Приложение №1 к распоряжению №12-р

от «23» марта 2020 г.

Профилактические меры по недопущению заражения информационных систем

Компьютерные вирусы зачастую распространяются с использованием вложений в сообщения электронной почты или мгновенных сообщений. По этой причине не следует открывать вложения в сообщениях электронной почты, полученных из неизвестных источников. Вирусы могут быть замаскированы под изображения, поздравительные открытки, звуковые или видеофайлы.

Кроме того, компьютерные вирусы распространяются через файлы, загружаемые из сети Интернет. Они могут быть скрыты в пиратском программном обеспечении или в других файлах и программах, загружаемых пользователями.

Вирусы могут иметь разный функционал, некоторые из них интегрированы с другим программным обеспечением (далее – ПО) так, что «жертва» даже не замечает, что было выполнено что-то кроме основного функционала запускаемого файла. Такие вирусы могут сохранять Ваши сохраненные пароли, файлы cookie, историю браузера, файлы с компьютера и иную информацию.

Бывают вирусы, предоставляющие удаленный доступ злоумышленнику, либо скрытно использующие вычислительные мощности Вашего компьютера для майнинга криптовалюты.

В последние время широкое распространение получили вирусы-шифровальщики. Эти файлы после запуска получают от удаленного сервера ключ шифрования и начинают шифровать все файлы жесткого диска, затем появляется баннер, в котором злоумышленники просят перевести им деньги для получения ключа дешифрования. Стоит понимать, что после перевода денег нет никаких гарантий в получении ключа дешифрования, более того, существуют вирусы, не сохраняющие на своем сервере сгенерированные ключи. Таким образом восстановление данных становится физически невозможным. Является это задумкой злоумышленников или ошибкой – сказать сложно. Таким образом, лучше не допускать заражение компьютера ни одним из видов вирусов.

Для уменьшения вероятности заражения компьютерными вирусами рабочих станций следует придерживаться простых правил:

На всех рабочих станциях должно быть установлено антивирусное ПО;

Необходимо регулярно обновлять базы данных антивирусного ПО;

Необходимо регулярно проводить полное сканирование рабочей станции средством антивирусной защиты;

Необходимо регулярно устанавливать обновления операционных систем;

Необходимо обновлять Web-браузер, так как вирусы эксплуатируют ошибки в работе браузера для внедрения вредоносного кода на компьютер «жертвы».

Запрещено скачивать ПО с неофициальных сайтов, с пометкой «реклама» или если адрес сайта явно не является официальным;

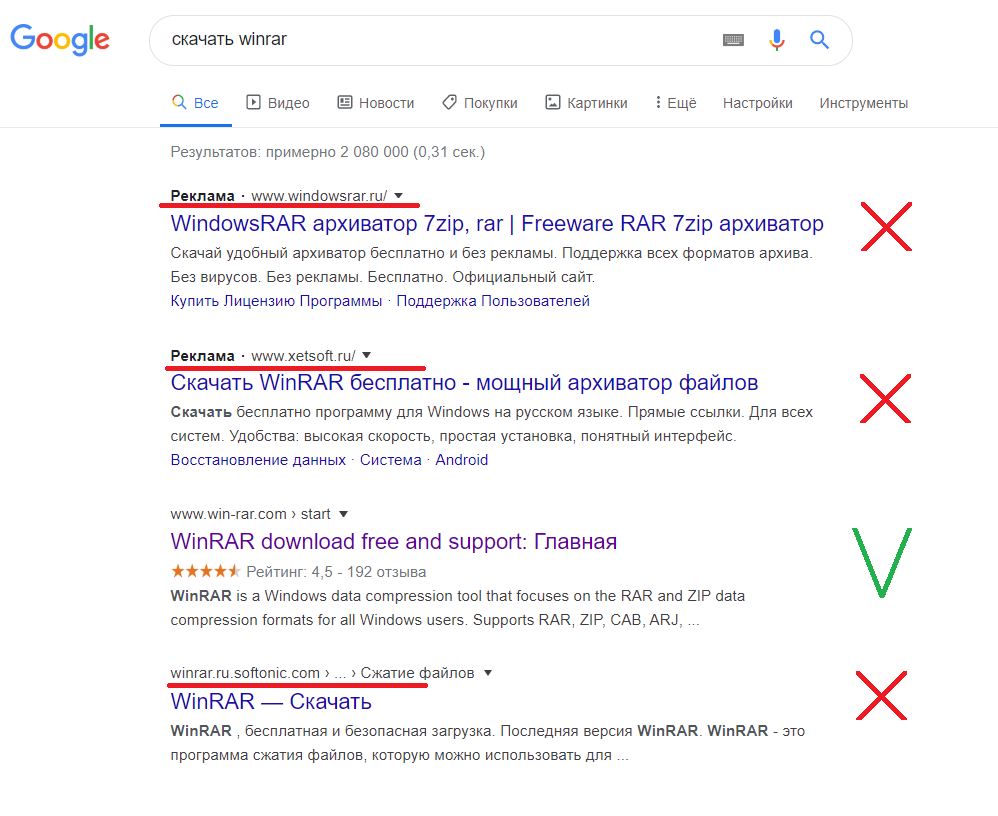


Рисунок 1. Примеры подозрительных сайтов

Запрещено на рабочих компьютерах использовать личные съемные носители (флешки, диски). Любые съемные носители должны быть просканированы средством антивирусной защиты. Для этого достаточно нажать на правку кнопку мыши, выбрав пункт «Проверить на вирусы»;

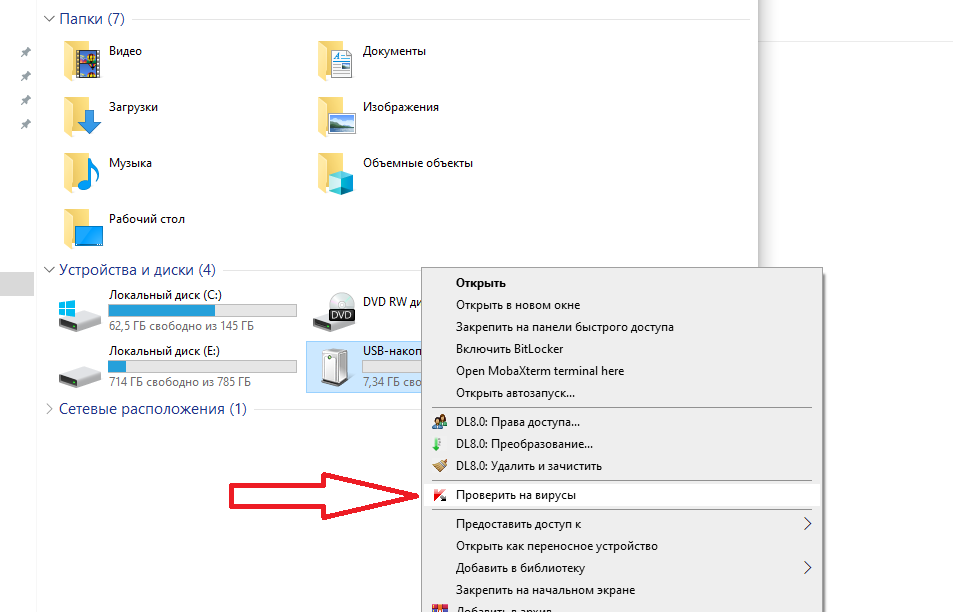


Рисунок 2. Проверка на вирусы съемных носителей

При подозрении ссылки на вредоносность рекомендуется по ней не переходить, однако, если это невозможно необходимо проверить ее с помощью онлайн-сервиса проверок, например, можно использовать <https://virusdesk.kaspersky.ru/>;

Необходимо внимательно смотреть на адреса сайтов и не вводить свои данные, если адрес страницы выглядит подозрителен. Примеры возможный фишинговых сайтов приведены в таблице 1.

|  |  |  |
| --- | --- | --- |
| Оригинальные сайты | Примеры вредоносных сайтов | Описание |
| rzd.ru | rzd.info | Замена домена «ru» на «info» |
| gosuslugi.ru | Gosus1ugi.ru | Заменена «l»(«L») на «1» (единица) |
| Yandex.ru | Yandeex.ru | Дублирована буква «e» |
| Samregion.ru | Sanregion.com | Замена домена «ru» на «com»  Заменена буква «m» на «n» |

Таблица 1 – Примеры фишинговых сайтов.

Запрещено открывать всплывающую рекламу поверх открытой Web-страницы, переходить по ссылкам в баннерах. При появлении рекламы, если Вы видите большую кнопку «Закрыть», нажав на нее, возможен запуск установки или загрузки вредоносного ПО на Вашу рабочую станцию;

При загрузке файлов необходимо обращать внимание на их расширения. Если при загрузке текстовых файлов, видеофайлов, картинок скачанный файл имеет расширение «.exe» - скорее всего это вирус;

При работе многие сайты выдают контекстную рекламу по краю от основного текста. Запрещается переходить по таким ссылкам. Пример рекламы приведен на рисунке 3;

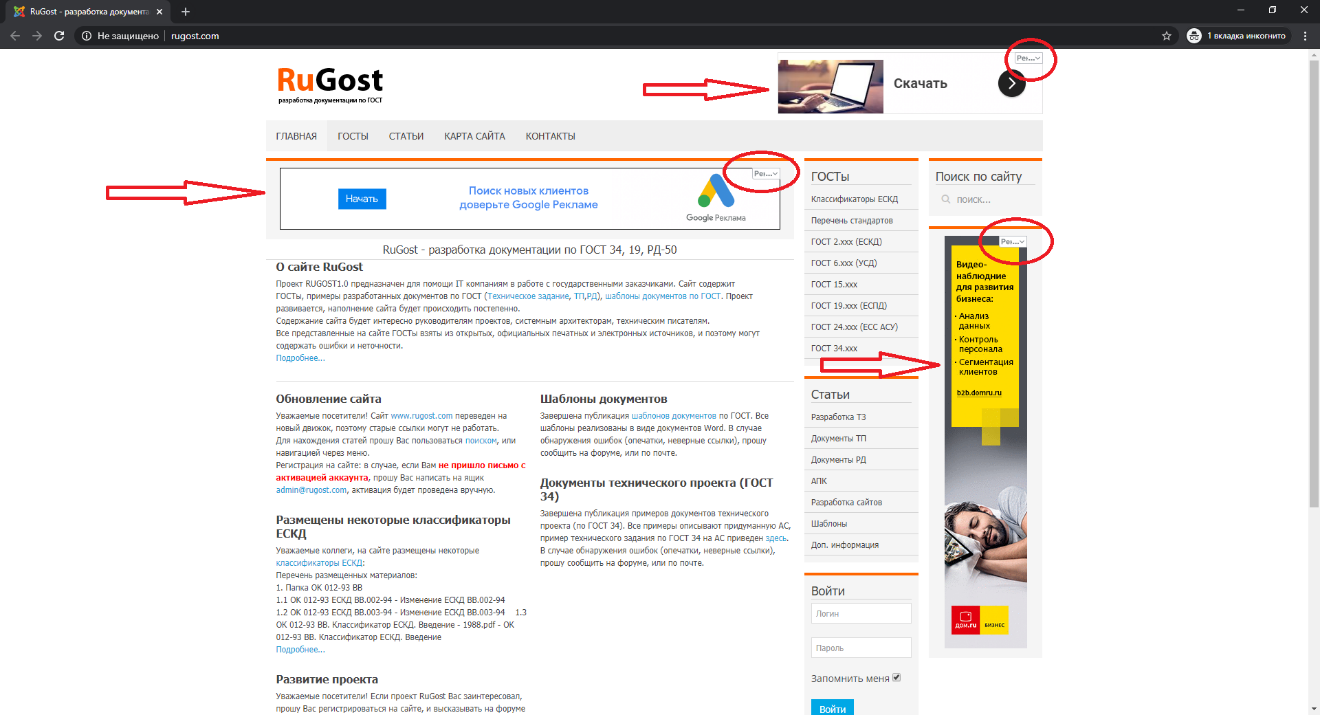


Рисунок 3.Примеры контекстной рекламы

Бэкапы важных файлов, конфигураций оборудования или образов виртуальных машин необходимо регулярно обновлять, а также рекомендуется хранить их на отдельных серверах.