Информационное сообщение ФСТЭК России от 02.07.2017 № 240/22/3171 "О мерах по защите информации, направленных на нейтрализацию угроз безопасности информации, связанных с проникновением и распространением вредоносного программного обеспечения WannaCry, Petya, Misha и их модификаций"

В мае - июне 2017 года отмечены масштабные компьютерные инциденты, связанные с проникновением в информационные и автоматизированные системы, в том числе системы органов государственной власти и организаций Российской Федерации, вредоносного программного обеспечения WannaCry, Petya, Misha и их модификаций.

Анализ компьютерных инцидентов, а также вредоносного программного обеспечения WannaCry, Petya, Misha показал, что проникновение указанных вирусов в информационные (автоматизированные) системы и их распространение осуществляется за счет эксплуатации уязвимости операционной системы Windows и пакета программ Microsoft Office (BDU:2017-01034), а также уязвимостей протокола SMB v.1 (BDU:2017-01095, BDU:2017-01096, BDU:2017-01097, BDU:2017-01098, BDU:2017-01099, BDU:2017-01100), позволяющих нарушителю выполнить произвольный код.

После успешного проникновения в информационную систему для распространения некоторых модификаций вредоносного программного обеспечения (Petya/ExPetr) используются методы перехвата учетных данных привилегированных пользователей. Таким образом, наличие указанных уязвимостей даже на одном компьютере локальной вычислительной сети компьютера ставит под угрозу все компьютеры данной системы.

При проникновении в информационную (автоматизированную) систему вредоносное программное обеспечение осуществляет шифрование файлов пользователей и (или) главных загрузочных записей загрузочных секторов машинных носителей информации, что приводит к нарушению целостности и доступности информации, а также к нарушению штатного режима функционирования информационных (автоматизированных) систем.

Отмечаем, что безопасность информации в государственных информационных системах, в

информационных системах персональных данных, а также в автоматизированных системах управления технологическими и производственными процессами на критически важных объектах должна обеспечиваться в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17, Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. № 21, а также в соответствии с Требованиями к обеспечению защиты информации в автоматизированных системах управлениях производственными и технологическими процессами на критически важных объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды, утвержденными приказом ФСТЭК России от 14 марта 2014 г. № 31.

Указанными нормативными правовыми актами ФСТЭК России установлена необходимость реализации в информационных (автоматизированных) системах мер защиты, направленных на нейтрализацию угроз безопасности информации, связанных с проникновением и распространением вредоносного программного обеспечения WannaCry, Petya, Misha и их модификаций. К указанным мерам по защите информации относятся:
обновление программного обеспечения до актуальных версий;
выявление и анализ уязвимостей информационной (автоматизированной) системы и оперативное устранение выявленных уязвимостей;
обнаружение и реагирование на поступление в информационную (автоматизированную) систему незапрашиваемых электронных сообщений (электронных писем, документов);
периодическое резервное копирование информации на резервные машинные носители информации и обеспечение возможности восстановления информации с резервных машинных носителей информации;
защита периметра информационной (автоматизированной) системы (исключение доступа к TCP-портам 139 и 445).

Кроме того, защита от угроз безопасности информации, связанных с проникновением вредоносного программного обеспечения, обеспечивается применением средств антивирусной защиты, в которых реализованы эвристические методы выявления вредоносного программного обеспечения, систем обнаружения (предупреждения) вторжений (атак), в которых настроены соответствующие решающие правила, а также систем управления и корреляции событий с настроенными индикаторами на действия вредоносного программного обеспечения WannaCry, Petya, Misha и их модификаций.

В ходе контроля состояния технической защиты информации в информационных (автоматизированных) системах органов государственной власти и организаций, проводимого ФСТЭК России в пределах своих полномочий, выявляются нарушения указанных выше требований по защите информации, что создает условия для реализации угроз безопасности информации, связанных с проникновением и распространением вредоносного программного обеспечения WannaCry, Petya, Misha и их модификаций.

Обращаем внимание специалистов по защите информации, операторов информационных

(автоматизированных) систем на необходимость неукоснительного выполнения требований по защите информации в информационных (автоматизированных) системах. Принятие указанных выше мер по защите информации позволит существенно снизить вероятность возникновения угроз безопасности информации, связанных с проникновением и распространением вредоносного программного обеспечения WannaCry, Petya, Misha и их модификаций.

Заместитель директора
ФСТЭК России
В.Лютиков