

А. А. Черкас
(ВА РБ, Минск)

ОБМАННЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ИНФОРМАЦИОННОЙ СЕТИ

Существующие на сегодняшний день методы и средства защиты информации в информационно-вычислительных системах достаточно разнородны из-за, разнообразных способов и средств несанкционированных действий. Главным недостатком существующих методов и средств защиты информации, включая современные средства поиска уязвимостей автоматизированных систем и обнаружения несанкционированных действий, является то, что они, в большинстве случаев организуют защиту информации лишь от уже выявленных угроз, что показывает определенную степень пассивности защиты.

Адекватный уровень защиты информации можно обеспечить применением комплексного подхода предполагающего использование традиционных организационных и программно-технических средств.

Одним из возможных направлений решения проблемы защиты информации в локальной информационной сети от несанкционированных действий является применение методов обмана. Такие системы получили название ложных или обманных.

Механизм функционирования обманной системы заключается в том, чтобы вовлечь злоумышленника (злоумышленник или легальный пользователь, нарушающий политику безопасности) в диалог с системой. При этом обманные системы имитируют уязвимости реальных информационных систем. Злоумышленнику приходится постоянно решать: работает он с реальной системой или обманной, затрачивая при этом ресурсы (время, вычислительные мощности и т.п.). Вербальная модель системы защиты информации с обманной системой (рисунок 1).

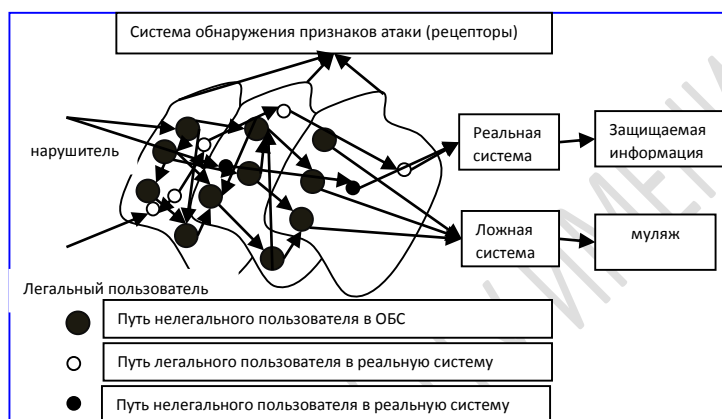


Рисунок 1 – Вербальная модель системы защиты информации с обманной системой

Применение обманных систем защиты информации в локальной информационной сети позволяет в той или иной степени ввести в заблуждение противника, увеличить время для принятия необходимых мер администратором и с некоторой долей вероятности отвести угрозу от реальной работающей информационной системы.

Литература

- 1 Гладких, А.А. Базовые принципы информационной безопасности информационных систем / А.А. Гладких. – УлГТУ.: Ульяновск, 2009. – 168 с.
- 2 Пескова, О. Ю. Использование обманных систем для защиты локальной сети от внешних угроз / О. Ю. Пескова. – М.: ТТИ ЮФУ, 2011. – 12 с.
- 3 Стюард, М. К. Секреты хакеров. Безопасность сетей / М. К. Стюард. – СПб.: Москва – Питер – Киев, 2002. – 699 с.