ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И НЕТРАДИЦИОННЫЕ УГРОЗЫ

Дмитрий Анатольевич Ловцов

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ПО НАУЧНОЙ РАБОТЕ ИНСТИТУТА ТОЧНОЙ МЕХАНИКИ И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ИМЕНИ С.А. ЛЕБЕДЕВА РОССИЙСКОЙ АКАДЕМИИ НАУК

В настоящее время гарантированную защиту привилегированной информации, перерабатываемой в системах управления различного государственного уровня, включая крупномасштабные государственные системы Российской Федерации «Правосудие», «Выборы», «Управление» и др., то есть эргатических (человеко-машинных) систем (эргасистем), можно обеспечить только путем выявления и нейтрализации всех возможных информационных каналов несанкционированного доступа (НСД) – как традиционных, так и нетрадиционных.

Под *нетрадиционным информационным каналом (unusual, covert, subliminal channel;* тайный, латентный, скрытый, потайной канал) понимается несанкционированный способ (организационный механизм) скрытой передачи нелегальной информации по действующим («традиционным») каналам связи. При этом возможно нарушение системной политики безопасности. Например, способ временной модуляции («задержка – ускорение») санкционированного приема потоков различной внутрисистемной легальной информации, осуществляемой принимающим абонентом (высокого уровня конфиденциальности) и распознаваемой («детектируемой») передающим абонентом (низкого уровня конфиденциальности), в результате чего в обратном направлении (!) как бы скрытно передается нелегальная информация (например, секретный шифр или ключ).

Нетрадиционные информационные каналы (НИК) «невидимы» для современных средств защиты информации даже при условии использования в эргасистеме сертифицированных и проверенных компонентов (согласно ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. – М.: Стандарты, 2002), отсутствуют эффективные методы и средства выявления, контроля и нейтрализации НИК, а также не разработана соответствующая продуктивная теория (известны лишь отдельные опубликованные результаты ее разработки). Поэтому гарантированное обеспечение информационной безопасности эргасистем представляет собой новую актуальную научную и важную прикладную *проблему*.

Решение данной проблемы осложняется тем, что создание и развитие отечественных информационно-компьютерных технологий, внедряемых в эргасистемы, характеризуются широким применением зарубежного технического и программного обеспечения, как общесистемного, так и специального.

Фирмы – производители компьютерной техники не гарантируют при этом отсутствие в поставляемом оборудовании встроенных аппаратно-программных «закладок» (АПЗ), компьютерных «вирусов» и других вредоносных недокументированных возможностей (типа *Aureate/Radiate, Gator, Look2Me, Loki, Back Office 2000 и др.;* см., например: *http://cexx.org/aureate.htm; http://simplythebest. net/info/spyware/gator_ spyware.html)*.

Вместе с тем вероятность наличия деструктивных «злонамеренных» компонентов в используемых компьютерных средствах обусловлена высоким уровнем развития зарубежной микропроцессорной элементной базы (размер АПЗ может составлять несколько Кбайт) и технологий транспортировки и внедрения программ-агентов из глобальных телематических (информационно-компьютерных телекоммуникационных) сетей (типа сетей Интернет, «Релком», «Ситек», *Sedab, Remart* и др.).

Данное обстоятельство служит основанием предполагать, что при определенных условиях деструктивные компоненты могут быть активизированы как непосредственно, так и дистанционно (например,

по информационным каналам Интернет) с целью обеспечения несанкционированного доступа к привилегированной (конфиденциальной) информации, перерабатываемой в эргасистемах. Для нейтрализации соответствующих угроз безопасности конфиденциальной информации как документированной информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации, проводятся государственная сертификация импортного программного обеспечения и специальные проверки импортного технического обеспечения, характеризуемые определенными временными и материальными затратами.

Концептуальные аспекты. Решение данной проблемы возможно, в частности, на базе известной концепции гарантированной защиты информации на основе всестороннего контроля каналов, суть которой заключается в синтезе аппаратно-программной среды, изолированной от внешнего нарушителя информационной безопасности, в которой АПЗ не могут выполнять свои деструктивные функции. В отличие от других известных подходов данная концепция базируется на принципе строгой формализации доказательства изоляции наиболее «чувствительных» аппаратно-программных модулей при сохранении высокой скорости переработки информации, что и обеспечивает гарантированность ее защищенности. Иными словами, предлагаемая концепция базируется на формально-логическом доказательстве гарантированности защиты информации.

Наличие такого доказательства может служить основанием отказа от дорогостоящих и ненадежных процедур поиска не документированных возможностей в импортном программном и техническом обеспечении, что позволит значительно снизить расходы на сертификацию и специальные проверки. С использованием соответствующего формально-логического аппарата представляется возможным создать надежное оборудование гарантированно защищенной переработки привилегированной информации.

Функция всестороннего контроля информационных каналов в эргасистеме включает, в частности, следующие четыре взаимосвязанные задачи: выявление НИК; оценка пропускной способности НИК и опасности, которую несет их скрытое функционирование; выделение сигнала или получение какой-либо информации, передаваемой по НИК; противодействие функционированию НИК вплоть до их нейтрализации (уничтожения).

Для решения данных сложных задач необходимо разработать соответствующий формально-логический аппарат, который, в частности, позволит также осуществлять:

– количественное оценивание защищенности информации, перерабатываемой в реальной эргасистеме, от НСД, осуществляемого с использованием современных НИК;
– формализованное обоснование требований к архитектуре создаваемой эргасистемы, выполнение которых обеспечит гарантированную защиту информации, перерабатываемой в эргасистеме, от НСД с использованием НИК.

В основу такого аппарата, учитывая множественность объектов, связей и отношений в современных телематических сетях, следует положить эффективные статистические критерии (правила) выявления и оценки скрытых каналов (например, построенных на преобразовании метрических расстояний между повторениями выделенного атрибута сообщения).

Целостная же разработка формально-логического аппарата представляется возможной на основе адекватной прикладной классификации и концептуально-логического моделирования современных НИК в эргасистеме.

Классификация и модели НИК. Классификация НИК в эргасистемах возможна по ряду практически значимых признаков, наиболее существенными из которых в настоящее время представляются следующие: механизм передачи данных; типы моделей нелегальных информационных потоков; уровень абстракции описания эргасистемы; механизм кодирования при передаче данных.

По первому признаку, то есть в зависимости от задействованных при передаче информации механизмов, НИК можно разделить на две большие группы:

– стеганографические (технически скрытые в сообщении-«контейнере»);
– сублимографические (организационно нарушающие действующую в эргасистеме политику безопасности).

Каналы первой группы используют для скрытой передачи данных стеганографические схемы, которые призваны скрыть сам факт передачи информации на фоне передачи данных, не вызывающих подозрений, – «контейнера». В зависимости от типа задействованного механизма встраивания данных в «контейнер» эти каналы можно разделить на структурированные и неструктурированные.

Структурированные *стеганографические* схемы используют для встраивания данных в «контейнеры» с формально описанной структурой и формальными правилами обработки.

Широко распространенным подвидом данного типа каналов являются стеганографические каналы в пакетных сетях передачи данных.

Сублимографические НИК представляют собой внутренние информационные потоки в эргасистеме, не разрешенные реализованной в эргасистеме политикой безопасности. Для скрытых каналов данного типа характерно использование для передачи нелегальной информации некоторого разделяемого информационно-вычислительного ресурса. В зависимости от способа использования разделяемого ресурса, среди этих скрытых каналов можно выделить каналы по времени, каналы по памяти, каналы в базах данных и знаний (БДЗ), а также комбинированные каналы.

Скрытые каналы по времени используют в той или иной форме временную модуляцию занятости разделяемого ресурса.

Скрытые каналы по памяти используют разделяемый ресурс как промежуточный буфер при передаче данных.

Скрытые каналы в БДЗ – это каналы, использующие зависимости между данными, возникающие в реляционных базах данных и знаний.

Скрытые комбинированные каналы могут сочетать в себе рассмотренные организационные механизмы.

В случае, когда понятие «нетрадиционный информационный канал» в эргасистеме эквивалентно понятию «нелегальный информационный поток», становится возможным классифицировать каналы данного типа *по второму признаку,* то есть по типам моделей информационных потоков, используемых для их построения/поиска.

К первой подгруппе можно отнести скрытые каналы, являющиеся нелегальными информационными потоками в системах с многоуровневой и дискреционной политиками безопасности. Эти каналы описываются с помощью известных моделей, таких, например, как модель «Белла – Лападула», модель *Take-grant* (см.: *A Guide to Understanding Covert Channel Analysis of Trusted Systems, NCSC-TG-030. – Ver. 1. – National Computer Security Center, 1993*) и др.

Ко второй подгруппе относятся скрытые каналы в эргасистеме, описываемые «шенноновской» моделью информационного потока.

К третьей подгруппе – каналы, описываемые автоматными моделями потоков, например известной моделью *Gogen – Meseguer* (см.: *Goguen J.A., Meseguer J. Security Policies and Security Models // Proceedings of the IEEE Symposium on Security and Privacy. – Oakland, 1982. – P. 11–20*).

Скрытые каналы можно также классифицировать и в зависимости от уровня абстракции описания эргасистемы, на котором функционирует скрытый канал, то есть *по третьему признаку* – на каналы в оборудовании, в микрокоде, в ядре операционной системы, в прикладном программном обеспечении.

В зависимости от используемого при передаче информации механизма кодирования, то есть *по четвертому признаку*, НИК можно классифицировать на детерминированные и стохастические.

Реляционная модель угроз. В соответствии с нормативной концепцией, изложенной в руководящих документах ФСТЭК (см.: Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. – М.: Гостехкомиссия России, 2002), модельное описание информационных угроз эргасистеме должно включать следующие виды описаний:

1) описание основных предположений относительно использования эргасистемы, в том числе особенности физического окружения;
2) перечисление защищаемых активов;
3) описание всех угроз активам эргасистемы, которое, в свою очередь, должно содержать описания:
   – источника угрозы – нарушителя, его компетентности, доступных ему ресурсов и мотивации к нападению;
   – возможностей для нападения, методов и используемых для этого «уязвимостей», характерных для эргасистемы;
   – актива, подвергающегося нападению;
   – последствий реализации угрозы и возможных деструктивных действий.

В связи с этим можно предположить следующее:

1. Эргасистема представляет собой распределенную человеко-машинную систему, компоненты которой (локальные вычислительные системы – ЛВС) соединены между собой через глобальную вычислительную систему (ГВС) общего доступа по защищенным каналам связи. Защищенные каналы связи строятся узлами защиты, находящимися на границе ЛВС и ГВС и реализующими функции виртуальной частной (закрытой) сети.
2. В качестве защищаемых активов рассматриваются следующие основные компоненты эргасистемы: физическое оборудование, программное обеспечение и перерабатываемая привилегированная (конфиденциальная) информация.
3. Нарушитель, не имея прямого доступа к информации и компонентам эргасистемы, обладает возможностью контролировать узлы ГВС, через которые происходит взаимодействие компонентов эргасистемы. У рассматриваемого нарушителя имеются значительные интеллектуальные, вычислительные и финансовые ресурсы. Мотивация нарушителя считается высокой. Кроме того, некоторые компоненты эргасистемы содержат «аппаратно-программные закладки» нарушителя.

В данном случае информационные угрозы активам эргасистемы можно разделить на следующие группы, включая угрозы:

1) нарушения конфиденциальности перерабатываемой в эргасистеме информации;
2) нарушения целостности информации, перерабатываемой в эргасистеме;
3) нарушения целостности программного обеспечения, используемого в эргасистеме;
4) несанкционированного доступа к ресурсам эргасистемы;
5) расширения интеллектуальных возможностей АПЗ;
6) нарушения работоспособности аппаратного обеспечения эргасистемы.

Модельное описание перечисленных угроз можно представить наглядно в табличной (реляционной) форме с конкретными примерами их реализации. Функционально достаточная упорядоченная совокупность разработанных (см.: Ловцов Д.А., Ермаков И.В. Классификация и модели нетрадиционных информационных каналов в эргасистеме // НТИ РАН. Сер. 2. Информ. процессы и системы. – 2005. – №2. – С. 1–7) реляционных описаний наиболее вероятных информационных угроз эргасистеме в целом представляет собой конструктивную реляционную модель потенциальных угроз.

Компьютерное моделирование (см.: Ловцов Д.А., Ермаков И.В. Защита информации от доступа по нетрадиционным информационным каналам // НТИ РАН. Сер. 2. Информ. процессы и системы. – 2006. – №9. – С. 1–9.) ряда организационных (комбинаторных – основанных на временных перестановках информационных пакетов) способов НСД, осуществляемое с использованием различных (детерминированного и стохастического) сублимографических НИК, дало положительные результаты по подтверждению реализуемости рассмотренных угроз и позволило экспери-

Таблица 1

ЭФФЕКТИВНОСТЬ СПОСОБОВ ПРОТИВОДЕЙСТВИЯ НИК

	Способ противодействия НИК			
Тип НИК	Перемешивание	Буферизация	Ложный трафик	Выравнивание
Модуляция расстояний	±	0	±	0
Модуляция временных интервалов	±	±	±	±
Перестановка пакетов по длинам	±	0	±	±

Примечание: «±» – частичное подавление; «0» – отсутствие подавления.

ментально получить соответствующие количественные вероятностно-временные оценки.

Экспериментальный анализ влияния механизмов противодействия на работу НИК показал, что, поскольку различные НИК используют различную модуляцию потока пакетов, для перекрытия каждого из них одни механизмы противодействия являются эффективными и делают передачу данных по НИК практически невозможной, другие затрудняют передачу нелегитимной информации по НИК и снижают их пропускную способность, третьи не оказывают на НИК никакого влияния (табл. 1).

В случае применения таких механизмов противодействия НИК, как выравнивание длин пакетов и вставка ложного трафика, НИК с модуляцией расстояний между пакетами обеспечивает прием лишь части переданных по нему сигналов. Использование буферизации и выравнивания длин пакетов не оказывает на данный НИК никакого влияния вследствие того, что порядок следования пакетов в этом случае остается неизменным.

Применение перемешивания пакетов для противодействия НИК с модуляцией временных интервалов между пакетами приводит к уменьшению доли принятых по НИК сигналов с увеличением длины перемешиваемого буфера. При использовании выравнивания длин пакетов и вставке ложного трафика с увеличением интенсивности применения средства противодействия существенного снижения доли принятой по НИК информации не происходит. Применение буферизации потока пакетов также приводит к снижению доли принятых данных, однако в том случае, если длина буфера, использованная при передаче сигнала НИК и при буферизации, совпадает, наблюдается резкое повышение доли принятой информации. Это связано с тем, что модуляция потока, используемая данным каналом, сходна с результатами буферизации потока.

Доля нелегитимной информации, принятой по НИК с перестановкой пакетов по длинам, равномерно уменьшается с ростом интенсивности всех методов противодействия, кроме буферизации. Это связано с тем, что при буферизации порядок следования пакетов и их длины не изменяются. При выравнивании длин пакетов размываются различия между длинами соседних пакетов, что затрудняет прием сигнала НИК. В случае выравнивания длин всех пакетов до максимальной длины, в потоке не остается пакетов с различными длинами, вследствие чего прием сигнала данного НИК невозможен. При добавлении ложных пакетов наблюдается рост доли принятых по НИК данных в случае добавления 100% ложных пакетов. В этом случае половина пакетов потока, поступающего к приемнику НИК, являются ложными, однако за счет того, что вставка происходит случайно и равномерно, часть сигналов, отправленных передатчиком, все же может быть обнаружена приемником.

В связи с этим для эффективного подавления НИК необходимо при выборе механизмов (способов) противодействия учитывать тип и параметры модуляции, используемой НИК. Выбор механизмов противодействия и их параметров случайным образом может оказаться крайне неэффективным. При этом увеличение интенсивности механизмов противодействия (увеличение длины буфера, в рамках которых происходит перемешивание пакетов, увеличение количества ложных пакетов и др.) неизбежно приводит к ухудшению характеристик легитимного канала связи вплоть до полной невозможности его использования. Часть существующих архитектур эргасистем не позволяет обеспечить защиту от НСД с использованием НИК. Для других архитектур, при выполнении ряда условий и требований, возможно гарантированное снижение пропускной способности НИК ниже установленной границы или их полное устранение, не позволяющее нарушителю осуществить НСД.

В процессе передачи данных по исследованным НИК измеренные характеристики трафика изменяются в сравнении с трафиком, в котором отсутствуют НИК, тем сильнее, чем больше пропускная способность НИК практически для всех схем кодирования, используемых НИК. Ни один из способов противодействия НИК не обеспечивает подавление всех рассмотренных НИК. Изменяя параметры модуляции, применяемой НИК, возможно обойти алгоритм противодействия, хотя это приведет к снижению пропускной способности НИК и ухудшению характеристик легитимного канала связи.

Повышая интенсивность средств противодействия, тип которых правильно подобран в зависимости от применяемой НИК модуляции, возможно снизить пропускную способность НИК до заданного предела. При этом, однако, характеристики легитимного канала связи резко ухудшаются вплоть до невозможности его использования.

В целом имеющиеся экспериментальные результаты позволяют сделать следующий основополагающий *вывод*: обеспечение гарантированной защиты современных эргасистем от НСД по НИК возможно при использовании «туннелирования» стандартных протоколов с использованием протоколов с минимальной избыточностью, не позволяющих модулировать поток пакетов. При этом пакеты стандартного протокола должны инкапсулироваться в пакеты протокола «туннелирования».

Таким образом, на основе комплексного теоретико-экспериментального анализа защищенности современных эргасистем от НСД по нетрадиционным (скрытым) информационным каналам, предложены прикладная классификация НИК, позволяющая оценить современное состояние проблемы обеспечения полноты их контроля; модели НИК, определяющие механизмы (схемы) их образования, а также функционально достаточная реляционная модель информационных угроз эргасистеме, обусловленных наличием НИК; оценена эффективность некоторых способов противодействия конкретным типам НИК, позволяющим снизить пропускную способность НИК или полностью устранить их.

Полученные в настоящее время соответствующие частные формально-логические результаты имеют важное теоретическое и прикладное значение в области решения выявленной проблемы *гарантированного* обеспечения информационной безопасности эргасистем.

С учетом всех современных достижений в данной сфере сотрудниками отечественного ООО «Криптоком» *(www.cryptocom.ru)* разработаны соответствующие национальные стандарты (ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. – М.: Стандартинформ, 2008; ГОСТ Р 53113.2-2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, ИТ и АС от атак с использованием скрытых каналов. – М.: Стандартинформ, 2009) защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.

Данные стандарты, являющиеся, по существу, первыми в мире, позволяют профильным учреждениям и компаниям начать организованную рациональную коллективную разработку способов и методов противодействия НИК (скрытым каналам) и гарантированного обеспечения информационной безопасности эргасистем.

Для формирования продуктивной теоретической базы создания и разработки эргасистем нового поколения, обладающих повышенной (гарантированной) информационной безопасностью, необходимы дальнейшие согласованные широкомасштабные теоретико-прикладные исследования и опытно-конструкторские работы. Это позволит также сократить прямые и эксплуатационные затраты на информационную защиту существующих эргасистем.