УДК 681.3.07

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Студент гр. 107316 Поклонский О.Ю.
Кандидат техн. наук, доцент Попова Ю.Б.
Белорусский национальный технический университет

Проблема несанкционированного доступа (НСД) к компьютерам и хранящейся на них информации всегда является актуальной. НСД опасен возможностью прочтения, модификации обрабатываемых электронных документов, внедрением управляемой программы для захвата одного или нескольких компьютеров локальной сети, уничтожением хранящейся информации.

В дополнение к стандартным средствам защиты компьютера необходимо использование специальных средств ограничения или разграничения доступа, которые можно разделить на две категории:

- средства ограничения физического доступа;
- средства защиты от НСД по сети.

Наиболее надежное решение проблемы ограничения физического доступа к компьютеру – использование аппаратных средств, выполняющихся до загрузки операционной системы, называемых «электронными замками». Здесь выполняется создание списка пользователей и ключевых носителей, по которым будет производиться аутентификация пользователя, формирование списка защищаемых файлов. Действия по контролю доступа на компьютер выполняются после его включения и получения управления от BIOS. Замок запрашивает у пользователя носитель с ключевой информацией. При успешной аутентификации замок рассчитывает контрольные суммы файлов, сравнивает полученные контрольные суммы с эталонными и возвращает управление компьютеру для загрузки штатной операционной системы.

Наиболее действенными методами защиты от НСД по компьютерным сетям являются виртуальные частные сети (VPN) и межсетевое экранирование. Суть VPN состоит в следующем: на все компьютеры, имеющие выход в Интернет, устанавливается программное средство - VPN-агент, который автоматически шифрует всю исходящую информацию и следит за ее целостностью с помощью криптографических контрольных сумм, рассчитанных с использованием ключа шифрования.

Межсетевой экран представляет собой программное или программно-аппаратное средство, обеспечивающее защиту локальных сетей и отдельных компьютеров от НСД со стороны внешних сетей путем фильтрации двустороннего потока сообщений.