ВВЕДЕНИЕ

Актуальность исследования

В настоящее время проблема защиты информации в целом и проблема защищенности автоматизированных систем как частный случай набирает все большую значимость. Мировое сообщество уже перешло на электронный документооборот, электронные деньги. Все большую популярность набирают электронные системы оплаты услуг, использование электронной почты, IP-телефония. Широкое распространение получили сервисы обмена информацией, мультимедийным контентом, новостями, среди которых наибольшую огласку получили социальные информационные сети. В связи с этим следует выделить такой тип атаки на АС, как «анализ сетевого трафика», которые очень часто применяются злоумышленниками для перехвата паролей, имен учетных записей, номеров банковских счетов[7, 15, 63, 103, 104].

При этом ущерб, нанесенный жертве, зависит от тех действий, которые производились во время сессии. Если в чужие руки попадает информация по кредитным картам, последствия могут оказаться весьма серьезными. Реквизиты этих карт злоумышленники используют для оплаты товаров и услуг по всему миру, естественно, за счет жертвы. Это продолжается до тех пор, пока пострадавший не обнаруживает пропажу денег со счета, что, как правило, происходит лишь в конце месяца, когда он получает выписку по счету[2, 36, 62].

Если злоумышленник получает доступ к корпоративномуэлектронному адресу, то потенциальный ущерб возрастает во много раз. Потери от кражи финансовой информации бывает не просто трудно подсчитать, в некоторых случаях уходят годы на то, чтобы полностью оценить весь причиненный ущерб. Если в результате атаки была украдена и предана огласке конфиденциальная информация (отчеты компании, техническая документация, клиентская база), репутации компании может быть нанесен сокрушительный удар – потеря доверия со стороны клиентов и партнеров, резкое сокращение сбыта продукции компании и даже крах бизнеса [2, 10, 24].

Как видно из статистики, публикуемой различными информационными порталами, число атак на пользовательские данные стремительно растет. При этом особенно уязвимыми элементами сети являются пользователи, использующие беспроводные системы связи [103, 104].

Компания StatCounter отмечает, что с января 2011 года доля мобильного интернет-трафика в среднем по миру выросла почти вдвое с 4,3 до 8,5 процента, при этом двукратный рост мобильного трафика наблюдается ежегодно с 2009 года. В России, по данным StatCounter, доля мобильного трафика в феврале 2012 года составила 2,95% [102].

Наиболее распространенными технологиями мобильной связи являются GSM (европейского стандарта сотовой связи второго поколения) и 3G (от англ. thirdgeneration– третье поколение)[60].

Мобильная связь третьего поколения (3G) строится на основе пакетной передачи данных и обеспечивает более высокую скорость передачи данных, что обуславливает ее широкое распространение среди пользователей Интернет[29, 101].

Как свидетельствует мировая статистика, уровень потерь операторов мобильной связи от разного рода мошенничества и вредительства составляет 2 – 6% от общего объема трафика, а по данным самих компаний он может доходить до 25%. Причем атаки мошенников направлены как против операторов, так и против абонентов [16, 25, 102].

Подсчитано, что из-за мошенничества отрасль мобильной связи во всем мире теряет ежегодно около 25 млрд. долларов, по информации от МГТС (Московской городской телефонной сети) ущерб только по Москве оценивается в пределах 3 – 5 млн. руб. в месяц[104]. Ежегодные убытки операторов сотовой связи в Великобритании, Испании, Германии исчисляются миллионами евро [102]. Поэтому вопросы обеспечения безопасности информации в мобильных сетях являются в настоящее время весьма актуальными и требуют к себе постоянного внимания и анализа.

Не меньшее распространение получили сети Wi-Fi. Большинство современных мобильных устройств оснащаются Wi-Fiадаптерами, а бесплатные точки доступа

Из выше сказанного очевидно, что атаки типа «анализ сетевого трафика»требуют глубокого анализа, изучения способов реализации, а также разработки специфических средств и методов создания системы защиты.

Степень научной разработанности

Как показывает анализ известной литературы, моделирование атак типа «анализ сетевого трафика»на беспроводные каналы связи ранее не проводился, что не позволяет обосновать требования к системе защиты АС от этих атак.

Таким образом, исходя из актуальности и степени научной разработанности проблемы защищенности АС от атак типа «анализ сетевого трафика», представляется целесообразным проведение исследований в данном направлении, изучение алгоритмов реализации атак с последующей разработкой мер по их противодействию.

Объектом исследования являются автоматизированные системы, имеющие в своем составе компоненты, осуществляющие передачу информации по беспроводным каналам, функционирующие в условиях высокого риска реализации атак типа «анализ сетевого трафика».

Предметом исследования выступают процессы реализации атак типа «анализ сетевого трафика» на беспроводные каналыАС и методы противодействия им.

Цель и задачи исследования

Целью настоящей работы является управлениериском от реализации атаки типа «анализ сетевого трафика» на беспроводные каналы АСс целью обеспечения защищенности этих систем.

Для достижения данной цели необходимо решить следующие задачи:

1. Разработать модель атаки типа «анализ сетевого трафика» с учетом особенностей построения АС и наличия ее специфических компонентов, участвующих в процессе передачи информации по беспроводным каналам.

2. Разработатьриск-модельреализации атак типа «анализ сетевого трафика» на основе анализапостроенной модели атаки, учитывающую особенности построения АС и наличия ее специфических компонентов, участвующих в процессе передачи информации по беспроводным каналам.

3. Исследовать динамическую риск-модельреализации атак типа «анализ сетевого трафика» на АС, включающую в себя множество компонентов, участвующих в процессе передачи информации по беспроводным каналам.

4. Разработать новый подход к управлению рискомреализации атак типа «анализ сетевого трафика» на АС, включающую в себя множество компонентов, участвующих в процессе передачи информации по беспроводным каналам.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе, обеспечивается корректным использованием математических методов в приложении обозначенному предмету исследования.

Методы исследования

Для решения поставленных задач необходимо использовать методы системного анализа,математической статистики, теории риска, теории вероятности и информационно-логического метода, предусматривающего анализ большого количества информационных источников и справочной литературы.

На защиту выносятся следующие основные положения работы:

1. Модель реализации атак типа «анализ сетевого трафика» с учетом особенностей построения АС и наличия ее специфических компонентов, участвующих в процессе передачи информации по беспроводным каналам.

2. Риск-модель реализации атак типа «анализ сетевого трафика» на основе анализа построенной модели атаки, учитывающей особенностей построения АС и наличия ее специфических компонентов, участвующих в процессе передачи информации по беспроводным каналам.

няемых алгоритмов кодирования и шифрования трафика и дает возможность уделить особое внимание защите от этих типов атак.

2. Построенная риск-модель может применяться для оценки рисков реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС, определения диапазона ущербов по заданному уровню риска, а также построения систем, устойчивых к атакам данного типа.

3. Исследуемая динамическая риск-модель включает выражения для интегрального риска АСи его экстремумов, которые позволяют оценить защищенность системы в целом, а также выявить наиболее уязвимые компоненты. Динамическая риск-модель позволяет так же определить оптимальные значения параметров компонент АС, при которых максимальное значение интегрального риска и диапазона ущербов по заданному уровню риска не превышают требуемого значения.

4. Подход к управлению риска реализации атак может применяться для оценки эффективности применяемых мер и средств контроля и управления рискомреализации атак типа «анализ сетевого трафика» на беспроводные каналы АС и выбора наиболее подходящих комплексов мер и средствс целью получения приемлемых показателей риска информационной безопасности АС, подвергающихся атакам типа «анализ сетевого трафика» на беспроводные каналы передачи информации.

ЗАКЛЮЧЕНИЕ

Работа посвящена исследованию рисков реализации атак типа «анализ сетевого трафика» на АС, имеющие в своем составе элементы, осуществляющие передачу информации по беспроводным каналам.

В ходе ее выполнения были получены следующие результаты:

1. На основании выполненных исследований разработана научная идея, обогащающая концепцию регулирования интегрального риска реализации асинхронных атак в АС путем выражения смещения интегрального риска через первоначальное выражение функции интегрального риска системы.

2. Предложеныоригинальные суждения по оценке интегрального риска АС, включающей несколько компонент, осуществляющих передачу информации по беспроводным каналам, и экстремумов рискав рамках регулирования риска реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС.

3. Возможностью применения исследуемой динамической риск-модели для оценки рисков реализации атак типа «анализ сетевого трафика» на беспроводные каналы АС доказана перспективность и состоятельность использования полученных выражений для экстремумов интегрального риска с целью его анализа в АС, выявления уязвимых компонент, защите которых необходимо уделить особое внимание, а также для построения защищенных АС.

4. Изменена трактовка понятия анализа сетевого трафика с точки зрения реализации перехвата трафика, циркулирующего в АС, технологического усовершенствования и возможности реализации перехвата в беспроводных каналах АС, а также учитывающая особенности построения таких каналов, такие как наличие канального кодирования и шифрования данных.

5. В ходе проведения оценки остаточного риска доказано, что функция рискареализации атак типа «анализ сетевого трафика» на беспроводные каналы АС является распределением с «тяжелым хвостом», что позволяет оценить остаточный риск путем оценки тяжести «хвоста» для данного вида распределения.