В.А. Минаев, И.С. Морозов

АНАЛИТИЧЕСКАЯ РАЗВЕДКА КАК СИСТЕМНАЯ ДЕЯТЕЛЬНОСТЬ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Возрастающие требования к управлению в современном обществе, сетевое построение информационных систем и распределенная обработка данных приводят ко все большей глобализации компьютерных сетей. Как следствие, это привело и будет приводить ко все более масштабным проблемам обеспечения информационной безопасности глобальных компьютерных сетей (ГКС). Тем более, что последние стали все более широко применяться в так называемых сферах критических приложений, к которым относятся не только институты государственной власти, но и финансовые структуры, предприятия военно-промышленного комплекса, энергетики, транспорта, а также области производственной деятельности, оказывающие существенное влияние на экологию.

Несмотря на очевидную разнородность сфер критических приложений, их объединяет одно очень важное обстоятельство - значительный ущерб как последствие нарушения безопасности функционирования входящих в них организаций и предприятий, в том числе - в информационной области.

Вытекающая из этого огромная ценность хранимых и обрабатываемых данных в их информационных системах обусловила активную разработку и совершенствование методов и средств противоправного доступа и манипулирования информацией в названных системах.

Основными противоправными действиями с информацией в таких системах выступают различные формы ее несанкционированной модификации (целенаправленная замена или искажение данных, их удаление) или копирования.

При этом сетевые технологии оказались особо уязвимыми для совершенно нового типа источников угроз информационной безопасности – вредоносных программ, при создании которых реализуются принципы реализации компьютерных вирусов. Такие программы обладают рядом свойств, которые, несмотря на предпринимаемые меры защиты, позволяют им во многих случаях практически беспрепятственно осуществлять вредоносное воздействие на информацию в ГКС.

Постоянное совершенствование технологий создания вредоносных программ и механизмов их использования для противоправного манипулирования информацией в ГКС не могли не привести, наряду с разработкой антивирусных программ (их в качестве технических мер безопасности практикуют 95 % предприятий России), межсетевых экранов (75 %), средств шифрования (35 %), виртуальных выделенных сетей – VPN (30 %), к целенаправленному и адекватному совершенствованию технологий обнаружения вредоносных воздействий – IDS (38 %) и математической обработке данных о них с целью оценки степени угроз информационной безопасности ГКС.

Одним из таких направлений, в основу которого положены математические методы обработки данных об информационных атаках или их подготовке, является аналитическая разведка.

Аналитическая разведка имеет все признаки системной деятельности в сфере обеспечения информационной безопасности. Это и разведывательный поиск, и техническая разведка, и комплексный анализ разведывательной информации.

Широкое использование информационных технологий в деятельности спецслужб способствовало как совершенствованию средств и методов, так и правовой базы аналитической разведки. Не будет преувеличением сказать, что сейчас она выступает

полноценным, активно развивающимся направлением оперативно-розыскной деятельности, а в специализированных учебных заведениях страны готовятся высококвалифицированные специалисты в области аналитической разведки.

Одной из основных целей аналитической разведки является оценка и прогнозирование угроз информационной безопасности абонентов ГКС. Безусловно, такая постановка цели влечет за собой решение целого комплекса взаимосвязанных проблем. Достаточно назвать основные из них, чтобы понять всю сложность достижения поставленной цели. Это:

создание адекватной концептуальной модели действий злоумышленника в ГКС;

детальная структуризация и программно-алгоритмическое описание направлений противоправных действий по отношению к информации в ГКС;

мониторинг ГКС с целью идентификации вредоносных программ, намечающихся и реализованных информационных атак;

оперативный анализ функций вредоносных программ и направлений информационных атак;

анализ и оценка степени угрозы информационной безопасности абонентов ГКС.

Основной вывод, который хотелось бы сделать в заключение – это то, что для эффективного функционирования системы информационной безопасности любой организации ее техническая политика должна быть нацелена в будущее, учитывать тенденции развития перспективных информационных технологий. Только на такой основе можно сделать безопасность одним из компонентов общей стратегии и планирования деятельности компании, эффективно управлять инвестиционными процессами в современных условиях.