ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
о применении сертифицированных по требованиям безопасности информации операционных систем Windows Server 2003 и Windows Server 2003 R2 в условиях прекращения их поддержки разработчиком

от 19 июня 2015 г. № 240/24/2497

По информации, полученной от ООО «Майкрософт Рус», компанией Microsoft Corporation (США) с 15 июля 2015 г. прекращается поддержка и выпуск обновлений для операционных систем Windows Server 2003 и Windows Server 2003 R2, в том числе направленных на устранение ошибок и уязвимостей в указанных операционных системах.

В настоящее время в системе сертификации ФСТЭК России сертифицированы по требованиям безопасности информации следующие версии операционных систем Windows Server 2003 и Windows Server 2003 R2:

Windows Server 2003 Standard Edition с пакетом обновлений Service Pack 2 (сертификат соответствия № 1017/4 от 5 августа 2008 г., срок действия – до 5 августа 2017 г.);

Windows Server 2003 Standard Edition Release 2 с пакетом обновлений Service Pack 2 (сертификат соответствия № 1017/5 от 5 августа 2008 г., срок действия – до 5 августа 2017 г.);

Windows Server 2003 Enterprise Edition Release 2 с пакетом обновлений Service Pack 2 (сертификат соответствия № 1017/7 от 5 августа 2008 г., срок действия – до 5 августа 2017 г.).

При этом в соответствии с эксплуатационной документацией на указанные сертифицированные версии операционных систем Windows Server 2003 и Windows Server 2003 R2 обязательным условием их применения в информационных системах является установка сертифицированных обновлений операционных систем Windows Server 2003 и Windows Server 2003 R2, выпущенных разработчиком (компанией Microsoft Corporation) и предоставляемых российским производителем операционной системы (заявителем).

В настоящее время значительная часть сертифицированных версий операционных систем Windows Server 2003 и Windows Server 2003 R2 продолжает применяться для защиты информации конфиденциального характера (в том числе персональных данных) в информационных системах федеральных

органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций (далее – органы государственной власти и организации). Это обусловлено, в том числе, наличием большого количества разработанного под Windows Server 2003 и Windows Server 2003 R2 специфичного прикладного программного обеспечения, применяемого для реализации органами государственной власти и организациями своих полномочий.

Необходимо отметить, что прекращение выпуска обновлений сертифицированных версий операционных систем Windows Server 2003 и Windows Server 2003 R2 в сочетании с вероятным обнаружением в них новых уязвимостей приведет к возможности реализации угроз безопасности информации конфиденциального характера, обрабатываемой в указанных информационных системах. Кроме того, прогнозируется повышение интереса к операционным системам Windows Server 2003 и Windows Server 2003 R2 со стороны отдельных категорий нарушителей.

В целях поэтапного перехода органами государственной власти и организациями на сертифицированные по требованиям безопасности информации операционные системы, поддерживаемые их производителями, ФСТЭК России планируется продление до августа 2017 г. (переходный период) сроков действия выданных ранее сертификатов соответствия на операционные системы Windows Server 2003 и Windows Server 2003 R2 с учетом включения в эксплуатационную документацию ограничений на дальнейшее применение изделий в условиях прекращения выпуска обновлений и возможности реализации угроз безопасности информации.

Аттестация по требованиям защиты информации информационных систем, работающих под управлением операционных систем Windows Server 2003 и Windows Server 2003 R2, должна проводиться с учетом ограничений на дальнейшее применение сертифицированных изделий, а также с учетом дополнительных угроз безопасности информации, связанных с окончанием обновления операционных систем Windows Server 2003 и Windows Server 2003 R2, и реализации дополнительных мер защиты информации, направленных на блокирование данных угроз. Для информационных систем, работающих под управлением операционных систем Windows Server 2003 и Windows Server 2003 R2, аттестованных до 15 июля 2015 г., повторная аттестация не требуется. Оценка реализованных дополнительных мер защиты информации осуществляется путем проведения дополнительных аттестационных испытаний в рамках действующих аттестатов соответствия.

Учитывая изложенное, органам государственной власти и организациям, использующим для защиты информации сертифицированные ФСТЭК России версии операционных систем Windows Server 2003 и Windows Server 2003 R2, **рекомендуется**:

1. Спланировать мероприятия по переводу до августа 2017 г. информационных систем на сертифицированные по требованиям безопасности информации операционные системы, поддерживаемые их производителями.

2. До перехода на сертифицированные по требованиям безопасности информации операционные системы с учетом моделей угроз безопасности информации принять следующие дополнительные меры защиты информации, направленные на минимизацию рисков реализации угроз безопасности информации:

установить все актуальные обязательные сертифицированные обновления сертифицированных версий операционных систем Windows Server 2003 и Windows Server 2003 R2, выпущенные российскими производителями (заявителями);

установить запрет на автоматическое обновление сертифицированных версий операционных систем Windows Server 2003 и Windows Server 2003 R2;

провести настройку и обеспечивать периодический контроль механизмов защиты сертифицированных версий операционных систем Windows Server 2003 и Windows Server 2003 R2 в соответствии с руководствами по безопасной настройке и контролю сертифицированных версий операционных систем Windows Server 2003 и Windows Server 2003 R2;

по возможности исключить подключение к сети Интернет и к ведомственным (корпоративным) локальным вычислительным сетям средств вычислительной техники или сегментов информационных систем, работающих под управлением операционных систем Windows Server 2003 и Windows Server 2003 R2;

при невозможности отключения от сети Интернет и (или) от ведомственных (корпоративных) локальных вычислительных сетей средств вычислительной техники или сегментов информационных систем, работающих под управлением операционных систем Windows Server 2003 и Windows Server 2003 R2, применять в обязательном порядке меры по сегментированию информационных систем и защите периметра информационной системы и выделенных сегментов (в том числе путем применения сертифицированных межсетевых экранов, средств антивирусной защиты, систем обнаружения вторжений, средств защиты от несанкционированной передачи (вывода) информации (DLP - систем), средств управления потоками информации);

обеспечить регулярное резервное копирование информации, программного

обеспечения и средств защиты информации, содержащихся на средствах вычислительной техники или в сегментах информационных систем, работающих под управлением операционных систем Windows Server 2003 и Windows Server 2003 R2, на внешние носители информации;

регламентировать и обеспечивать контроль за применением съемных машинных носителей информации, исключив при этом использование не зарегистрированных в информационной системе машинных носителей информации и не проверенных средствами антивирусной защиты;

проводить периодический анализ уязвимостей сегментов информационных систем, работающих под управлением операционных систем Windows Server 2003 и Windows Server 2003 R2, с использованием сертифицированных средств контроля (анализа) защищенности информации, а также периодический контроль целостности установленных операционных систем;

проводить мониторинг общедоступных источников, публикующих сведения об уязвимостях, на предмет появления в них информации об уязвимостях в операционных системах Windows Server 2003 и Windows Server 2003 R2 и принимать меры, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителями выявленных уязвимостей (в том числе за счет применения дополнительных средств защиты информации);

разработать и внедрить правила и процедуры действий должностных лиц в случае выявления уязвимостей в операционных системах Windows Server 2003 и Windows Server 2003 R2 или возникновения инцидентов информационной безопасности, связанных с их применением.

Начальник 2 управления ФСТЭК России В.Лютиков