В.В. Киселев, Е.А. Золотарева

ПРИЗНАКИ РАСПОЗНАВАНИЯ ВРЕДОНОСНЫХ ПРОГРАММ В КОМПЬЮТЕРНЫХ СЕТЯХ

Возросшие требования к оперативности информационных процессов в различных областях деятельности современного общества, а также расширение возможностей сетевого построения информационных систем и внедрение методов распределенной обработки данных за счет реализации теледоступа к вычислительным средствам привело к интегрированию систем обработки информации и систем ее обмена. Результатом такого интегрирования явилось создание компьютерных сетей (КС).

Широкое применение технологии КС в различных сферах общественной деятельности, в том числе в так называемых критических инфраструктурах, к которым относится деятельность институтов государственной власти, финансовых структур, деятельность в областях военно-промышленного комплекса, энергетики, транспорта, а также в областях, оказывающих существенное влияние на экологию, значительно повысило эффективность этих сфер. Несмотря на очевидную разнородность критических инфраструктур их объединяет одно очень важное обстоятельство – значительный ущерб от нарушения безопасности деятельности, в том числе и информационной, в этих сферах.

Значительная ценность хранимых и обрабатываемых данных в критических инфраструктурах обусловила разработку и совершенствование методов и средств противоправного доступа и манипулирования информацией в этих структурах. Основными противоправными действиями с информацией могут быть самые различные формы ее несанкционированной модификации (целенаправленная замена или искажение данных, их удаление) или копирования. При этом сетевые технологии оказались наиболее уязвимыми для совершенно нового типа источников угроз информационной безопасности – вредоносных программ. Разрабатываемые по технологии компьютерных вирусов такие программы обладают рядом свойств, которые позволяют им практически беспрепятственно осуществлять вредоносное воздействие на информацию в КС.

К настоящему времени в теории информационной безопасности сложился ряд направлений противодействия вредоносным программам. Одним из таких направлений, в основу которого положены математические методы, является аналитическая разведка.

Термин "аналитическая разведка" впервые появился в нормативных документах МВД России в 1992 году для обозначения особой формы деятельности оперативно-поисковых подразделений. Аналитическая разведка была определена как разведывательный поиск, техническая разведка, комплексное изучение материалов скрытого наблюдения и оперативной установки, а также анализ сообщений, публикаций и выступлений в средствах массовой информации, статистических данных, сведений автоматизированных банков данных. В дальнейшем аналитическая разведка, кроме оперативно-поисковых подразделений, стала применяться в уголовном розыске, борьбе с организованной преступностью и других направлениях деятельности криминальной милиции.

С 1997 года, когда в нормативных документах МВД России ее понятие существенно расширилось, под аналитической разведкой стали понимать систематизацию и комплексный анализ разведывательной информации [1].

Одним из видов аналитической разведки, целенаправленно используемым для мониторинга КС, является компьютерная разведка. Необходимо отметить, что выбранный термин до настоящего времени не применяется в нормативных документах МВД России. Однако, существует мнение, что в качестве рабочего этот термин наиболее наглядно отражает сущность средств и методов оперативно-розыскной деятельности в рассматриваемой области.

Компьютерная разведка, с учетом специфики объектов, средств и методов исследования, оказывается не только перспективным, мощным и весьма сложным инструментарием оперативно-розыскной деятельности, но и единственным средством анализа угроз информационной безопасности элементов КС в случае, когда источник угроз - вредоносные программы.

К настоящему времени целостная методическая база компьютерной разведки еще не сформировалась. Вместе с тем уже наметился ряд тенденций ее развития. Одним из таких направлений является использование методов теории распознавания.

Анализ информационного пространства КС как объекта угроз информационной безопасности в условиях решения задачи их распознавания позволяет установить следующие группы первичных признаков распознавания:

- данные антивирусного мониторинга информационного пространства КС;

- данные анализа вредоносной программы;

- временные характеристики угроз.

Первую группу признаков составляют:

- новизна;
- целенаправленность;
- активность;
- местоположение;
- траектория движения по сети.

Признак *новизны* вредоносной программы соотносит ее к двум основным типам – известным и неизвестным.

Признак *целенаправленности* характеризует вредоносную программу как средство воздействия на информационное пространство КС – является или не является таким средством. С помощью данного признака можно отфильтровать специализированную вредоносную программу от типового компьютерного вируса.

Признак *активности* характеризует состояние вредоносной программы на текущий момент времени – выполняющей или не выполняющей свои функции.

Признак *местоположения* характеризует фактическое размещение вредоносной программы.

Признаки *траектории движения* вредоносной программы по сети характеризует следующие адреса:

- адрес отправителя вредоносной программы;
- адрес получателя вредоносной программы;
- адреса серверов сети, обеспечивших движение вредоносной программы.

Вторую группу признаков составляют системные вызовы, стандартные процедуры и функции операционной системы, задействованные вредоносной программой.Третью группу признаков составляют величины:

- времени реализации угрозы;
- времени анализа угрозы;
- времени противодействия угрозе.

В соответствии с существующей классификацией признаков первая и вторая группы относятся к классу логических признаков, а третья группа – к классу вероятностных признаков. При этом все признаки второй группы являются статистическими.

Литература

1. Скрыль С.В., Киселев В.В. Аналитическая разведка в оценке угроз информационной безопасности // Системы безопасности, 2003, - № 6(48). - С. 96-97.