РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2003 125 471** (13) **A**

(51) МПК[7] **G 06 F 12/14, 11/00**

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2003125471/09, 18.08.2003**

(43) Дата публикации заявки: **20.02.2005 Бюл. № 5**

Адрес для переписки:
394030, г.Воронеж, ул. Студенческая, 36, ГНИИИ ПТЗИ Гостехкомиссии России

(71) Заявитель(и):
Государственный научно-исследовательский испытательный институт проблем технической защиты информации Государственной технической комиссии при Президенте Российской Федерации (RU)

(72) Автор(ы):
Бугров Юрий Григорьевич (RU),
Мирошников Вячеслав Викторович (RU),
Тесцов Алексей Александрович (RU)

(54) СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Формула изобретения

1. Способ защиты информации от несанкционированного доступа в локальной вычислительной сети, основанного на перехвате и анализе сетевого трафика, заключающийся в противодействии несанкционированному копированию и модификации сетевых кадров в среде распространения локальной вычислительной сети, сбору сетевых пакетов и сегментов из несанкционированно перехваченных в среде распространения сетевых кадров, отличающийся тем, что в технологии взаимодействия открытых систем ISO/OSI устанавливают узел безопасности между подуровнем MAC канального уровня и физическим уровнем стандарта взаимодействия открытых систем ISO/OSI, перед передачей сетевого кадра в узле безопасности выделяют служебную информацию, предшествующую полю данных уровня приложений стандарта взаимодействия открытых систем ISO/OSI, осуществляют защитное математическое преобразование служебной информации, передают сетевой кадр с преобразованной служебной информацией из узла безопасности на физический уровень для дальнейшей трансляции в среде распространения локальной вычислительной сети, при приеме сетевых кадров с физического уровня в узле безопасности выполняют обратное математическое преобразование служебной информации, проверяют легитимность полученных сетевых кадров посредством проверки корректности служебной информации после выполнения обратного математического преобразования, осуществляют передачу сетевых кадров на подуровень MAC канального уровня в случае положительного результата проверки корректности служебной информации сетевых кадров, блокируют передачу сетевых кадров на подуровень MAC канального уровня в случае отрицательного результата проверки корректности служебной информации сетевых кадров.

2. Способ по п.1, отличающийся тем, что защитное математическое преобразование выполняют по отношению к информации, содержащейся в заголовках сетевых кадров канального уровня, а также в заголовках всех инкапсулированных сетевых пакетов и сегментов, при этом защитному математическому преобразованию подвергают часть

RU 2003125471 A

RU 2003125471 A

сетевого кадра фиксированного размера, начинающуюся исключительно от начального ограничителя SFD кадра канального уровня и содержащую служебную информацию всех инкапсулированных протоколов от канального до транспортного уровня стандарта взаимодействия открытых систем ISO/OSI.

3. Способ по любому из п.1 или 2, отличающийся тем, что блокируют передачу сетевого кадра с канального уровня на более высокие уровни стандарта взаимодействия открытых систем ISO/OSI для дальнейшей сборки сетевых пакетов, сегментов и файлов минуя обратное математическое преобразование служебной информации при несанкционированном копировании сетевого кадра из среды распространения локальной вычислительной сети.

4. Способ по любому из п.1 или 3, отличающийся тем, что защиту от несанкционированного копирования сетевого кадра осуществляют посредством передачи последнего по среде распространения локальной вычислительной сети со значением контрольной суммы не соответствующим тому, которое будет рассчитано на нелегитимной рабочей станции локальной вычислительной сети.

5. Способ по любому из п.1 или 4, отличающийся тем, что защиту от несанкционированного копирования сетевого кадра осуществляют посредством передачи последнего по среде распространения локальной вычислительной сети с ложным значением поля длины данных кадра, истинное значение которого восстанавливается после обратного математического преобразования служебной информации сетевого кадра на легитимной рабочей станции локальной вычислительной сети.

6. Способ по любому из п.1 или 5, отличающийся тем, что исключают возможность использования в анализаторах протоколов правил фильтраций, основанных на указании MAC-и IP-адресов легитимных участников информационного обмена и используемых ими протоколов сетевого обмена, тем самым противодействуя несанкционированному использованию анализаторов протоколов для мониторинга и перехвата сетевого трафика на нелегитимной рабочей станции локальной вычислительной сети.

7. Способ по любому из п.1 или 6, отличающийся тем, определяют факт модификации сетевых кадров и блокируют передачу несанкционированно модифицированных сетевых кадров с физического уровня на подуровень MAC канального уровня.

RU 2003125471 A

RU 2003125471 A