помощью таких технических средств, включает в себя следующие взаимосвязанные этапы: обнаружение, идентификацию и опознавание объекта наблюдения.

На практике, при обнаружении объекта освещенность местности (фона), где он расположен, может создавать экспозицию (освещенность) фотоприемника выше пороговой, поэтому на первый план выходит задача обнаружения объекта с минимальным контрастом относительно фона. В соответствие с чем, важным показателем является контрастная чувствительность оптико-электронной системы, которая определяется минимально необходимым контрастом объекта наблюдения, который может быть обнаружен при пороговом отношении сигнал/шум фотоприемника оптико-электронной аппаратуры.

Для снижения заметности объекта наблюдения используются различные способы его скрытия, которые реализуются на практике за счет использования средств защиты. Одним из подходов в оценке эффективности средств защиты является их натурные испытания, при которых объект наблюдения скрывается с помощью средства защиты и выполняется процедура его обнаружения с использованием оптико-электронной системы обнаружения. Такой подход требует значительных финансовых и временных затрат, а полученный результат оценки эффективности соответствует тем условиям, при которых проводился такой натурный эксперимент.

Отдельные элементы оптического изображения, получаемого с помощью оптико-электронной системы, могут отличаться по яркости, цвету, размеру, геометрической форме, поэтому условием обнаружения объектов является их контраст по выше перечисленным параметрам. Наиболее важным из которых является контраст по яркости.

Возникновение контраста по яркости между объектом и фоном обусловлено отражением объектом и фоном, на котором он размещается оптического излучения, в результате чего объект может быть темнее или светлее фона. Защита информации от утечки по оптическим каналам обеспечивается с использованием средств защиты (маскировочного окрашивания, оптических искусственных масок и т.д.). Их спектральный коэффициент яркости (СКЯ) должен соответствовать аналогичному параметру окружающего фона, на котором обеспечивается скрытие объекта, что позволит существенно снизить демаскирующие признаки объекта. Для оценки их эффективности предлагается использовать следующую методику.

Исследования КСЯ средств защиты выполняется на лабораторном стенде, который содержит источник оптического излучения видимого и ближнего инфракрасного диапазона длин волн и аппаратуру позволяющую обеспечить регистрацию СКЯ при различных углах падения и отражения оптического излучения источника. В результате первого этапа записываются СКЯ исследуемого средства защиты, обработка которых позволяет рассчитать степень поляризации отраженного оптического излучения средством защиты.

На втором этапе рассчитываются дальности обнаружения, опознавания и идентификации объекта наблюдения, скрытого с помощью исследуемого средства защиты, с учетом возможных погодных условий наблюдения и основных технических характеристик телевизионной техники.

Полученные результаты дают возможность проанализировать эффективность исследуемого средства защиты для выбранного варианта применения и разработать рекомендации по его дальнейшему использованию и совершенствованию.

РАСПРЕДЕЛЕНИЕ КЛЮЧЕВОЙ ИНФОРМАЦИИ В СОВРЕМЕННЫХ КРИПТОСИСТЕМАХ

Алхалбус Муаяд Абдулкадес Аббас, В.Ф. Голиков

Современные криптосистемы строятся таким образом, что их надежность обеспечивается стойкими криптографическими алгоритмами взлом, которых без знания секретных параметров, называемых ключевой информацией, даже с использованием самых

передовых математических методов и мощных компьютеров, невозможен за обозримое человеком время.

Однако, в условиях удаленных сеансов связи с использованием открытых электронных каналов с учетом территориальной рассредоточенности и высокой мобильности абонентов возникает задача конфиденциальной доставки ключевой информации.

Криптостойкость используемых алгоритмов, протоколов и процедур существенно зависит от свойств ключевой информации. Под ключевой информацией понимают всю совокупность ключей, используемых в рассматриваемой криптосистеме. Часто нарушителю проще осуществить атаку на ключевую систему, чем непосредственно на сам алгоритм, лежащий в основе криптосистемы.

Важнейшим свойством ключевой информации для симметричных криптосистем является ее конфиденциальность (секретность). Поэтому процесс распределения ключевой информации должен обеспечивать ее максимальную конфиденциальность. По сложившейся в криптографии терминологии под распределением понимается доставка готовой ключевой информации или ее формирование у абонентов системы.

Распределение ключей в симметричных криптосистемах основано на использовании защищенных каналов и криптографических протоколов. В двухключевых и гибридных криптосистемах распространение (передача, распределение) ключей основано на предварительной аутентификации открытых ключей, которая осуществляется некриптографическими методами, и последующем использовании криптографических протоколов. Различают два типа протоколов распределения ключей:

– протоколы передачи (пересылки, доставки) ключей, которые предварительно уже сгенерированы.

– протоколы совместного формирования (выработки) ключей.

Основное отличие второго типа от первого состоит в том, что вырабатываемый ключ зависит от произвольного выбора двух и более сторон и каждая из взаимодействующих сторон получает этот ключ в результате проведенных вычислений. Различают протоколы и схемы распределения ключей между двумя пользователями (протоколы типа «точка — точка»), в которых передача (или выработка) ключей осуществляется в результате непосредственного взаимодействия двух сторон, и между многими пользователями. При распределении ключей между многими пользователями выделяют схемы централизованного распределения ключей.

ПРОГРАММНЫЙ КОМПЛЕКС АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ПРОТИВОДЕЙСТВИЯ АТАКАМ

А.И. Понамарчук, Вахаб Алаа, Т.В. Борботько, Юнис Али Аюб Юнис

Современные информационные системы используются для обработки различных сведений, в том числе в банковском секторе. Атаки на подобные системы приносят существенный ущерб банкам и влияют на их репутацию. Одним из способов противодействия таким угрозам является обнаружение уязвимостей в информационной системе и их своевременное устранение. Для практической реализации указанного способа созданы программные средства, которые позволяют обнаруживать уязвимости, а так же проверять возможность их использования при реализации тех или иных атак. Однако существенной проблемой применения таких средств является решение задачи снижения вероятности ложных тревог. Такая задача может быть решена за счет повышения достоверности получаемых сведений, когда события безопасности регистрируются несколькими датчиками и решение о наличии угрозы принимается на основе корреляции таких событий.

Разработанный комплекс основан на использовании программного обеспечения VMware Workstation и включает в себя: виртуальные машины с IDS/IPS, HoneyPot и с программным обеспечением для имитации атак; интерфейсы настройки HoneyPot, просмотра сообщений о событиях безопасности, управления атаками.