ЗАЩИТА ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ ПРИ РАБОТЕ В КОМПЬЮТЕРНЫХ СЕТЯХ

В.А. Рыбак, А. Мелешко, А. Шокр

На современном этапе развития науки и техники вопрос актуальности защиты информации не вызывает сомнений. Вместе с тем, объём затрачиваемых средств на организацию информационной безопасности должен определяться ценностью информации и величиной предотвращённого ущерба.

При рассмотрении вопроса защиты информации в компьютерных сетях, где циркулирует информация государственных информационных ресурсов, необходимо учитывать необходимость реализации как организационных, так и технических мероприятий.

Хотя банковская сфера считается достаточно защищённой, ежегодно становится известно о десятках крупных хищениях, выполненных дистанционно и виртуально (без физического присутствия). При этом для беспроводных сетей, когда сигнал распространяется во все стороны от источника, проблема обеспечения безопасных и защищённых транзакций приобретает критическую актуальность.

Существующие на сегодняшний день подходы к обнаружению внешних атак и несанкционированного доступа не в полной мере гарантируют сохранность информации. Вместе с тем применение комбинированных технологий, включая мониторинг трафика по различным сетевым протоколам, позволяет существенно повысить вероятность обнаружения нежелательных вмешательств и своевременно принять меры к защите (включая резервное копирование) предметной информации.

Всё выше сказанное также актуально и применимо для информационных ресурсов в области рационального природопользования и охраны окружающей среды, так как информация о залежах минерально-сырьевых ресурсов, их добыче и транспортировке, выбросах и сбросах, может быть использована злоумышленниками в корыстных целях, и поэтому должна сохраняться должным образом с применением новейших программно-аппаратных средств защиты.

ЗАЩИТА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ В КОНТЕКСТЕ ГЕНЕРАЦИИ КРИПТОВАЛЮТ

В.А. Рыбак, З. Ганбари

Актуальность защиты информации возникла вместе с появлением самой информации и данной проблеме уделяется внимание на протяжении достаточно долгого периода существования человечества. С появлением вычислительной техники и персональных компьютеров задача обеспечения информационной безопасности вынуждена была начать учитывать виртуальные угрозы, которые не проявляются в реальном физическом мире, однако могут полностью удалить важные пользовательские данные.

При невозможности получить доступ к важной информации на винчестере, паролям и номерам кредитных карточек (в силу их полного отсутствия) злоумышленники могут завладеть вычислительными ресурсами (процессором, памятью, видеокартой) и таким образом получить незаконный доход. Это стало возможным с изобретением криптовалют, которые, в отличие от реальных денег, не печатаются национальными банками, а генерируются виртуально.

Современные видеокарты, особенно производимые фирмой ATI, становятся целью для злоумышленников в силу своих специфических возможностей. Так, например, видеоускоритель Radeon R9 390X имеет 44 вычислительных блока с числом операций (ALU) в блоке 64, что позволяет говорить о 2816 потоковых процессорах. Это делает видеокарты во многих случая более предпочтительными для майнинга, при этом их производительность по сравнению даже с самыми мощными процессорами больше в сотни и тысячи раз.

В заключении необходимо отметить, что существующие антивирусные программы и сетевые экраны не могут гарантировать безопасности от указанных выше угроз, поэтому прерывать работы по совершенствованию систем сетевой защиты нельзя. Рассчитывать на получение бесплатных разработок из Интернет наивно. Каждая вторая такая программа сама содержит в себе spyware. Поставщик антивирусной программы (особенно бесплатной версии) может быть сам разработчиком вируса или трояна. Таким образом, разработка методов и средств обеспечения информационной безопасности компьютерных сетей в контексте несанкционированного майнина является важной научной и практической задачей.