Заключение

Из вышеизложенного видно, что используя различный математический аппарат нами получен эквивалентный вывод о неразрешимости абсолютного определения факта несанкционированной утечки информации через периметр абстрактного наперед заданного контейнера, т.е. не существует алгоритма, который бы позволил однозначно определить является ли ввод/вывод инсайдерским. Речь идет даже не о нехватке ресурсов, а о принципиальной невозможности создать подобный алгоритм. В связи с этим проблема естественным образом переходит из теоретической области в практическую, где применяются частные решения для задач обнаружения утечек. В частности решаются задачи определения утечек по сигнатурам или используются эвристические алгоритмы, а это уже искусство нежели, наука.

Литература:

1. Материалы статьи «Формализм Ф. Лейтольда». [Электронный ресурс] – Режим доступа: http: //ra32.ru/.

СТАТИСТИЧЕСКИЕ И НЕЙРОСЕТЕВЫЕ МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

А.И. Трубей, В.А. Дмитриев, В.В. Анищенко,
ОИПИ НАН Беларуси, г. Минск

История поиска информационных излучений по техническим каналам началась в далеком 1918 году, когда известный американский криптоаналитик Герберт Ярдли был привлечен для исследования методов обнаружения, перехвата и анализа сигналов военных телефонов и радиостанций. Проведенные исследования позволили установить, что подобное оборудование обладает демаскирующими излучениями, которые могут быть использованы для перехвата секретной информации. По мере развития технологий совершенствовались как средства перехвата ПЭМИ, так и средства защиты от перехвата ПЭМИ. В ход идут всевозможные методы маскировки: использование ППРЧ, расширение спектра сигнала до шумоподобности, сверхкороткие выходы в эфир в наиболее безопасное время, выходы в частотные диапазоны, не подвергающиеся контролю со стороны служб защиты. Уже в середине 80-х годов отмечены случаи применения иностранными спецслужбами «закладок» с частотой излучения до 40 ГГц. Технические разработки становятся все более совершенными, алгоритмы передачи информации позволяют создавать устойчивые, не подверженные помехам каналы связи на гораздо более высоких частотах, чем ранее.

В зависимости от природы информационного сигнала можно провести следующую классификацию ТКУИ, обрабатываемой СВТ [1, 2]:

1. Естественные технические каналы утечки информации:

1.1. ТКУИ, возникающие за счет побочных (паразитных) электромагнитных излучений (электромагнитные каналы утечки информации).

1.2. ТКУИ, возникающие за счет наводок побочных (паразитных) электромагнитных излучений (электрические каналы утечки информации).

2. Специально созданные технические каналы утечки информации:

2.1. ТКУИ, создаваемые путем высокочастотного облучения СВТ.

2.2. ТКУИ, создаваемые путем внедрения в СВТ электронных устройств перехвата информации («закладных устройств»).

Особенностью средств радиоперехвата является то, что они ориентированы на поиск произвольных по характеристикам радиоизлучений. Основным способом обнаружения таких сигналов является пороговый энергетический метод, а наиболее важной проблемой его реализации – способ выбора порога обнаружения.

Обеспечение защиты информации от утечки по техническим каналам выполняется тремя основными методами: пассивным, активным или их комбинацией. Пассивный метод заключается в экранировании источника излучения, использовании фильтрации на линиях, а также радиопоглощающих материалов в экранированных объемах. Активный метод предполагает применение специальных широкополосных передатчиков помех.

Защищенность информации, обрабатываемой СВТ, от утечки по электромагнитным каналам обеспечивается при выполнении следующего условия [3].

$$\delta \le \delta_n, \quad \textbf{(1)}$$

где δ – отношение сигнал / шум при обработке сигналов, излучаемых СВТ на входе приемника;

δ_n – предельно допустимое (пороговое) значение отношения сигнал / шум.

Большинство генераторов шума обеспечивает защищенность СВТ с большим запасом, то есть:

$$\delta << \delta_n. \quad \textbf{(2)}$$

Это приводит к значительному засорению эфира, борьба за чистоту которого является важнейшей задачей. В Европе вообще запрещено применение генераторов шума как средств активной защиты [3]. Поэтому необходимо применять адаптивные по мощности и спектру к уровню опасных сигналов генераторы шума, которые, с одной стороны, обеспечивают гарантированную защиту информации, а с другой – не засоряют эфир. Для адаптации генератора шума с целью маскировки электромагнитного излучения СВТ необходимо провести расчет пороговых значений δ_n. Нужно выбирать генераторы под конкретные СВТ, интенсивность излучения шума которых обеспечивается условием:

$$\delta \approx \delta_{п}. \quad (3)$$

В качестве критерия для оценки возможностей средств радиоперехвата будем использовать вероятность обнаружения сигнала P_o. Данная вероятность характеризует возможность средств радиоперехвата при фиксированной (допустимой) вероятности ложной тревоги $P_{лт}$ осуществить выделение сигнала на фоне шума на входе приемника.

Эффективность радиоперехвата, в конечном счете, определяется требуемым отношением сигнал / шум на входе приемника. В общем случае, это отношение обусловлено параметрами радиоприемного устройства, уровнем сигнала, условиями распространения радиоволн. В частности, многолучевое распространение радиоволн в условиях городской застройки снижает показатель эффективности по отношению к потенциально достижимому в 20 – 30 раз. В таблице 1 приведены вероятности обнаружения сигналов P_o для различных статистических и нейросетевых алгоритмов [4].

Установлено, что статистические алгоритмы обеспечивают фиксированное значение вероятности ложной тревоги $P_{лт} \le 10^{-3}$. Вероятность ложно тревоги для сети Хемминга без параметра – $P_{лт} \le 10^{-4}$. [4]. При этом, следует отметить, что для ведения радиоперехвата значения вероятностей $P_{лт}$ должны лежать в диапазоне $10^{-6} – 10^{-3}$.

Проведем обоснование критериев оценки возможностей по скрытию информации, обрабатываемой СВТ (работы на излучение радиоэлектронных средств, информации, передаваемой радиоэлектронными средствами). При определенных допущениях (процесс на входе приемного устройства является случайным и подчиняется нормальному закону распределения, база сигнала – $\Delta F_{пр} T_a \ge 10$, $T_a \le T_{лт}$, значимость ошибок первого и второго рода одинакова и т.д.) вероятность правильного обнаружения сигнала с неизвестными параметрами P_o можно рассчитать по формуле [5]

$$P_o = \Phi\left|\frac{\delta\sqrt{\Delta F_{пр} T_a} - \Phi^{-1}(1 - P_{лт})}{1+\delta}\right|, \quad (4)$$

где $\Delta F_{пр}$ – полоса пропускания тракта приемника, Гц;

T_a – время осреднения (анализа) процесса, с.

Выбор порогового значения $P_{оп}$ целесообразно осуществлять с точки зрения минимизации вероятности полной ошибки, которая рассчитывается по формуле [5]:

$$P_{ош} = P^*(1 - P_o) + (1 - P^*)P_{лт}, \quad (5)$$

где P^* – априорная вероятность наличия сигнала на входе приемного устройства.

Анализ формулы (5) показывает, что для случая наибольшей неопределенности ($P^* = 0{,}5$) значения вероятностей полной ошибки $P_{ош}$ становятся соизмеримыми с вероятностями правильного обнаружения сигнала P_o ($P_{ош} \approx P_o$) при $P_o \approx 0{,}33(1 + P_{лт})$.

Поэтому в качестве порогового значения при решении задач обнаружения сигнала целесообразно принять значение вероятности правильного обнаружения $P_{оп} \approx 0{,}33(1 + P_{лт})$.

Для обеспечения достаточной для инженерных расчетов точности ошибка измерения $P_{ош}$ не должна превышать от значения вычисляемой величины ($P_{ош} \le 0{,}05\ P_o$). Поэтому при решении задачи измерения параметров сигнала в качестве порогового значения вероятности получим $P_{оп} \approx 0{,}91(1 + P_{лт})$.

Из формулы (4), получаем предельно допустимое (пороговое) значение отношения сигнал / шум на входе приемного устройства [5].

$$\delta_{п} = \frac{\Phi^{-1}(P_{оп}) + \Phi^{-1}(1 - P_{лт})}{\sqrt{\Delta F_{пр} T_a} - \Phi^{-1}(P_{оп})}. \quad (6)$$

Средний интервал между ложными тревогами рассчитаем по формуле [5]:

$$T_{лт} = \frac{\sqrt{12}}{\Delta F_{пр}} \exp\left(\frac{\left[\Phi^{-1}(1 - P_{лт})\right]^2}{2}\right). \quad (7)$$

В таблице 2 приведены результаты вычислений по данной формуле при решении задачи скрытия сигнала $P_{оп} \approx 0{,}33(1 + P_{лт})$, а в таблице 3 – при решении задачи скрытия передаваемой информации $P_{оп} \approx 0{,}91(1 + P_{лт})$ (при $T_a \approx T_{лт}$).

Сравнение значений отношения сигнал / шум, вычисленных для конкретного объекта СВТ (при заданных значениях вероятностей обнаружения сигнала и ложной тревоги), с полученными пороговыми значениями позволяет оценить уровень надежности технической защиты информации (если $\delta \le \delta_{п}$, то полагаем, что перехват информации невозможен). Это позволит обосновать целесообразность использования тех или иных технических

Таблица 1 – Зависимость вероятности обнаружения сигнала от отношения сигнал / шум

Алгоритм	Отношение сигнал/шум										
	0.001	0.3	0.5	0.6	0.7	0.8	1	1.2	1,5	2	3
Статистические алгоритмы											
Минимаксный	0.5	0.51	0,697	0,815	0,912	0,965	0,999	0,999	0,999	0,999	0,999
Байеса	0.5	0.56	0,8	0,92	0,97	0,99	0,999	0,999	0,999	0,999	0,999
Знаковый	0.5	0.505	0,525	0,561	0,6	0,648	0,754	0,878	0,968	0,999	0,999
Ранговый	0.5	0.507	0,567	0,617	0,709	0,801	0,942	0,994	0,999	0,999	0,999
Сеть Хемминга с параметром	0.5	0.715	0,857	0,9	0,92	0,94	0,965	0,99	0,993	0,999	0,999
Сеть Хемминга без параметра	0.5	0.51	0,538	0,611	0,699	0,8	0,91	0,976	0,999	0,999	0,999
РБФ-сеть	0.5	0.759	0,913	0,943	0,966	0,977	0,988	0,993	0,997	0,999	0,999
Карты Кохонена	0.504	0.532	0,638	0,68	0,712	0,73	0,745	0,746	0,746	0,748	0,75

Таблица 2 – Зависимость $\delta_п$ от $P_{лт}$ при скрытии (факта наличия) сигнала

Вероятность ложной тревоги $P_{лт}$	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
Отношение сигнал/шум $\delta_п$	0,128	0,055	0,022	0,008	0,003	0,0012

Таблица 3 – Зависимость $\delta_п$ от $P_{лт}$ при скрытии передаваемой информации

Вероятность ложной тревоги $P_{лт}$	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
Отношение сигнал/шум $\delta_п$	0,235	0,088	0,032	0,012	0,004	0,0014

средств защиты и исключить из дальнейшего рассмотрения неопасные средства перехвата или воздействия на информацию, а также избежать излишнего засорения эфира при применении активных мер защиты. Аналогичные результаты получены также для скрытия ПЭМИ видеосистемы и клавиатуры компьютера.

Литература:

1. Хорев А.А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники // Специальная техника. – 2010. – № 2. – С. 39–56.

2. Нагорный С.И., Артамошин С.А. О применяемых технологиях предотвращения утечки информации по техническим каналам // Защита информации. Inside. – 2012. – № 2. – С. 82–86.

3. Акимов В.И., Данилов Н.С., Суворов П.А. Предложения по созданию адаптивных генераторов шума системы зашумления информативных сигналов средств электронно-вычислительной техники // Специальная техника. – 2012. – № 3. – С. 9–13.

4. Прасолова А.Е. Нейросетевые и статистические алгоритмы в задаче обнаружения сигналов // Телекоммуникации. – 2010. – № 2. – С. 2–6.

5. Хорев А.А. Оценка эффективности защиты информации от утечки по техническим каналам // Специальная техника. – 2006. – № 6. – С. 53–61.

ИЗОЛЯЦИЯ ПРИЛОЖЕНИЙ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ПОРТАТИВНЫХ УСТРОЙСТВ

В.Ю. Коваленко, Д.А. Костюк,
БрГТУ, г. Брест

Одной из особенностей встраиваемых систем (ВС) является их длительное функционирование без перезагрузки и/или какого-либо специфического обслуживания. Поэтому для ВС часто характерны повышенные требования к надежности работы системного и прикладного программного обеспечения и устойчивости к сбоям, происходящим по вине как пользователя, так и из-за внутренних ошибок, а также достаточно актуальной становится устойчивость к попыткам проникновения и взлома. С другой стороны, для портативных ВС большая длительность работы сочетается с сильно ограниченным сроком работы без подзарядки. Для увеличения срока непрерывной работы от батареи подобные системы часто оснащают весьма ограниченными ресурсами (на текущий момент типичны частоты центрального процессора до 1ГГц, а чаще 200–400 МГц).

Высокой надежности функционирования многозадачной среды можно добиться несколькими путями: использованием только высококачественного и многократно оттестированного кода; изоляцией от внешних сетей, включая Интернет, использованием дополнительных средств защиты, таких как супервизоры, фаерволы, антивирусные программы. Однако ни одно из решений не является универсальным, а их совокупность оказывается слишком ресурсоемкой для работы на портативном устройстве.

Одним из способов добиться приемлемой производительности при высокой изоляции приложений друг от друга является виртуализация, подразумевающая запуск приложения в изолированной среде (англ. sandbox), когда его действия жестко контролируются виртуальной машиной (ВМ) [1]. Приложение изолировано от других программ и взаимодействует с ними через специальные интерфейсы, а доступ к ресурсам (памяти, портам и т.д.) инкапсулируется и также находится под контролем. В настоящее время это решение широко используется на серверах и высокопроизводительных системах, периодически применяется на рабочих станциях, однако, оно пока не характерно для маломощных портативных систем [2].

В настоящее время в сегменте ВС наблюдается интенсивный рост доли систем под управлением Unix-подобных операционных систем (ОС), в первую очередь, GNU/Linux. Для данного класса программных платформ, благодаря их длительному доминированию в сегменте серверов, сравнительно легко реализуем ряд подходов, обеспечивающих изоляцию отдельных программных компонент и, таким образом, повышающих общую надежность функционирования системы. В рамках данной работы нами выполнена адаптация одного из таких решений для нужд портативных ВС, работающих под управлением GNU/Linux.

Виды виртуализации зависят от того, насколько полно осуществляется эмуляция аппаратного обеспечения для виртуализованной ОС или приложения, и сильно различаются по степени потребления ресурсов хост-системы. К наименее ресурсоемким относятся следующие разновидности:

– частичная или нативная (native) виртуализация предполагает, что виртуальная машина имитирует лишь то количество аппаратного обеспечения, которое необходимо, чтобы она могла быть запущена изолированно; подход позволяет запускать гостевые ОС, разработанные только для той же архитектуры, что и у хост-системы;

– паравиртуализация избавляет от необходимости симулировать аппаратное обеспечение, однако, вместо этого используется специальный программный интерфейс для