производиться не может. Таким образом, возникает задача идентификации вновь обнаруженных воздушных объектов преодолевших разрыв зон радиолокационного наблюдения и отождествление с ранее сопровождаемыми объектами.

В виду актуальности данной проблемы разработана методика сопровождения воздушных объектов в условиях наличия разрывов зон радиолокационного наблюдения.

Она основывается на выделении областей пространства вероятного нахождения воздушного объекта, рассчитанных на основе его летно-тактических характеристик и информации получаемой от средств радиолокации.

Применение данной методики в алгоритмах сопровождения воздушных объектов комплексов средств автоматизации, позволяет повысить достоверность радиолокационной информации, а в целом качество функционирования информационной подсистемы.

Литература

1. *Дубровский В.И.* Эксплуатация средств навигации и УВД. М., 2005.

2. *Кузьмин С.В.* Цифровая обработка РЛИ. Киев. 2001

ПРИМЕНЕНИЕ ОБМАННЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ИНФОРМАЦИОННОЙ СЕТИ

А.А. Черкас, В.В. Моисеев, Е.И. Хижняк

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.

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 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.

Выполняющий все инструкции пользователь, преодолевает все области с наименьшими временными затратами. Нарушитель, пытаясь определить уязвимые места в СЗИ, сканирует поверхность упругого экрана, в результате чего он либо отражается от экрана, либо поглощается областями. Так как площади эмулированных уязвимостей значительно больше, чем реально существующих, то нарушитель с большой вероятностью попадает именно в "муляж". При этом, до некоторого момента времени нарушитель не подозревает, что работает с обманной системой. Пытаясь закрепиться в системе, и найти слабое место в следующей ступени защиты, он проявляет себя. В момент работы обманной системы настоящая система продолжает функционировать и успешно решать возложенные на нее задачи.

Применение обманных систем защиты информации в локальной информационной сети позволяет 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. Ульяновск, 2009.

2. Пескова О.Ю. Использование обманных систем для защиты локальной сети от внешних угроз. М., 2011.