ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Парольная защита

- Не использовать простые пароли (например, ФИО пользователя, qwerty, pa$$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 блокировать 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.

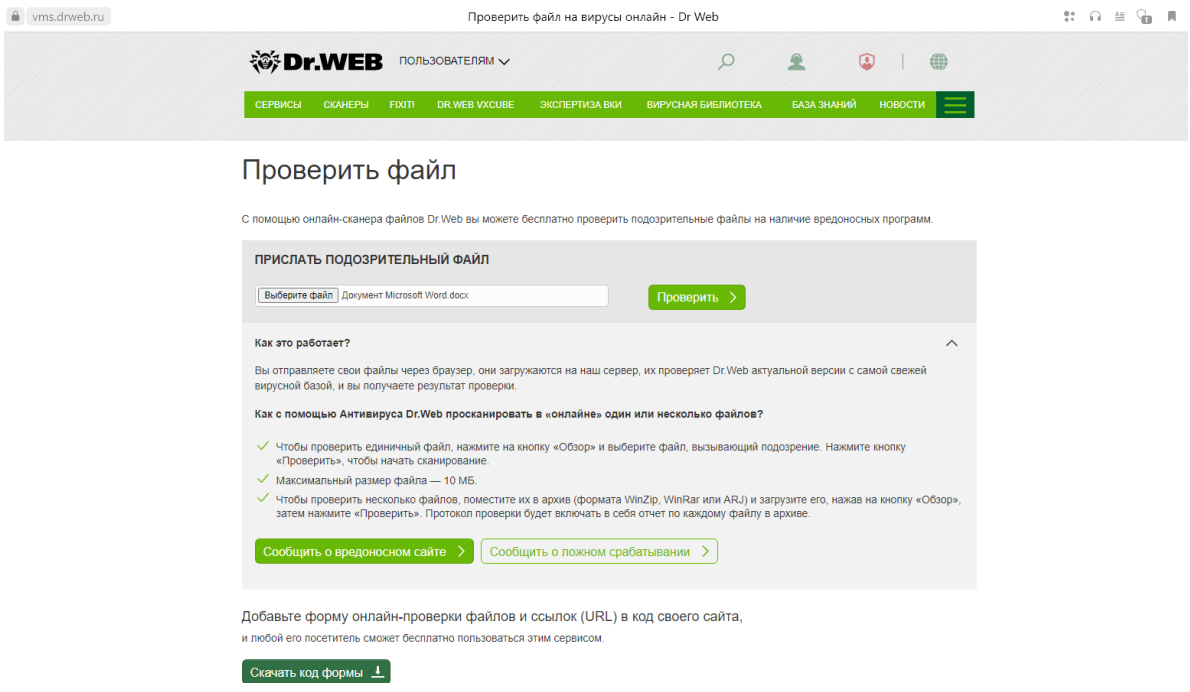
Инструкция по проверке подозрительных файлов и ссылок на наличие угроз безопасности

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.

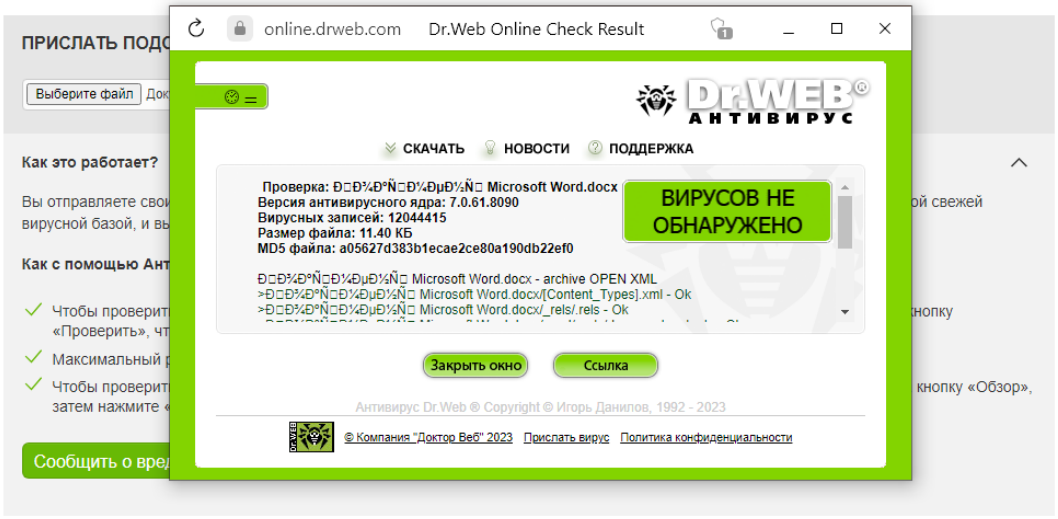
1. Для проверки необходимо зайти на сайт Dr.Web по этой ссылке https://vms.drweb.ru/scan_file/

Дальше следует выбрать и прикрепить файл



Проверить файл

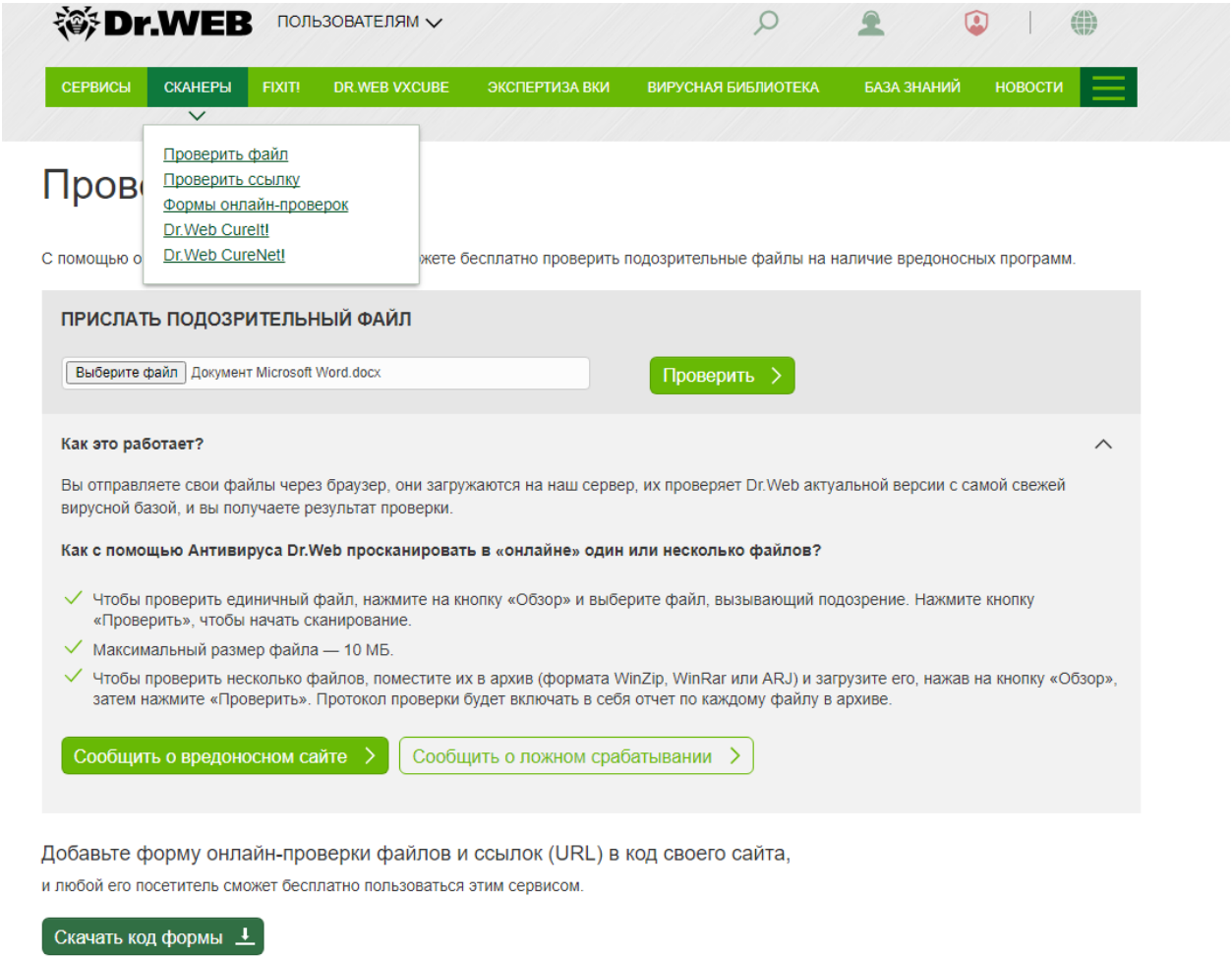
С помощью онлайн-сканера файлов Dr.Web вы можете бесплатно проверить подозрительные файлы на наличие вредоносных программ.



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

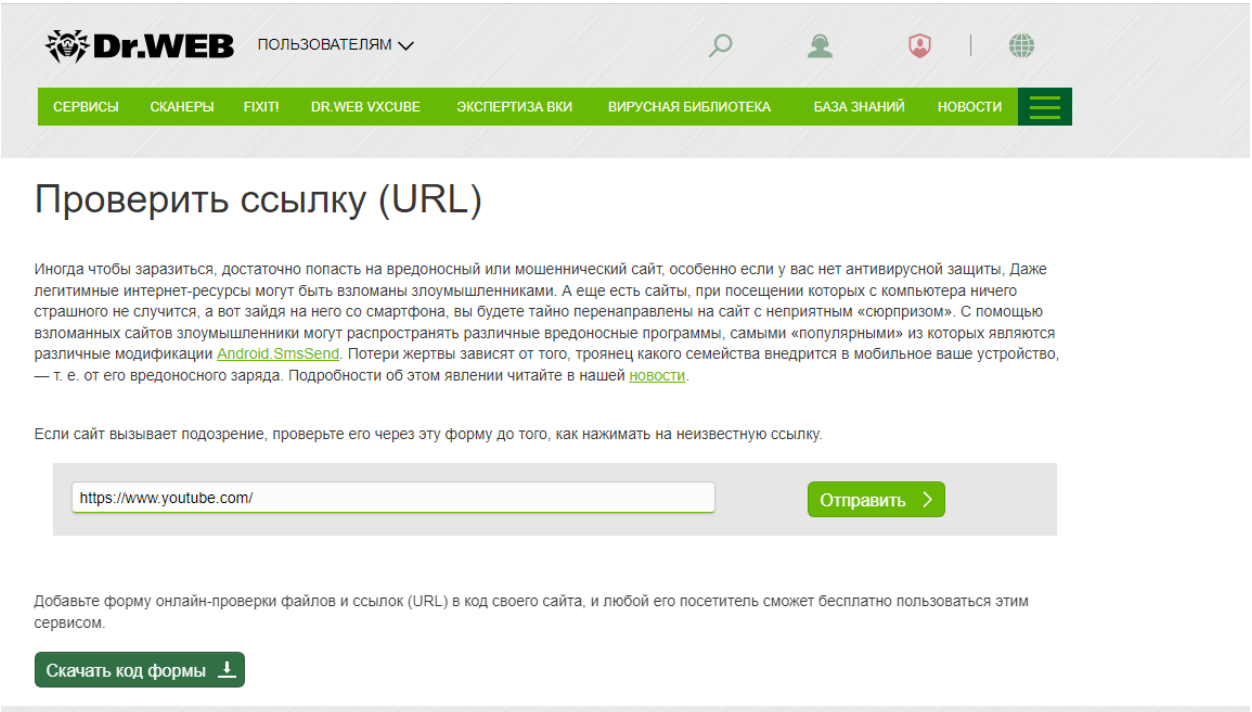
Скачать код формы

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.

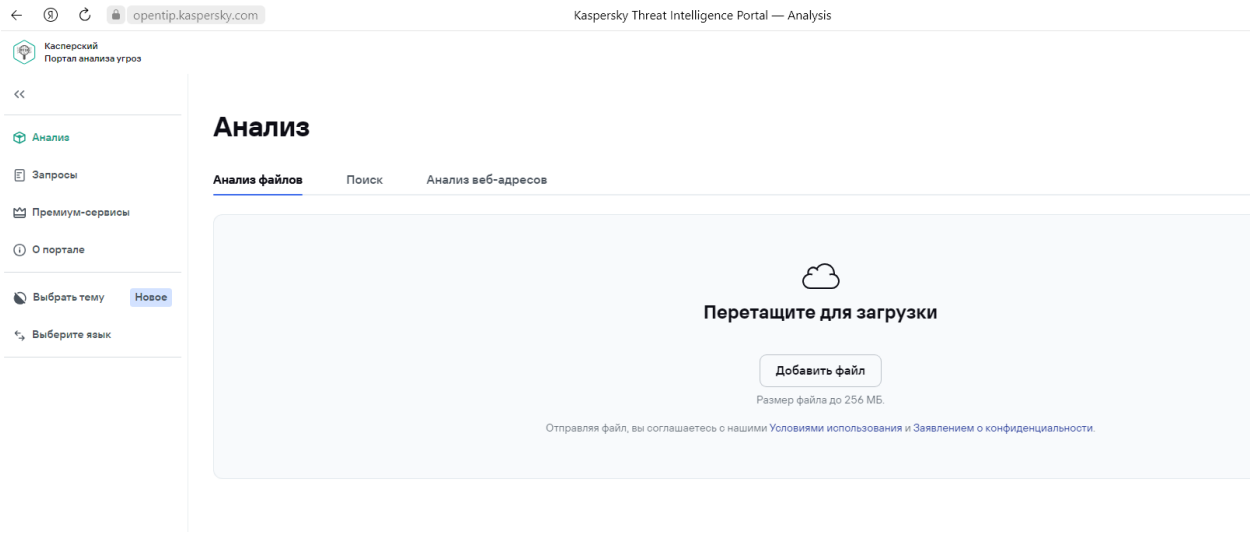
Скачать код формы



2. Антивирус Kaspersky

Необходимо перейти по ссылке

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



Анализ файлов | Поиск | Анализ веб-адресов

Перетащите для загрузки

Размер файла до 256 МБ.

Добавить файл

Сообщить

Отчет по хэшу

578282D1AB478A8E19521EDBF59187E6D506E7E34D20C3F05E32A092842DF6A6

Очистить

Отправить на повторный анализ

Обзор

Просмотры	—
Впервые увиденный	—
Последний просмотр	—

Формат	docx
Размер	11.40 КБ (11673 B)
Подписано	—
Составлено	—

MD5	A05627D383B1ECAE2CE80A190DB22EF0
SHA-1	6A1318C9C8C71462F5B669673125336C03D74FF8
SHA-256	578282D1AB478A8E19521EDBF59187E6D506E7E34D20C3F05E32A092842DF6A6

Категории: Общая информация

Названия обнаружений

Данные не найдены