Протокол самостоятельной работы

По Теории Защиты Информации

На тему: Черви

Выполнил студент К17.1

Шишелов Владимир

**Введение**

Сетевой червь - разновидность [вредоносной программы](https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0), самостоятельно распространяющейся через локальные и глобальные ([Интернет](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)) компьютерные сети.

Все механизмы («[векторы атаки](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BA%D1%82%D0%BE%D1%80_%D0%B0%D1%82%D0%B0%D0%BA%D0%B8_(%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C))») распространения червей делятся на две большие группы:

1. Использование [уязвимостей](https://ru.wikipedia.org/wiki/%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D1%8C_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)) и ошибок администрирования в программном обеспечении, установленном на компьютере. [Червь Морриса](https://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D1%80%D0%B2%D1%8C_%D0%9C%D0%BE%D1%80%D1%80%D0%B8%D1%81%D0%B0) использовал известные на тот момент уязвимости в программном обеспечении, а именно в почтовом сервере [sendmail](https://ru.wikipedia.org/wiki/Sendmail" \o "Sendmail), сервисе finger и подбирал пароль по словарю. Такие черви способны распространяться автономно, выбирая и атакуя компьютеры в полностью автоматическом режиме.
2. Используя средства так называемой [социальной инженерии](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F), провоцируется запуск вредоносной программы самим пользователем. Чтобы убедить пользователя в том, что файл безопасен, могут подключаться недостатки пользовательского интерфейса программы - например, червь [VBS.LoveLetter](https://ru.wikipedia.org/wiki/VBS.LoveLetter) использовал тот факт, что [Outlook Express](https://ru.wikipedia.org/wiki/Outlook_Express) скрывает расширения файлов. Данный метод широко применяется в спам-рассылках, социальных сетях и т. д.

Иногда встречаются черви с целым набором различных векторов распространения, стратегий выбора жертвы, и даже [эксплойтов](https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D1%81%D0%BF%D0%BB%D0%BE%D0%B9%D1%82) под различные [операционные системы](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0).

**Вирус Петя**

Petya (также известна как Petya.A, Petya.D[[2]](https://ru.wikipedia.org/wiki/Petya" \l "cite_note-:5-2), Trojan.Ransom.Petya, PetrWrap[[2]](https://ru.wikipedia.org/wiki/Petya" \l "cite_note-:5-2), NotPetya[[2]](https://ru.wikipedia.org/wiki/Petya" \l "cite_note-:5-2), ExPetr, GoldenEye[[2]](https://ru.wikipedia.org/wiki/Petya" \l "cite_note-:5-2)) — [вредоносная программа](https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0), [сетевой червь](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%87%D0%B5%D1%80%D0%B2%D1%8C) и [программа-вымогатель](https://ru.wikipedia.org/wiki/Ransomware), поражающая компьютеры под управлением [Microsoft Windows](https://ru.wikipedia.org/wiki/Microsoft_Windows" \o "Microsoft Windows). Первые разновидности вируса были обнаружены в марте 2016 года.

Программа [шифрует](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) файлы на [жёстком диске](https://ru.wikipedia.org/wiki/%D0%96%D1%91%D1%81%D1%82%D0%BA%D0%B8%D0%B9_%D0%B4%D0%B8%D1%81%D0%BA) [компьютера-жертвы](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80-%D0%B7%D0%BE%D0%BC%D0%B1%D0%B8), а также перезаписывает и шифрует [MBR](https://ru.wikipedia.org/wiki/%D0%93%D0%BB%D0%B0%D0%B2%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BE%D1%87%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%8C) — данные, необходимые для загрузки [операционной системы](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0). В результате все хранящиеся на компьютере файлы становятся недоступными. Затем программа требует денежный выкуп в [биткойнах](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82%D0%BA%D0%BE%D0%B9%D0%BD) за расшифровку и восстановление доступа к файлам. При этом первая версия вируса шифровала не сами файлы, а [MFT-таблицу](https://ru.wikipedia.org/wiki/Master_File_Table) — базу данных с информацией о всех файлах, хранящихся на диске. Уплата выкупа является бесполезной, так как версия Petya 2017 года (названная NotPetya) не предполагает возможности расшифровки информации на жёстком диске, а уничтожает её безвозвратно.

**Атаки с использованием червя Петя**

Первые версии в 2016

Впервые вирус Petya был обнаружен в марте 2016 года. Компания «[Check Point](https://ru.wikipedia.org/wiki/Check_Point" \o "Check Point)» тогда отметила, что, хотя ему удалось заразить меньше компьютеров, чем другим программам-вымогателям начала 2016 года, таким как [CryptoWall](https://ru.wikipedia.org/wiki/CryptoWall" \o "CryptoWall), поведение нового вируса заметно отличается, благодаря чему он «немедленно был отмечен как следующий шаг в развитии программ-вымогателей». За восстановление доступа к файлам программа требовала от пользователя 0,9 [биткойна](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82%D0%BA%D0%BE%D0%B9%D0%BD) (около 380 долларов США по состоянию на март 2016 года). Другую разновидность программы обнаружили в мае 2016 года. Она содержала дополнительную [полезную нагрузку](https://ru.wikipedia.org/wiki/Payload): если вирусу не удаётся получить права администратора для перезаписи [MBR](https://ru.wikipedia.org/wiki/%D0%93%D0%BB%D0%B0%D0%B2%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BE%D1%87%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%8C) и последующего шифрования [MFT](https://ru.wikipedia.org/wiki/Master_File_Table), он устанавливает на зараженный компьютер другую вредоносную программу — Mischa, которая шифрует файлы пользователя напрямую (такая операция обычно не требует прав администратора), а затем требует выкуп в размере 1,93 биткойна (на тот момент — 875 долларов США).

Массовое заражение в 2017

[27 июня](https://ru.wikipedia.org/wiki/27_%D0%B8%D1%8E%D0%BD%D1%8F) [2017 года](https://ru.wikipedia.org/wiki/2017_%D0%B3%D0%BE%D0%B4) началось массовое распространение новой модификации программы. На этот раз вирус использует те же уязвимости системы, что и [WannaCry](https://ru.wikipedia.org/wiki/WannaCry) (к примеру, [эксплойт](https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D1%81%D0%BF%D0%BB%D0%BE%D0%B9%D1%82) [EternalBlue](https://ru.wikipedia.org/wiki/EternalBlue) от [АНБ](https://ru.wikipedia.org/wiki/%D0%90%D0%9D%D0%91) и [бэкдор](https://ru.wikipedia.org/wiki/%D0%91%D1%8D%D0%BA%D0%B4%D0%BE%D1%80) [DoublePulsar](https://ru.wikipedia.org/wiki/DoublePulsar)), а за восстановление доступа к данным требует отправить 300 долларов в биткойнах. Однако специалисты не рекомендуют пользователям идти на поводу у вымогателей, поскольку это всё равно не поможет им восстановить доступ к данным: электронный адрес, на который злоумышленники просят отправить данные после осуществления платежа, уже заблокирован провайдером. По мнению главного инженера компании «[McAfee](https://ru.wikipedia.org/wiki/McAfee" \o "McAfee)» Кристиана Бика, эта версия была разработана так, чтобы распространяться максимально быстро. В компании «[ESET](https://ru.wikipedia.org/wiki/ESET)» заявили, что распространение вредоносной программы началось на [Украине](https://ru.wikipedia.org/wiki/%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D0%B0) через популярное бухгалтерское [программное обеспечение](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) [M.E.Doc](https://ru.wikipedia.org/wiki/M.E.Doc). Атаке подверглись энергетические компании, украинские банки, [аэропорт Харькова](https://ru.wikipedia.org/wiki/%D0%A5%D0%B0%D1%80%D1%8C%D0%BA%D0%BE%D0%B2_(%D0%B0%D1%8D%D1%80%D0%BE%D0%BF%D0%BE%D1%80%D1%82)), [Чернобыльская АЭС](https://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D1%80%D0%BD%D0%BE%D0%B1%D1%8B%D0%BB%D1%8C%D1%81%D0%BA%D0%B0%D1%8F_%D0%90%D0%AD%D0%A1), правительственные сайты. [Национальный банк Украины](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B1%D0%B0%D0%BD%D0%BA_%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%8B) опубликовал на своём сайте официальное заявление о хакерской атаке на банки страны и борьбе с ней. Позднее стали появляться сообщения о хакерской атаке на российские банки, компании, предприятия: «[Сбербанк](https://ru.wikipedia.org/wiki/%D0%A1%D0%B1%D0%B5%D1%80%D0%B1%D0%B0%D0%BD%D0%BA)», [«Хоум Кредит»](https://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D1%83%D0%BC_%D0%BA%D1%80%D0%B5%D0%B4%D0%B8%D1%82_%D1%8D%D0%BD%D0%B4_%D1%84%D0%B8%D0%BD%D0%B0%D0%BD%D1%81_%D0%B1%D0%B0%D0%BD%D0%BA), «[Роснефть](https://ru.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D0%BD%D0%B5%D1%84%D1%82%D1%8C)», «[Башнефть](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D1%88%D0%BD%D0%B5%D1%84%D1%82%D1%8C" \o "Башнефть)» и «[Евраз](https://ru.wikipedia.org/wiki/%D0%95%D0%B2%D1%80%D0%B0%D0%B7" \o "Евраз)».

Также сообщения о заражении стали поступать из [Италии](https://ru.wikipedia.org/wiki/%D0%98%D1%82%D0%B0%D0%BB%D0%B8%D1%8F), [Израиля](https://ru.wikipedia.org/wiki/%D0%98%D0%B7%D1%80%D0%B0%D0%B8%D0%BB%D1%8C), [Сербии](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B1%D0%B8%D1%8F), [Венгрии](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BD%D0%B3%D1%80%D0%B8%D1%8F), [Румынии](https://ru.wikipedia.org/wiki/%D0%A0%D1%83%D0%BC%D1%8B%D0%BD%D0%B8%D1%8F), [Польши](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%8C%D1%88%D0%B0), [Аргентины](https://ru.wikipedia.org/wiki/%D0%90%D1%80%D0%B3%D0%B5%D0%BD%D1%82%D0%B8%D0%BD%D0%B0), [Чехии](https://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D1%85%D0%B8%D1%8F), [Германии](https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D0%B8%D1%8F), [Великобритании](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D1%8F), [США](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D1%91%D0%BD%D0%BD%D1%8B%D0%B5_%D0%A8%D1%82%D0%B0%D1%82%D1%8B_%D0%90%D0%BC%D0%B5%D1%80%D0%B8%D0%BA%D0%B8), [Дании](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%B8%D1%8F), [Нидерландов](https://ru.wikipedia.org/wiki/%D0%9D%D0%B8%D0%B4%D0%B5%D1%80%D0%BB%D0%B0%D0%BD%D0%B4%D1%8B), [Испании](https://ru.wikipedia.org/wiki/%D0%98%D1%81%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F), [Индии](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D0%B4%D0%B8%D1%8F), [Франции](https://ru.wikipedia.org/wiki/%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D0%B8%D1%8F) и [Эстонии](https://ru.wikipedia.org/wiki/%D0%AD%D1%81%D1%82%D0%BE%D0%BD%D0%B8%D1%8F).

Согласно сообщениям киберполиции Украины, атака, вероятно, началась через механизм обновления бухгалтерского программного обеспечения M.E.Doc, которую по всей стране используют для подготовки и отправки налоговой отчетности. Это может объяснить, почему пострадало большое количество украинских организаций, в том числе правительство, банки, государственные энергетические компании, киевский аэропорт и метро. Так, например, система радиационного мониторинга в [Чернобыльской АЭС](https://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D1%80%D0%BD%D0%BE%D0%B1%D1%8B%D0%BB%D1%8C%D1%81%D0%BA%D0%B0%D1%8F_%D0%90%D0%AD%D0%A1) была отключена от [сети](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82), вынуждая сотрудников перейти на ручные счётчики и ручное управление в целом. Вторая волна эпидемии была воспроизведена [фишинговой](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3) кампанией с вредоносными вложениями. Сама компания M.E.Doc опровергает, что распространение вируса может быть связано с её файлами обновления. Однако специалисты Microsoft подтверждают, что первые случаи заражения начались именно с установки обновления M.E.Doc.

**Вывод**

Черви каждый год повреждают данные на миллионах устройств. Так как черви наносят непоправимый вред необходимо как можно чаше обновлять алгоритмы их обнаружения и оборудование для пресикания их проникновения.

Для избегания вреда требуется исключить метод социальной инженерии из арсенала злоумышленников методом проведения инструктажа среди персонала и выделить достаточный бюджет для привлечения компетентных специалистов отрасли ИБ и организации безопасности на объекте либо в сетевом пространстве.