онлайн-сканерам.

## [Dr.Web](#)

Всё, что нужно, ввести URL сайта в соответствующее окошко и нажать «Отправить», после чего Доктор Веб проверит уязвимые файлы и предоставим вам отчёт. Меню – АВ-Лаборатория:



## Проверить ссылку (URL)

Иногда чтобы заразиться, достаточно попасть на вредоносный или мошеннический сайт, особенно если у вас нет антивирусной защиты. Даже легитимные интернет-ресурсы могут быть взломаны злоумышленниками. А еще есть сайты, при посещении которых с компьютера ничего страшного не случится, а вот зайдя на него со смартфона, вы будете тайно перенаправлены на сайт с неприятным «сюрпризом». С помощью взломанных сайтов злоумышленники могут распространять различные вредоносные программы, самыми «популярными» из которых являются различные модификации [Android.SmsSend](#). Потери жертвы зависят от того, троянец какого семейства внедрится в мобильное ваше устройство, — т. е. от его вредоносного заряда. Подробности об этом явлении читайте в нашей [новости](#).

Если сайт вызывает подозрение, проверьте его через эту форму до того, как нажимать на неизвестную ссылку.

Добавьте форму онлайн-проверки файлов и ссылок (URL) в код своего сайта, и любой его посетитель сможет бесплатно пользоваться этим сервисом.

[Скачать код формы](#) ↓

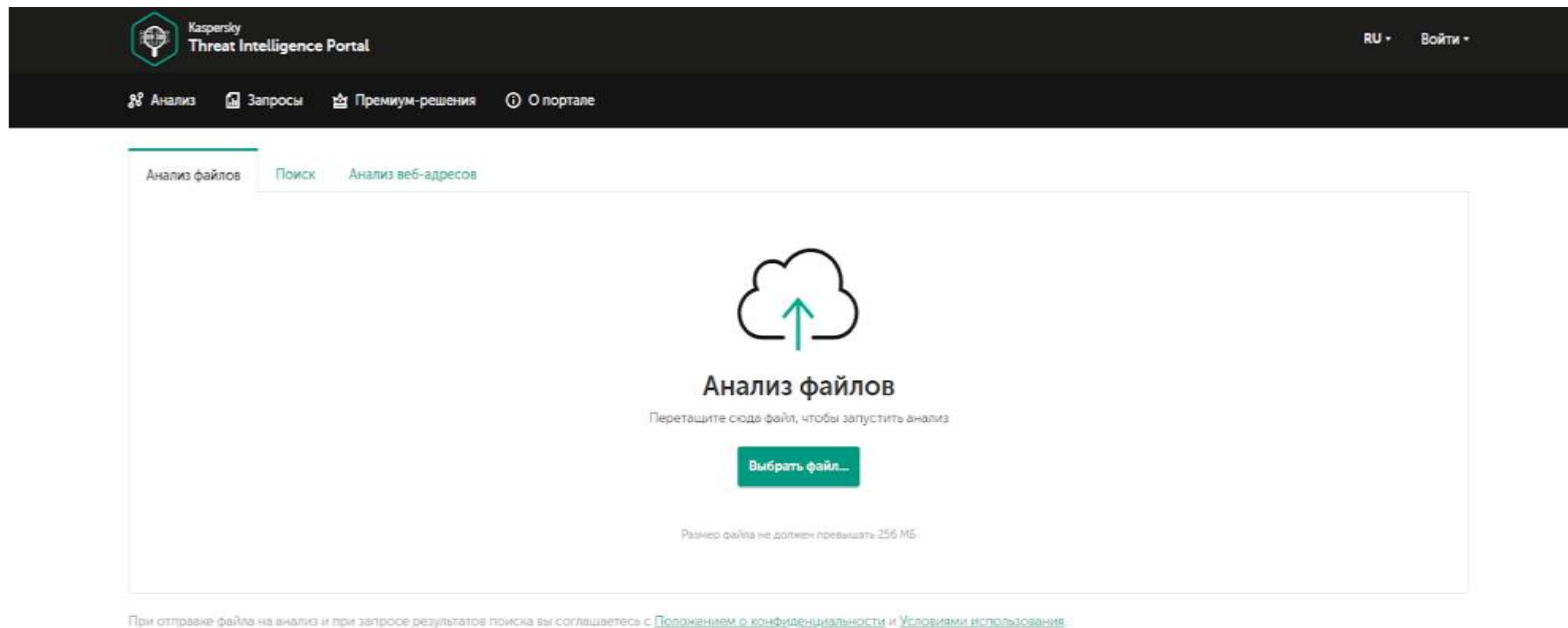
## URL-фильтр Dr.Web

Установите на мобильное устройство **Dr.Web Security Space для Android** с компонентом [URL-фильтр](#). Этот модуль ограничит доступ к нерекомендуемым и потенциально опасным сайтам по нескольким категориям, что особенно актуально для защиты ваших детей от нежелательного интернет-контента.

**URL-фильтр** присутствует только в полнофункциональной версии Dr.Web для Android (его нет в Dr.Web для Android Lite). Для покупателей

# Kaspersky Threat Intelligence Portal

Наверное, один из самых популярных русскоязычных антивирусов, который выполняет и проверку сайтов. В нём можно проверить файлы размером до 50 МБ простым перетаскиванием мышкой. После проверки пользователь получит результат в виде отчёта, которая может содержать три статуса: плохая репутация, хорошая или неизвестная. <https://opentip.kaspersky.com/>



The screenshot shows the Kaspersky Threat Intelligence Portal interface. At the top, there is a dark navigation bar with the Kaspersky logo and the text "Kaspersky Threat Intelligence Portal" on the left, and "RU" and "Войти" on the right. Below this, a secondary navigation bar contains icons and labels for "Анализ", "Запросы", "Премиум-решения", and "О портале". The main content area has three tabs: "Анализ файлов" (selected), "Поиск", and "Анализ веб-адресов". In the center of the "Анализ файлов" tab, there is a large icon of a cloud with an upward-pointing arrow. Below the icon, the text reads "Анализ файлов" and "Перетащите сюда файл, чтобы запустить анализ". A prominent green button labeled "Выбрать файл..." is positioned below the text. At the bottom of the main area, a small note states "Размер файла не должен превышать 256 МБ". At the very bottom of the screenshot, a line of text reads: "При отправке файла на анализ и при запросе результатов поиска вы соглашаетесь с [Положением о конфиденциальности](#) и [Условиями использования](#)."

"Лаборатория Касперского" признана лидером в  
отчёте международного аналитического  
агентства Forrester Wave™:  
External Threat Intelligence Services, Q1 2021

# QUTTERA

Абсолютно бесплатный сервис, ориентированный на зарубежные сайты, но отлично справляется и с проверкой доменов Рунета. Хорошо обнаруживает угрозы, связанные с загрузкой или размещением троянов, завирусированных исполняемых файлов и проверяет репутацию ресурса в чёрных списках.

The screenshot shows the Quttera website homepage. At the top is a navigation bar with the Quttera logo, links for Home, Products, Partners, Plans & Pricing, About Us, and Quttera Labs, and buttons for Sign up and Sign in. The main content area features a large heading: "You want to run a malware-free website. We want to help." Below this is a sub-heading: "Get malware scanning & removal, web application firewall, domain blacklist check, and other essential tools for the safe and trusted website." To the right is a video player for "THREATSIGN! WEBSITE ANTI-MALWARE" with a "Sign up to ThreatSign! plan now" button. Below the heading are two buttons: "Sign in to THREATSIGN dashboard" and "About malware removal". A second section features a carousel slide with a background image of a computer monitor displaying "UNAVAILABLE" and a warning sign. The slide text asks "Your web host disabled your website?" and lists services: "Detect malware source & attack vector", "Enable HTTP-based monitoring", "Enable FTP-based monitoring", "Security audit by experts", and "Detailed scanning reports". A button at the bottom of the slide says "Fix site & get back online now". Below the carousel, it says "Among supported platforms:" followed by logos for WordPress, Joomla!, Drupal, Bulletin, SharePoint, Joomla!, and Magento. At the bottom is a search bar with the text "Scan website for free", a text input field "What's your website?", an "Enter URL" button, and a "Scan for Malware" button.

Quttera Home Products Partners Plans & Pricing About Us Quttera Labs Sign up Sign in

## You want to run a malware-free website. We want to help.

Get malware scanning & removal, web application firewall, domain blacklist check, and other essential tools for the safe and trusted website.

Sign in to THREATSIGN dashboard About malware removal

### THREATSIGN! WEBSITE ANTI-MALWARE

Sign up to ThreatSign! plan now

### Your web host disabled your website?

Detect malware source & attack vector

- Enable HTTP-based monitoring
- Enable FTP-based monitoring
- Security audit by experts
- Detailed scanning reports

Fix site & get back online now

Among supported platforms:

WordPress Joomla! Drupal Bulletin SharePoint Joomla! Magento

Scan website for free What's your website? Enter URL Scan for Malware »

## Sucuri

Платный сервис, который проводит эвристический анализ по собственному алгоритму проверки.

*Эвристический анализ — метод обнаружения вирусов и вредоносного ПО, которого нет в базах (вирусных сигнатурах), через изучение фрагментов кода и сравнения их с известными вирусными угрозами.*

Sucuri хорош тем, что обнаруживает спам-ссылки и опасные скрипты, проверяет актуальность версий CMS и веб-серверов. Для использования надо зарегистрироваться и выбрать тарифный план. Несмотря на то, что цены могут показаться высокими, сервис предлагает полную поддержку и даже удаление вредоносного кода специалистами.

**SUCURI** Products Features Pricing Resources **Immediate Help** Login

### We Clean and Protect Websites

Gain peace of mind by securing all your websites. We fix hacks and prevent future attacks. A cloud-based platform for every site.

[Fix Hacked Site](#) [Learn More](#)

- WAF Protection**  
Defend your website against hacks and DDoS attacks with our WAF.  
[Learn More >>](#)
- Monitoring**  
Identify indicators of compromise with various alerting options.  
[Learn More >>](#)
- Incident Response**  
Unlimited malware removal and premium response SLAs.  
[Learn More >>](#)
- Performance Boost**  
Lightning fast page speed with our highly optimized CDN.  
[Learn More >>](#)

[Sucuri Cookie Policy](#) x

# VirusTotal

Можно сказать, что это настоящая «рок-звезда» подборки. Вам не нужно регистрироваться и платить — достаточно вставить ссылку, загрузить файл или найти страницу в поисковике. Сервис просто выдаст результат онлайн проверки сайта на вирусы, показав оценку свыше 65-ти антивирусных систем. <https://www.virustotal.com/>

[Intelligence](#) [Hunting](#) [Graph](#) [API](#)



[Sign in](#)

[Sign up](#)



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE

URL

SEARCH



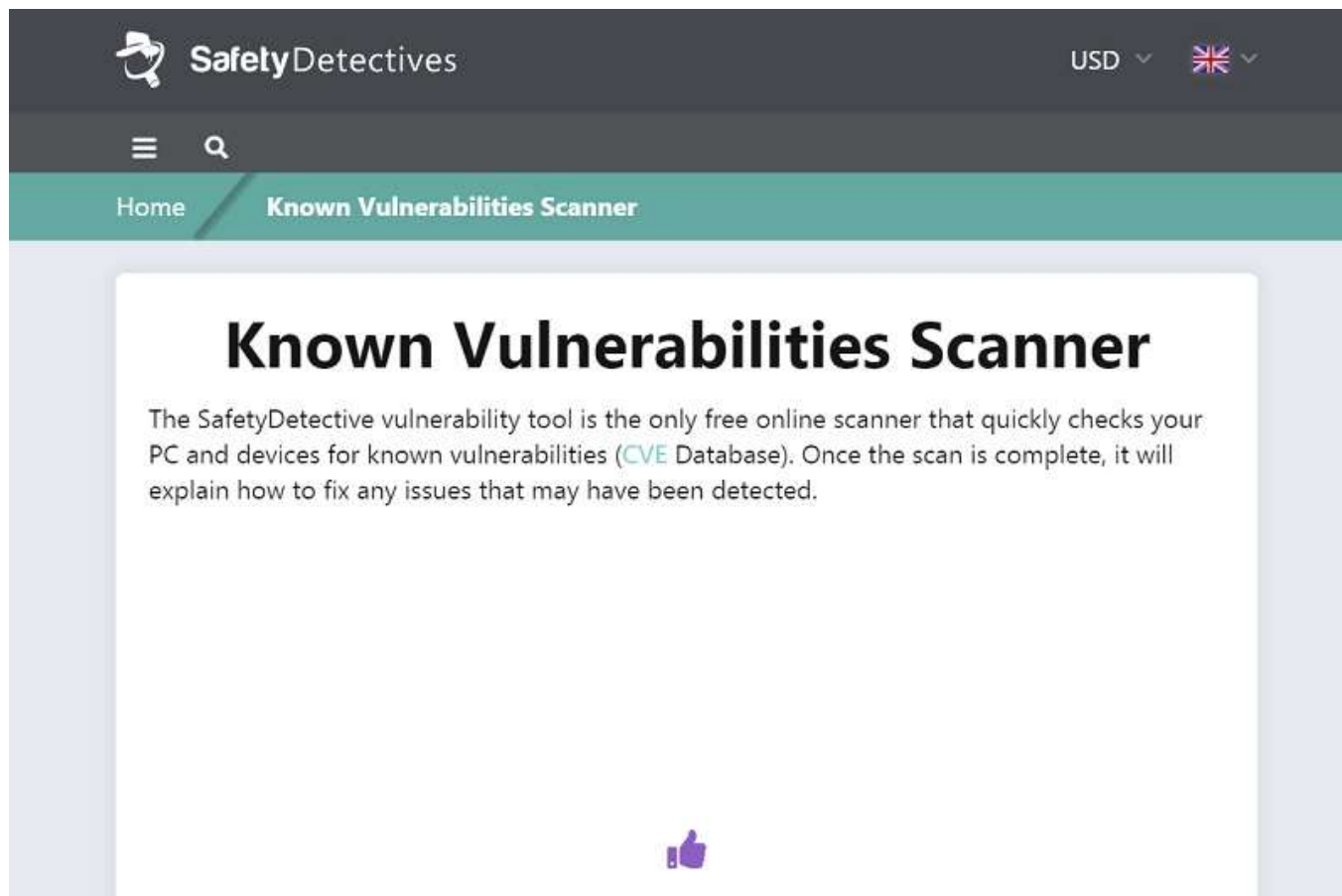
By submitting data below, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more.](#)

[Choose file](#)

Want to automate submissions? [Check our API](#), free quota grants available for new file uploads



# SAFETY DETECTIVE VULNERABILITIES SCANNER



Один из самых популярных сервисов, полностью бесплатный и позволяющий просканировать систему на наличие уязвимостей. После такого сканирования, на которое понадобится не больше нескольких минут, утилита предупреждает о возможных проблемах. Среди отличий от других похожих сервисов – высокая эффективность определения вирусов и отсутствие необходимости скачивать какие-либо файлы на ПК. А ещё – бесплатное использование и кроссплатформенность.

Минусы Safety Detective Vulnerabilities Scanner – обнаруженные проблемы не исправляются. Чтобы удалить такие вирусы, придётся использовать более эффективные средства. Зато работает сервис намного быстрее любого антивируса.

# Профилактика вирусного поражения сайта

- Регулярно (желательно с периодичностью раз в неделю) делайте бэкапы сайта. Подробнее о бэкапах читайте в тематическом посте «[Нет бэкапа — жди факапа, или Почему важно вовремя делать резервные копии](#)».
- Проверяйте бэкап антивирусом.
- Подключите к системе оповещения о возникших выявленных проблемах на сайте, например, можно воспользоваться Yandex.Метрикой.
- Регулярно обновляйте программное обеспечение.
- Меняйте пароли и используйте [менеджеры паролей](#)
- Контролируйте входящий и исходящий трафик.
- И, конечно же, регулярно сканируйте сайт на вирусы.

## Дополнительное задание

1. Проверить файл с помощью virustotal
2. Проверить компьютер с помощью Dr. Web Cureit