Рекомендации
по защите от вредоносных программ-шифровальщиков

Что такое программа-шифровальшик

В последние месяцы распространенной угрозой безопасности информации, обрабатываемой на компьютерах, стали вирусные программы-шифровальщики, которые попадая на компьютер, шифруют все файлы пользователя на локальном диске, доступных сетевых дисках (документы, таблицы, презентации, базы данных, фото-, видео-, аудиофайлы и т.д.) и затем предлагают выплатить злоумышленнику деньги за их расшифровку.

Как осуществляется атака с помощью программ-шифровальщиков

1) В большинстве случаев программа-вирус приходит по электронной почте в виде вложения к электронному письму от неизвестного отправителя или якобы от имени судебных органов, банковских или других организации, наименование которых вам уже известно. Электронные письма приходят с заголовками вида: «Акт сверки…», «Акт выполненных работ…», «Ваша задолженность перед банком …», «Проверка регистрационных данных», «Блокировка расчетного счета» и тому подобное. В письмах содержатся файлы-вложения с документами, якобы подтверждающими факт, указанный в заголовке письма. При открытии этого вложения (двойным нажатием кнопки «мыши») происходит запуск выполнения программы-шифровальщика, которая незаметно зашифрует все доступные файлы на компьютере и доступных сетевых дисках.

Вложения этих писем чаще всего бывают в архивных файлах с расширениями .zip, .rar, .7z. Внутри этих архивов находятся на первый взгляд безобидные документы. Если в настройках системы отключена функция отображения расширения файлов, то вы увидите лишь файлы вида «Документ.doc» или «Акт.xls» или что-то подобное. Если же включить отображение расширения файлов, то сразу будет видно, что на самом деле это не документы, а исполняемые программы или скрипты, так как полные имена файлов с расширением будут другого вида, например, «Документ.doc.exe» или «Акт.xls.js».

Краткий список «опасных» расширений файлов, за которыми спрятан вирус-шифровальщик: .exe, .com, .js, .wbs, .hta, .bat, .cmd, .vbs, .scr.

2) Зараженный программой-вирусом файл может иметь имя с видимым ложным расширением и множеством символов «точка» или «пробел». Например, «акт.doc…….....exe», «накладная.doc .exe». Если видна только часть имени «акт.doc», а остальная часть имени с расширением не видна, то вы подумаете, что это word-файл. Дважды нажав на файл, вы запускаете вредоносную программу «Акт.doc.....exe».

3) Встречаются случаи получения по почте обычного word-файла (.doc-файла), внутри которого помимо текста есть изображение или гиперссылка (на неизвестный сайт в сети «Интернет») или связанный, встроенный объект. При

нажатии на такой объект (ссылка, изображение и т.д.) происходит незаметное заражение компьютера вирусом-шифровальщиком.

4) Возможно проникновение на компьютер при скачивании из сети «Интернет» каких-либо программ, утилит, файлов (платных или бесплатных) с неизвестных сайтов.

5) Имеет место вариант запуска на компьютере вредоносной программы, которая находится на флэш-носителе, съемном диске, не проверенном антивирусным программным обеспечением.

Как не допустить заражения вредоносной программой-вирусом

1) Относитесь подозрительно к каждому письму, полученному от неизвестного отправителя. Никогда не открывайте для просмотра двойным щелчком «мыши» вложения в письмах от незнакомых вам людей или организаций.

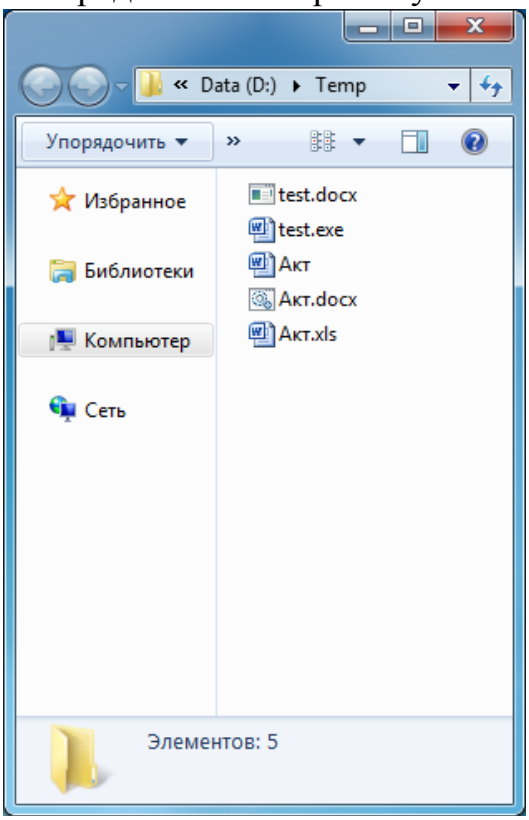
2) Не полагайтесь всецело на антивирусные программы. Не всегда антивирус быстро реагирует на появление новой модификации вируса-шифровальщика. Своевременно обновляйте антивирусные базы.

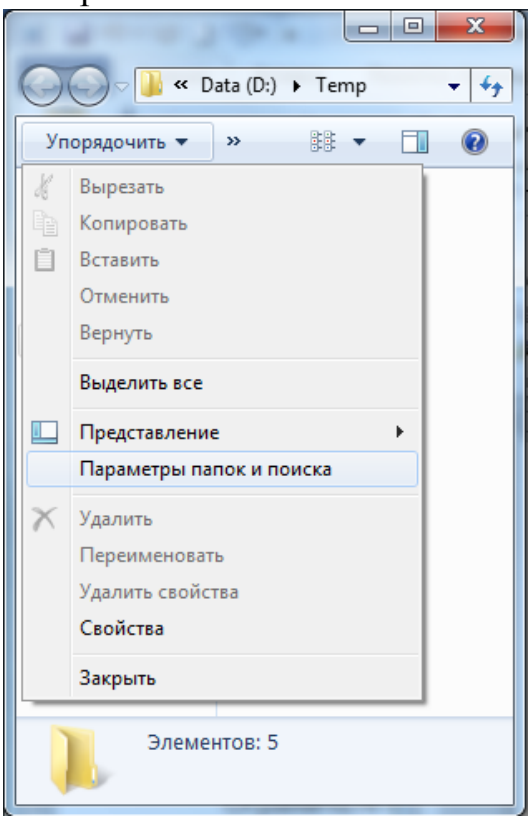
3) Регулярно делайте резервные копии важных данных на внешние носители информации (флеш-носители, съемные жесткие диски).

4) Обязательно проверяйте расширения имен всех вложенных файлов, даже если письмо пришло от известного вам отправителя. Если имя вложенного файла заканчивается на вышеуказанные «опасные» расширения, то ни в коем случае не открывайте их. Попросите отправителя выслать файлы в другом формате.

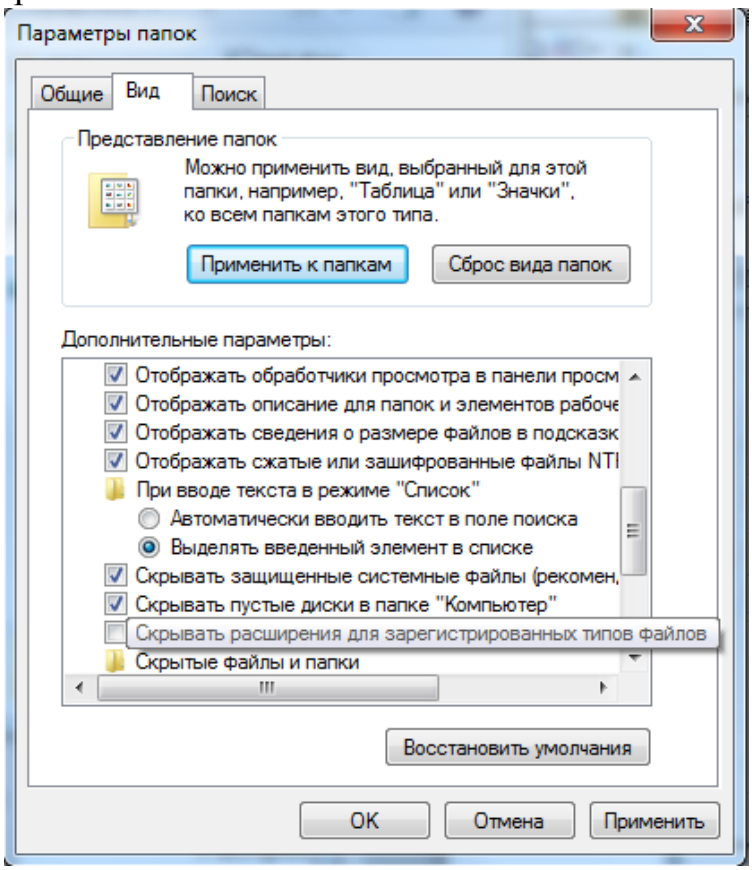
5) В файловом менеджере (проводник, обзор) включите отображение расширение имени файлов (это последовательность символов, добавляемых к имени файла после последней «точки» и предназначенных для идентификации типа файла).

Для включения отображения расширения необходимо в проводнике в меню «Упорядочить» выбрать пункт «Параметры папок и поиска».

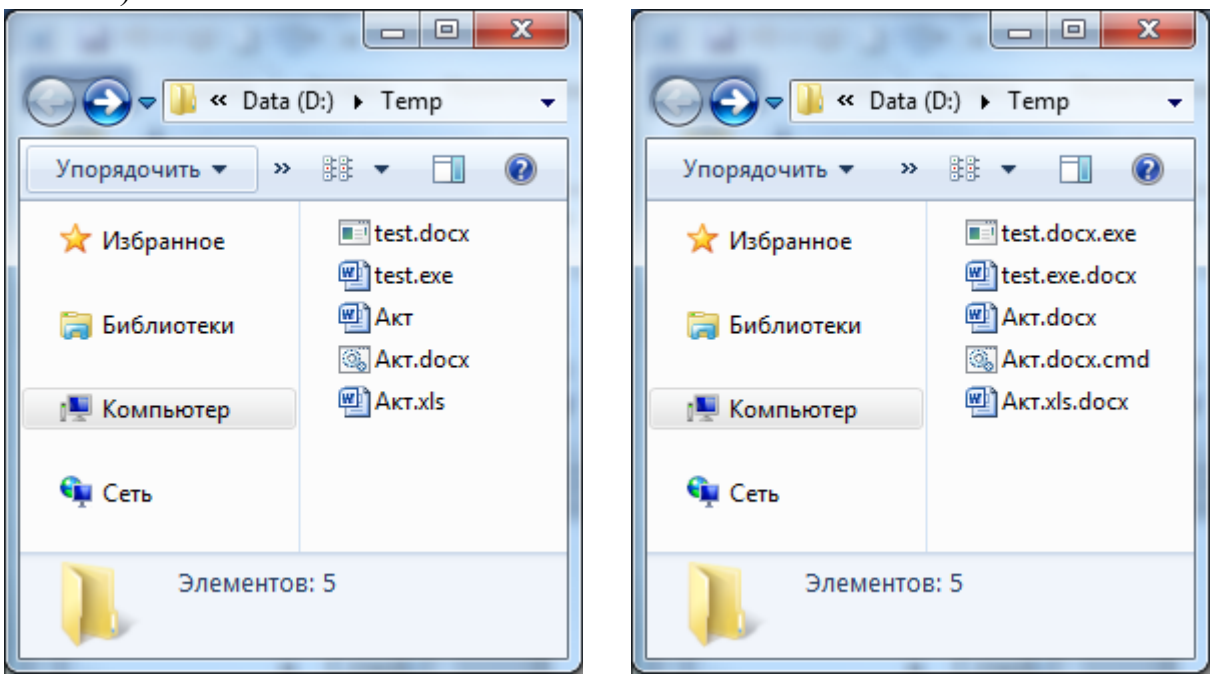




в окне «Параметры папок» в закладке «Вид» в дополнительных параметрах снять галочку «Скрывать расширение для зарегистрированных типов файлов» и нажать кнопку «Применить».

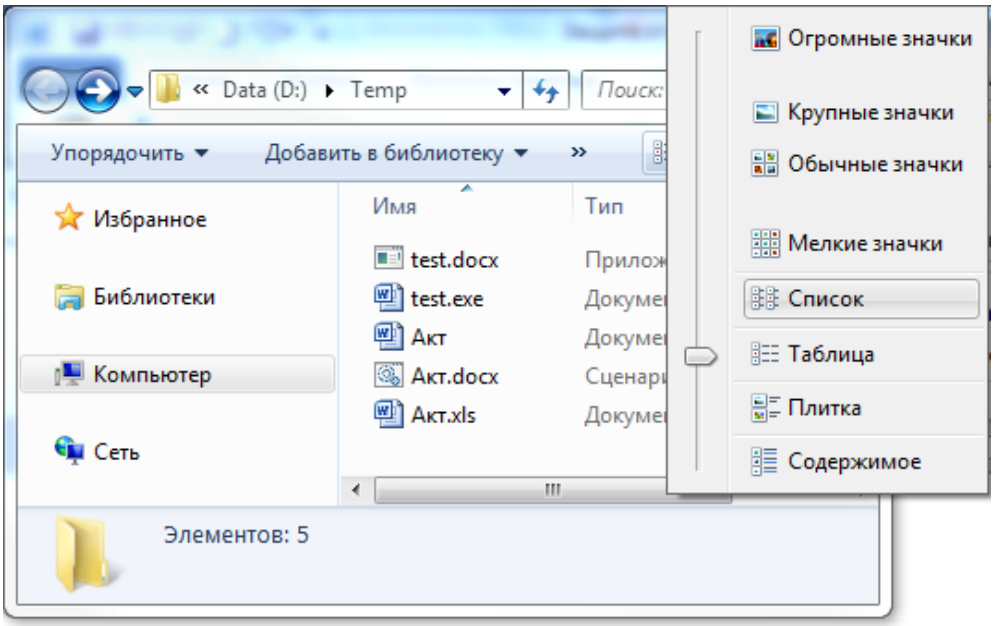


Сравните полученный результат отображения одних и тех же файлов (слева вид файлов при установленной «галочке», справа – без установленной «галочки»):

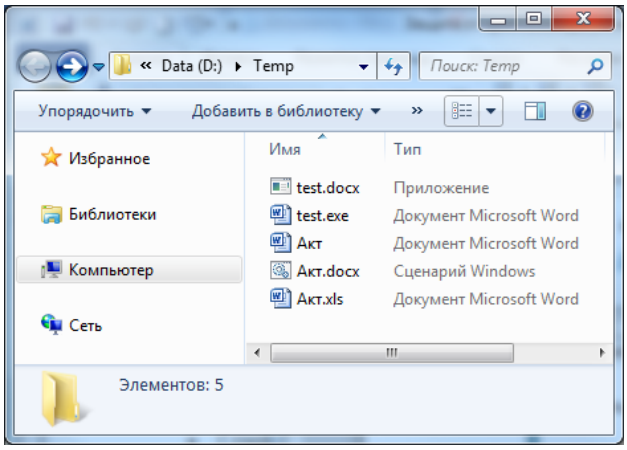


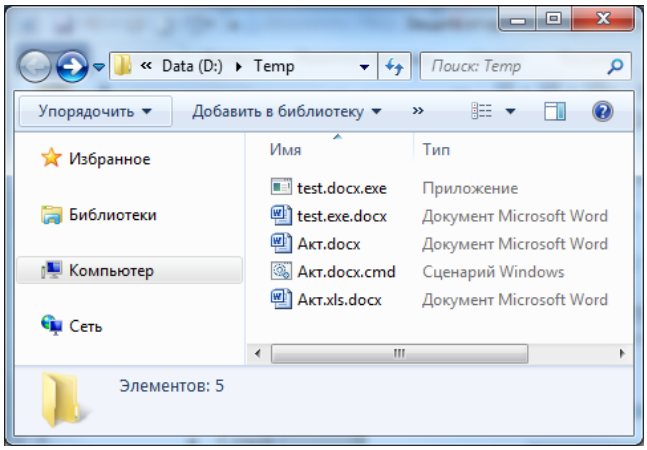
Наличие расширений файлов справа от имен файлов заставляет задуматься над их происхождением и является поводом обратиться к вашему системному администратору.

Аналогично работает изменение способа отображения вида файлов в виде «Таблицы».



Еще один способ представления вида файлов в проводнике Windows – представление в виде «Таблицы». Обратите внимание на то, что независимо от того скрыты или нет расширения фалов, по типу документа можно определить является ли документ чем вы ожидаете.





Однако данный способ является менее приемлемым в силу того, что представление файлов распространяется только на текущую папку (отображение расширения для зарегистрированных типов файлов – на все папки компьютера). Кроме того, информация о типе файла менее «притягивает взгляд», чем расширение непосредственно в имени файлов (пользователь редко обращает внимание на тип файлов).

Также можно использовать сторонний файловый менеджер, который позволяет отображать расширение файлов.

Помните: Внимательность – один из самых эффективных методов предотвращения угрозы запуска вредоносной программы

Запустить выполнение программы-шифровальщика может только сам пользователь. Повышенная бдительность и внимание к вновь появившемся файлам на компьютере и аккуратное обращение с ними поможет не допустить заражение и последующего блокирования файлов на компьютере и в сети организации.

Что делать пользователям компьютеров, зараженных вирусом-шифровальщиком

Если на компьютере не установлены средства антивирусной защиты и нет резервных копий информации на съемных носителях, то после запуска программы-шифровальщика от пользователя практически ничего не зависит.

Неофициальное программное обеспечение из сети «Интернет», которое якобы может расшифровать зараженные данные, может быть опасным. Его использовать нельзя. В лучшем случае оно окажется просто бесполезным, а в худшем – заразит компьютер дополнительным вирусом.

В случае запуска программы-шифровальщика необходимо НЕЗАМЕДЛИТЕЛЬНО:

1. Отключить электропитание компьютера (без корректного завершения сеанса и без сохранения всех результатов) вплоть до физического отключения питания от электросети.

2. Поставить в известность о данном факте своего непосредственного руководителя, системного администратора (при его наличии в штате

организации), начальника управления информационных технологий управления делами Правительства области Склёмина Андрея Вячеславовича по тел. 21-00-77, начальника отдела технической защиты информации УИТ управления делами Правительства области Носова Игоря Владимировича по тел. 21-08-91.

Руководителю организации рекомендуется провести служебную проверку по факту шифрования файлов с целью установления его причин, а также провести дополнительные занятия со всеми сотрудниками организации по защите от вредоносных программ-шифровальщиков.

Управление информационных технологий
управления делами Правительства области