

ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Парольная защита

- Не использовать простые пароли (например, ФИО пользователя, qwerty, ra\$\$w0rd, 12345 и т.п.) Пароли должны быть не менее 6 символов и содержать не менее 3-х цифр, 3-х букв, из них не менее одной букву заглавной и одной строчной;
- Сохранять личный пароль в тайне. Не сообщать пароль другим лицам. Не хранить записанный пароль на общедоступных местах (на мониторе, под клавиатурой и т.д.);
- Если при необходимости пароль на время передавался другому сотруднику, то по завершению работ, этот пароль нужно сменить;
- При смене пароля новый пароль должен отличаться от старого не менее, чем двумя символами;
- Не использовать личные пароли (например, от социальных сетей, личной почты и т.д.) для служебных программ и наоборот;
- Не сохранять пароли в программах или браузере для интернет-банков, личных кабинетов платежных систем и других сервисов с персональной, коммерческой и иной информации конфиденциального характера;
- При временном оставлении рабочего места в течение рабочего дня необходимо в обязательном порядке заблокировать компьютер нажатием комбинации клавиш «Win + L» или «Ctrl+Alt+Delete» и выбрать функцию заблокировать компьютер.

Антивирусная защита

- На компьютере, подключенном к локальной сети или сети Интернет должен быть установлен антивирус. Если его нет, то необходимо обратиться к администратору безопасности;
- При перебоях в работе антивируса (например, перестал обновляться, не работает) на экран выводится сообщение, либо в правом нижнем углу на иконке антивируса появился восклицательный знак необходимо обратиться к техническому специалисту;
- Проверка на наличие вирусов всех внешних носителей информации (диски, флешки, карты памяти, приложения к письмам) обязательна.

Интернет и электронная почта

- Не открывать вложенные к письму файлы и документы от неизвестных отправителей;
- Не переходить по ссылкам, не запускать программы, полученные по электронной почте от неизвестных отправителей, а также проверять ссылки даже если письмо получено от другого пользователя информационной системы;
- Проверка адресата отправленного письма обязательна;
- Проверка адреса отправителя, даже в случае совпадения имени с уже известным контактом;
- Проводить поверку писем, содержащих призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
- Следует внимательно отнестись к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;
- Запрещается использование в служебных целях иностранные Интернет-сервисы: системы обмена мгновенными сообщениями (ICQ, QIP, Jabber, Viber, WhatsApp и т.д.) и облачные сервисы (iCloud, Google Drive, Dropbox и т.д.);
- Игнорировать, направляемые от имени ФСТЭК России «фишинговые» электронные письма с именем домена отправителя «cfo_1 lotd@fstec.support.», не открывать содержащийся в письме вредоносный архив с наименованием «Меры. Список уязвимостей и принимаемых мер по их устранению.exe».

Документы и программы

- Не устанавливать самостоятельно программное обеспечение, если это не входит в обязанности. Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению должностных обязанностей программное обеспечение;
- Делать резервные копии важных документов на разные носители (другой диск, внешний накопитель, сетевой диск, облачное хранилище, флешки и т.п.). При необходимости обратиться за помощью к техническому специалисту или для настройки регулярного резервного копирования ценной информации.

Инструкция по проверке подозрительных файлов и ссылок на наличие угроз безопасности

В случае получения подозрительного письма на электронную почту необходимо проверить его на наличие угроз безопасности. Рекомендуется, дополнительно к штатному средству антивирусной защиты, проводить проверку на веб-сайте производителя другого антивирусного средства защиты, так как обновление базы данных на сайте производителя происходит в реальном масштабе времени и являются наиболее актуальными, а второе антивирусное средство защиты применяется в качестве дополнительной меры защиты, с целью более точного обнаружения и определения вредоносных программ. Как вариант можно применить антивирус Dr.Web в дополнение к Kaspersky, и наоборот.

I. Антивирусное средство защиты Dr.Web.

1. Для проверки необходимо зайти на сайт Dr.Web по этой ссылке https://vms.drweb.ru/scan_file/

Дальше следует выбрать и прикрепить файл

The screenshot shows the Dr.Web online file scanner interface. At the top, there's a navigation bar with the Dr.Web logo and a menu. Below the navigation bar, the main heading is "Проверить файл". Underneath, there's a sub-heading "ПРИСЛАТЬ ПОДОЗРИТЕЛЬНЫЙ ФАЙЛ". A text input field contains "Выберите файл" and "Документ Microsoft Word.docx". To the right of the input field is a green button labeled "Проверить >". Below the input field, there's a section titled "Как это работает?" which explains the scanning process. It mentions that files are uploaded to the Dr.Web server and scanned with the latest virus database. It also provides instructions on how to use the scanner, including a list of steps: 1. Click "Обзор" and select the file. 2. Click "Проверить" to start scanning. 3. The maximum file size is 10 MB. 4. To scan multiple files, upload them to an archive (WinZip, WinRAR, or ARJ) and click "Обзор", then click "Проверить". At the bottom of the form, there are two green buttons: "Сообщить о вредоносном сайте >" and "Сообщить о ложном срабатывании >". Below the form, there's a text block explaining that the online file scanner and URL links can be added to a website's code, allowing visitors to use the service for free. At the bottom, there's a green button labeled "Скачать код формы" with a download icon.

Проверить файл на вирусы онлайн - Dr Web

Dr.WEB ПОЛЬЗОВАТЕЛЯМ

СЕРВИСЫ СКАНЕРЫ FIXIT DR.WEB VXSCUBE ЭКСПЕРТИЗА VKI ВИРУСНАЯ БИБЛИОТЕКА БАЗА ЗНАНИЙ НОВОСТИ

Проверить файл

С помощью онлайн-сканера файлов Dr.Web вы можете бесплатно проверить подозрительные файлы на наличие вредоносных программ.

ПРИСЛАТЬ ПОДОЗРИТЕЛЬНЫЙ ФАЙЛ

Выберите файл Документ Microsoft Word.docx **Проверить >**

Как это работает?

Вы отправляете свои файлы через браузер, они загружаются на наш сервер, их проверяет Dr.Web актуальной версии с самой свежей вирусной базой, и вы получаете результат проверки.

Как с помощью Антивируса Dr.Web просканировать в «онлайн» один или несколько файлов?

- ✓ Чтобы проверить единственный файл, нажмите на кнопку «Обзор» и выберите файл, вызывающий подозрение. Нажмите кнопку «Проверить», чтобы начать сканирование.
- ✓ Максимальный размер файла — 10 МБ.
- ✓ Чтобы проверить несколько файлов, поместите их в архив (формата WinZip, WinRar или ARJ) и загрузите его, нажав на кнопку «Обзор», затем нажмите «Проверить». Протокол проверки будет включать в себя отчет по каждому файлу в архиве.

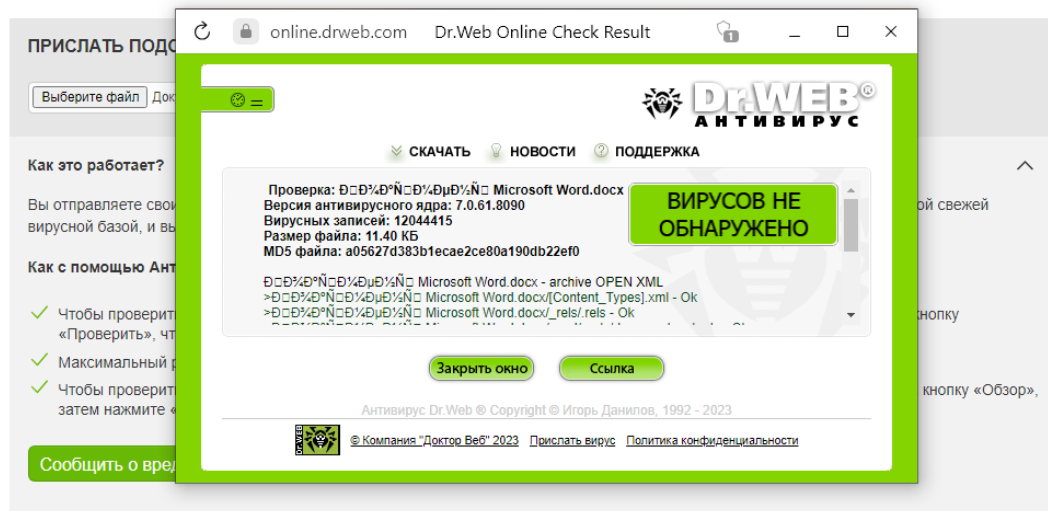
Сообщить о вредоносном сайте > **Сообщить о ложном срабатывании >**

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

Скачать код формы

Проверить файл

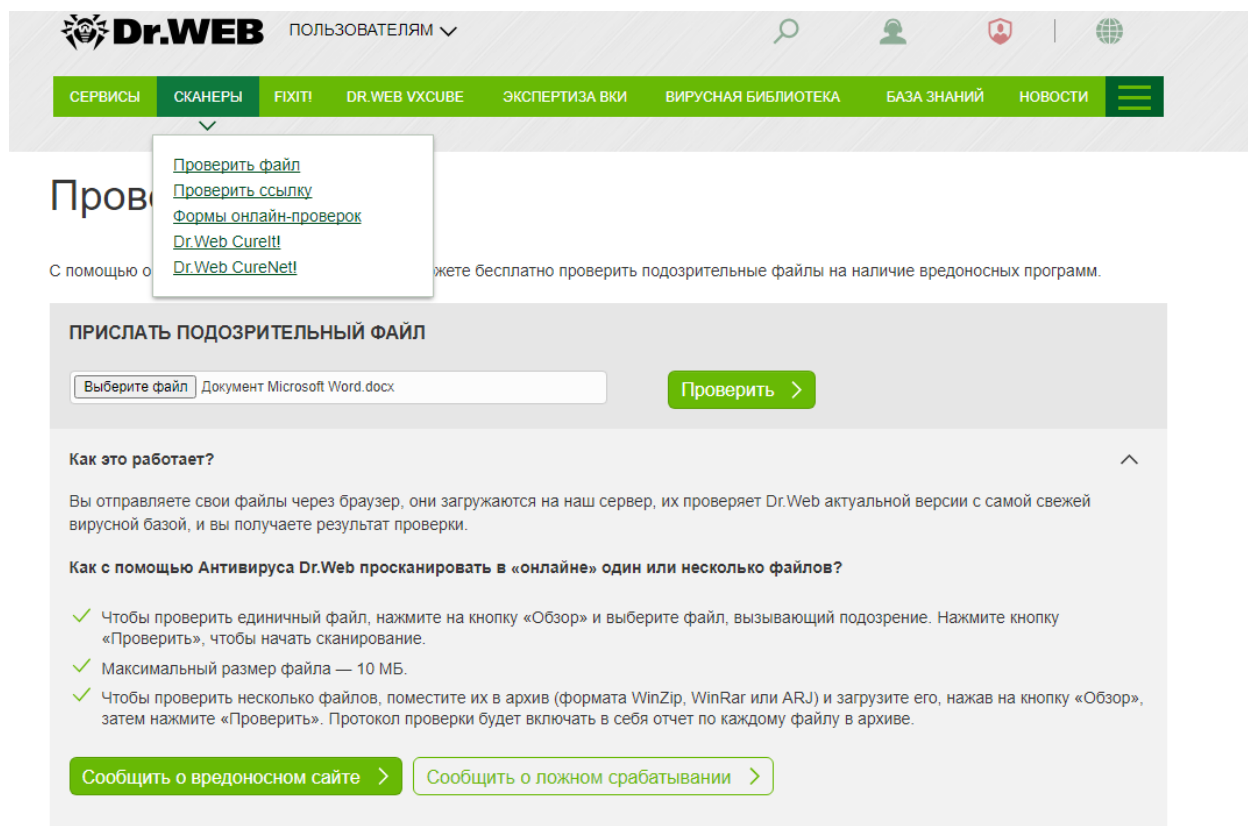
С помощью онлайн-сканера файлов Dr.Web вы можете бесплатно проверить подозрительные файлы на наличие вредоносных программ.



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

[Скачать код формы](#)

Также можно проверить ссылки



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

[Скачать код формы](#)

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.

Отправить >

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

Скачать код формы 

2. Антивирус Kaspersky

Необходимо перейти по ссылке

<https://opentip.kaspersky.com/?tab=upload>

← ⓘ ↻ 🛡 opentip.kaspersky.com

Kaspersky Threat Intelligence Portal — Analysis

 Касперский
Портал анализа угроз

<<

Анализ

Запросы

Премиум-сервисы

О портале

Выбрать тему Новое

Выберите язык

Анализ

Анализ файлов Поиск Анализ веб-адресов



Перетащите для загрузки

Добавить файл

Размер файла до 256 МБ.

Отправляя файл, вы соглашаетесь с нашими [Условиями использования](#) и [Заявлением о конфиденциальности](#).



Перетащите для загрузки

Размер файла до 256 МБ.

Добавить файл

Сообщить

Отчет по хэшу

578282D1AB478A8E19521EDBF59187E6D506E7E34D20C3F05E32A092842DF6A6

Отправить на повторный анализ

Очистить

Обзор

Просмотры

—

Впервые увиденный

—

Последний просмотр

—

Формат

docx

Размер

11.40 КБ (11673 Б)

Подписано

—

Соотавлено

—

MD5

A05627D383B1ECAE2CE80A190DB22EF0

SHA-1

6A1318C9C8C71462F5B669673125336C03D74FF8

SHA-256

578282D1AB478A8E19521EDBF59187E6D506E7E34D20C3F05E32A092842DF6A6

Категории

Общая информация

Названия обнаружений

Данные не найдены

Активация Windows