УДК 681.3

В. А. Артамонов

DLP – СИСТЕМЫ : ФУНКЦИОНИРОВАНИЕ И МОДЕЛЬ

(Часть 1. Принципы функционирования)

В последнее время упоминания об утечках информации из самых разных – коммерческих, некоммерческих, государственных и пр. организаций в новостных лентах информационных агенств и Интернет становятся фактически ежедневными. В связи с ростом таких инцидентов естественно растет интерес к системам, которые могли бы противостоять подобного рода угрозам.

Сама проблема обеспечения конфиденциальности информации стара как мир. Ранее задача предотвращения утечек конфиденциальных данных из информационных систем решались в основном тремя способами. Во-первых, методом ограничения прав доступа субъектов к различным информационным ресурсам (ролевое управление, дискреционный и мандатный допуск к ресурсам) во-вторых, за счет использования программного обеспечения (ПО) контроля внешних устройств (USB, CD-ROM и пр.) – на уровне можно/нельзя использовать этот носитель, и, в третьих, за счет шифрования данных.

Однако данные способы статичны и позволяют обеспечить защиту конфиденциальной информации, только в местах ее хранения ***(Data-at-Rest),*** и не дают возможности контроля за процессом обработки и передачи информации.

В результате появились специализированные технологии и решения, которые могут контролировать данные в процессе обработки и передачи ***(Data-in-Motion)*** по различным каналам: HTTP, SMTP, передача данных на сменные устройства, печать на локальные и сетевые принтеры и т.д. При этом охват каналов должен быть как можно более полным, чтобы решение можно было назвать полноценным. Не менее важна и задача анализа передаваемой информации. Система должна реагировать только на конфиденциальную информацию и свободно пропускать информацию, которая не относится к этой категории.

Что такое современные системы DLP ***(Data Leak Prevention)*** – это технологии, позволяющие предотвратить утечку из организации именно конфиденциальной информации. При этом информация, которая не попадает в категорию «конфиденциальная» может свободно передаваться по любым электронным каналам.

В течение последних нескольких лет использовалась разная терминология: Information Leakage Protection (ILP), Information Leak Protection (ILP), Information Leakage Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), Extrusion Prevention System (EPS) и др. Но наиболее точным термином принято считать Data Leak Prevention (DLP,

предложен агентством Forrester в 2005 г.). В качестве русского аналога принято словосочетание «системы защиты конфиденциальных данных от внутренних угроз».

При этом, под внутренними угрозами подразумевают как умышленные злоупотребления, так и непреднамеренные действия сотрудников в рамках своих прав доступа к данным.

Если говорить об истории развития DLP-технологий, то первыми появились технологии сетевого мониторинга – без возможности блокировки утечки через сетевые протоколы (HTTP, SMTP и пр.). В дальнейшем производители решений добавляли функции блокировки информации при передаче через сеть. Затем появились возможности контроля рабочих станций за счет внедрения программных «агентов», чтобы можно было предотвратить передачу конфиденциальной информации с этих устройств: контроль функций ***«copy/paste»,*** снятия скриншотов, а также контроль передачи информации на уровне приложений. И, наконец, появились технологии поиска конфиденциальной информации на сетевых ресурсах и ее защиты, если информация обнаружена в тех местах, где ее не должно быть. Конфиденциальная информация при этом задается предварительно ключевыми словами, словарями, регулярными выражениями, «цифровыми отпечатками» и др. В результате поиска система может показать – где она обнаружила конфиденциальную информацию, и какие политики безопасности при этом нарушаются. Далее сотрудник (офицер) службы безопасности может принимать соответствующие меры, в соответствии с инструкцией по расследованию инцидентов по нарушению ИБ. Есть решения, которые не просто показывают наличие конфиденциальной информации в неположенном месте, а переносят эту информацию «в карантин» (по аналогии с антивирусными системами), оставляя в файле, где была обнаружена информации, запись – куда перенесена конфиденциальная информация и к кому обратиться за получением доступа к этой информации.

На текущий момент на рынке представлено довольно много DLP-решений, позволяющих определять и предотвращать утечку конфиденциальной информации по тем или иным каналам. Однако действительно комплексных решений, покрывающих все существующие каналы, значительно меньше. В этих условиях чрезвычайно важным становится выбор технологии, обеспечивающей защиту от утечек конфиденциальной информации с максимальной эффективностью и минимальным количеством ложных срабатываний.

Первое, чему следует уделить внимание при выборе DLP-решения – это как данное решение осуществляет анализ передаваемой информации и какие технологии используются для определения наличия конфиденциальных данных?

Для защиты корпоративных данных от утечек этого недостаточно – нельзя просто делить информацию на конфиденциальную и неконфиденциальную. Нужно уметь классифицировать информацию по функциональной

принадлежности (финансовая, производственная, технологическая, коммерческая, маркетинговая), а внутри классов – категоризировать её по уровню доступа (для свободного распространения, для ограниченного доступа, для служебного использования, секретная, совершенно секретная и так далее).

Большинство современных систем ***лингвистического анализа*** используют не только контекстный анализ (то есть в каком контексте, в сочетании с какими другими словами используется конкретный термин), но и семантический анализ текста. Эти технологии работают тем эффективнее, чем больше анализируемый фрагмент. На большом фрагменте текста точнее проводится анализ, с большей вероятностью определяется категория и класс документа. При анализе же коротких сообщений (SMS, интернет-пейджеры) ничего лучшего, чем ***стоп-слова***, до сих пор не придумано.

Всего существует пять методов анализа:

Поиск по словарям (по точному совпадению слов, в некоторых случаях с учетом морфологии)

Регулярные выражения. Регулярные выражения — система синтаксического разбора текстовых фрагментов по формализованному шаблону, основанная на системе записи образцов для поиска. Например, номера кредитных карт, телефонов, адреса e-mail, номера паспортов, лицензионные ключи и т.п.

Сравнение по типам файлов. Политиками безопасности может быть запрещена отправка вовне некоторых типов файлов. При этом если пользователь изменит расширение файла, то система все равно должна «опознать» тип файла и предпринять необходимые действия.

Статистический («поведенческий») анализ информации по пользователям. Если пользователь имеет доступ к конфиденциальной информации, и в то же время он посещает определенные сайты (web-storage, web-mail, хакерские и т.п.), то он попадает в «группу риска» и к нему возможно применение дополнительных ограничивающих политик безопасности. Статистические технологии относятся к текстам не как к связной последовательности слов, а как к произвольной последовательности символов, поэтому одинаково хорошо работают с текстами на любых языках. Поскольку любой цифровой объект – хоть картинка, хоть программа – тоже последовательность символов, то те же методы могут применяться для анализа не только текстовой информации, но и любых цифровых объектов. И если совпадают хеши в двух аудиофайлах – наверняка в одном из них содержится цитата из другого, поэтому статистические методы являются эффективными средствами защиты от утечки аудио и видео, активно применяющиеся в музыкальных студиях и кинокомпаниях.

Технологии цифровых отпечатков. Наиболее перспективные и достаточно сложные технологии, при которых производятся определенные математические преобразования исходного файла (алгоритмы эвристических преобразований производителями, как правило, не

раскрываются). Процесс преобразования строится следующим образом: исходный файл – математическая модель файла – цифровой отпечаток. Такой процесс позволяет существенно сократить объем обрабатываемой информации (объем цифрового отпечатка не более 0,01 от объема файла). Цифровые отпечатки затем размещаются в центральном репозитарии (Oracle, MS SQL) и могут быть продублированы в оперативной памяти устройства, осуществляющего анализ информации (зависит от производителя и типа развертывания). Отпечатки затем используются для сравнения и анализа передаваемой информации. При этом отпечатки передаваемого и «модельного» файлов могут совпадать не обязательно на 100%, процент совпадения может задаваться (или «зашивается» в ПО производителем). Технологии устойчивы к редактированию файлов и применимы для защиты практически любых типов файлов: текстовых, графических, аудио, видео. Количество «ложных срабатываний» не превышает единиц процентов (все другие технологии дают 20-30% ложных срабатываний). Эта технология устойчива к различным текстовым кодировкам и языкам, используемым в тексте.

Также следует обратить внимание на систему отчетности и наборы преднастроенных политик безопасности, представляемых DLP-решением, так как это поможет избежать некоторых проблем и сложностей при внедрении.

Основная проблема внедрения – это, как правило, отсутствие классификации данных. Поэтому на первом этапе внедрения система DLP должна проработать в организации в режиме мониторинга до полугода. В этом режиме на базе преднастроенных в соответствии с типом предприятия (промышленные предприятия, медицинские или образовательные учреждения или др.) политик безопасности система может помочь выявить места хранения и способы обработки и передачи конфиденциальной информации.

Для финансовых организаций, которые на текущий момент являются основными потребителями DLP-решений, проблема с классификацией данных нивелируется уже имеющимися в наличии достаточно качественными преднастроенными политиками, предоставляемыми производителями DLP-решений.

После принятия решения о завершении этапа мониторинга, система переводится в режим либо нотификации пользователей и сотрудника безопасности, и/или в режим блокирования передачи конфиденциальной информации.

Когда система DLP работает в режиме мониторинга, то количество инцидентов в силу отсутствия «кастомизации» политик может насчитывать тысячи. Постепенно применяемые политики безопасности настраиваются в соответствии с реальными потребностями и возможностями организации таким образом, чтобы уже в режиме нотификации, а в дальнейшем и блокировки, количество инцидентов не было «зашкаливающим» и система «отлавливала» только действительно конфиденциальную информацию.

Таким образом, полный цикл внедрения решения может занять около года в случае крупной организации.

Система DLP, как правило, состоит из множества компонент. В состав типового решения DLP, как правило, входят:

1. Центральный сервер управления (монитор обращений), выполняющий следующие функции:

– объединение всех остальных компонентов DLP - решения в единую систему;

– определение данных, содержащих конфиденциальную информацию;

– создание, редактирование и распространение политик безопасности для работы с конфиденциальными данными;

– реализация правил разграничения доступом;

– сбор, хранение и обработку инцидентов, создание и рассылку отчетов;

– предоставление ролевого доступа к управлению системой сотрудникам службы информационной безопасности;

2. Модули мониторинга и блокировки конфиденциальной информации, передаваемой по сетевым каналам. Они могут быть представлены как одним устройством, реализующим обе функции, так и отдельными (например, Network Monitor, Network Prevent for Web, Network Prevent for E-mail).

3. Агенты для рабочих станций и серверов, обеспечивающие контроль:

– перемещения конфиденциальных данных на сменные носители информации (USB, CD/DVD и др.);

– помещения данных в буфер обмена ***(функция «Вставка/Копирование»);*** функции снятия снимка с экрана ***(«Print Screen»);***

– контроль функции поиска конфиденциальных данных на локальных дисках.

При всём этом отметим, что системы DLP на сегодняшний день достаточно эффективный инструмент для защиты конфиденциальной информации только в интеграции с другими сервисами безопасности и актуальность интегрированных решений будет со временем только увеличиваться. Даже уже сейчас, в свете необходимости обеспечения требований ФЗ-№152 и ПП РФ-№ 1119, на особенности внедрения DLP-систем нужно посмотреть под совершенно другим ракурсом. Согласно статье 19 ФЗ-№152 («Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий») и пунктам 4,6 и 7 Постановления РФ-№1119 («Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной

службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона «О персональных данных» и в части угроз (каналов утечки информации) – « Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия »…, «Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18^1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных»…).

Учитывая многообразие угроз/уязвимостей (каналов утечки информации), которым подвержены современные системы информационно – коммуникационных технологий (ИКТ) [1], в дальнейшем DLP- системы целесообразно рассматривать как специфичный сервис безопасности ИКТ-технологий со всеми присущими ему свойствами и ограничениями, но не как некую «панацею» от всех бед.

Л и т ер а т у р а

1.Артамонов В.А., Артамонова Е.В. Каналы утечки информации.// Аналитический обзор. [Электронный ресурс] – Точка доступа: http://itzashita.ru/analitics/analiticheskij-obzor-kanaly-utechki-informacii.html.

УДК 681.3

В. А. Артамонов

DLP – СИСТЕМЫ : ФУНКЦИОНИРОВАНИЕ И МОДЕЛЬ

(Часть 2. Математическая модель)

В основу построения математической модели положим принципы объектно – ориентированного подхода и поэтапной декомпозиции слабо формализуемых сред. Весьма распространённой конкретизацией объектно – ориентированного подхода являются компонентные объектные среды, с введением самостоятельных понятий: ***компонент*** и ***контейнер.***

Неформально ***компонент*** можно определить как многократно используемый объект, допускающий обработку в инструментальном (в том числе графическом) окружении и сохранение в долговременной памяти.

Контейнеры могут включать в себя множество компонентов, образуя общий контекст взаимодействия с другими компонентами и с окружением. Контейнеры могут выступать в роли компонентов других контейнеров.

Компонентные объектные среды обладают всеми достоинствами, присущими объектно – ориентированному подходу:

- инкапсуляция объектных компонентов скрывает сложность реализации, делая видимым только предоставляемый вовне интерфейс;
- наследование позволяет развивать созданные ранее компоненты, не нарушая целостности объектной оболочки;
- полиморфизм по сути даёт возможность группировать объекты, характеристики которых, с некоторой точки зрения, можно считать сходными.

Введённые понятия компонента и контейнера необходимы нам потому, что с их помощью мы можем естественным образом представить защищаемую систему (продукт) ИКТ и сами защитные средства (сервисы безопасности). В частности, контейнер может определять границы контролируемой зоны, задавая тем самым так называемый «периметр безопасности».

Таким образом, руководствуясь изложенными выше принципами, перейдём к поэтапному формированию модели DLP-систем начиная от политик безопасности как совокупности правил разграничения доступом (ПРД) субъектов к объектам в рамках контролируемых этими системами контейнеров.

Дискреционная политика безопасности – политика безопасности, основанная на дискреционном управлении доступом, которое определяется двумя свойствами:

- все субъекты и объекты системы идентифицированы;

- права доступа субъектов на объекты системы определяются на основе некоторого внешнего по отношению к системе правила.

Основным способом задания дискреционной политики безопасности является построение таблицы прав доступа субъектов к объектам:

	Субъект 1	Субъект 2	…	Субъект k	…
Объект 1	Права 1-1	Права 2-1		Права k-1	
Объект 2	Права 1-2	Права 2-2		Права k-2	
…	…	…	…	…	…
Объект n	Права 1-n	Права 2-n		Права k-n	
…	…	…	...	…	…

Здесь ***Права i-j*** – набор прав доступа субъекта ***i*** к объекту ***j*** (например «**RWE**» – набор прав на чтение (Read), запись (Write) и выполнение (Execute)). Формальная теория дискреционной политики безопасности изложена нами в [1].

Мандатное разграничение доступа предполагает назначение объекту грифа секретности (метки конфиденциальности), а субъекту – уровня допуска. Доступ субъектов к объектам в мандатной модели определяется на основании правил «не читать выше» и «не записывать ниже». Это означает, что пользователь не может прочитать информацию из объекта, уровень доступа которого выше, чем его уровень допуска. Также пользователь не может перенести информацию из объекта с большим уровнем доступа в объект с меньшим уровнем доступа.

Для реализации этого принципа должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т. п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.

Комплекс средств защиты (КСЗ), а в данном контексте мы подразумеваем DLP-систему, при вводе/выводе новых данных должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов и объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

DLP-сервис должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе любого из субъектов:

- субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше,

чем иерархическая классификация в классификационном уровне объекта, и иерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;

- субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в иерархические категории в классификационном уровне объекта.

Реализация мандатных правил разграничения доступа должна предусматривать возможности сопровождения – изменения классификационных уровней субъектов и объектов специально выделенными субъектами (например, «офицерами безопасности»).

В DLP-системе как в КСЗ должен быть реализован диспетчер доступа (монитор обращений), т.е. средство, осуществляющее перехват всех обращений субъектов к объектам в пределах выделенного контейнера, а также разграничение доступа в соответствии с заданными ПРД. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными и мандатными ПРД. *Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.* Более полный формализм мандатного разграничения доступа изложен нами в [2].

Оценка сложности лингвистического анализа информации покидающей контейнер будет базироваться на модификации формализма Ференца Лейтольда в части более точного моделирования компьютеров и операционных систем [3].

Для этого предлагается сигнатурный метод обнаружения утечки информации из контейнера по строке или подстроке её кода. Естественно, таким образом невозможно обнаружить так называемые полиморфные утечки. Но для обнаружения обычных или олигоморфных утечек такой способ годится: олигоморфные утечки могут обнаруживаться по строке или подстроке кода расшифровщика. В случаях, когда обнаружение осуществляется по подстроке кода (либо даже по полному коду распаковщика для олигоморфных утечек) возможны ложные срабатывания. Приведём оценку вероятности ложных обнаружений при следующих допущениях:

- Длина сигнатуры – **N**;
- Общая длина анализируемых данных – **L >> N**;
- Количество символов в алфавите – **n**, и встречаются они в анализируемых данных с равной вероятностью;
- Количество контролируемых DLP – системой объектов – **M**.

В этом случае оценка количества ложных обнаружений будет примерно равна:

$$p \approx L \cdot M \cdot \frac{1}{n^N}$$

Можно также подсчитать вычислительную сложность алгоритма, выполняющего поиск утечек по сигнатуре. Для выполнения поиска требуется последовательно сравнить все ячейки анализируемой строки данных с первыми ячейками сигнатур. В общем случае это **L·M** сравнений. Далее, при обнаружении совпадения потребуется провести сравнение со второй ячейкой сигнатуры. Учитывая вероятность совпадения значения первой ячейки, количество сравнений второй ячейки будет $L \cdot M \cdot \frac{1}{n}$. Аналогично, третьей – $L \cdot M \cdot \frac{1}{n^2}$ и т. д. Общее количество сравнений составит:

$$s = L \cdot M \cdot \left(1 + \frac{1}{n} + \frac{1}{n^2} + \ldots + \frac{1}{n^{N-1}}\right) = L \cdot M \cdot \frac{\frac{1}{n^N} - 1}{\frac{1}{n} - 1}$$

В худшем сценарии, когда все сигнатуры полностью различны, а **n** и **N** достаточно велики, количество сравнений составит **s = L·M·N**. Следовательно, сигнатурный поиск может быть выполнен за полиномиальное время. Необходимо понимать, что полученные оценки приблизительны и соответствуют худшему варианту поиска случайной подпоследовательности в случайной последовательности. На практике код программы анализа и код утечки информации не являются случайными последовательностями и с учетом знания их структуры алгоритм поиска может быть существенно оптимизирован, а оценка времени – уменьшена.

Проблема обнаружения утечек эвристическими методами.

Определение 1. Проблема обнаружения утечек по интерфейсу ввода/вывода информации является задачей теории алгоритмов: ***существует ли эвристический алгоритм, с помощью которого можно было бы определить произошла ли утечка информации, или нет.***

Предполагается, что все данные о структуре программ и машины, на которой они выполняется доступны (очень сильное предположение с нашей стороны – ибо большинство эвристических алгоритмов и программ обнаружение утечек недоступны. И данное действо сродни шаманству в его закрытом исполнении.) Неизвестными являются только данные о наличии утечек. Согласно тезису Тьюринга-Черча (в нашей его модификации), если бы существовал алгоритм обнаружения, можно было бы создать **Машину Тьюринга** (с одной лентой), которая бы выполняла этот алгоритм. Покажем, что такой **Машины Тьюринга** не существует.

Определение 2. Машина Тьюринга с одной лентой может быть определена как совокупность семи элементов:

$$T = \langle Q, S, I, d, b, q_0, q_f \rangle,$$

где Q – множество состояний **Машины Тьюринга**, S – множество символов, которые могут быть записаны на ленте, I – множество символов входящей последовательности, $I \in S$, $b \in S \mid I$ – пустой символ, q_0 – начальное состояние **Машины Тьюринга**, q_f – конечное состояние **Машины Тьюринга**, $d: Q \times S \rightarrow Q \times S \times \{l, r, s\}$ – множество функций перехода, которые состоянию и символу ленты ставят в соответствие новое состояние, новый символ и перемещение по ленте: на шаг влево, на шаг вправо, остаться на месте. Машина начинает свою работу в состоянии q_0 и в дальнейшем меняет состояния согласно функциям перехода в зависимости от текущего состояния и значения ячейки ленты. Попутно ячейки ленты перезаписываются новыми значениями согласно тем же функциям перехода. **Машина Тьюринга** может содержать и большее количество лент, но вычислительная способность такой машины будет находиться в полиномиальной зависимости от вычислительной способности Машины Тьюринга с одной лентой.

Теорема 1. *Не существует **Машины Тьюринга**, которая могла бы определять наличие утечки контейнера ввода/вывода в произвольной программе.*

Доказательство. Рассмотрим программу **P**, которая эмулирует работу **Машины Тьюринга** (произвольной). Программа **P** печатает на выходе **1**, если эмулируемая **Машина Тьюринга** завершает свою работу. Построим простой алгоритм утечки, который сперва запускает программу **P** на случайном, но фиксированном (для данной утечки) входе **B**, после чего начинает выполнять собственно часть контейнерного ввода/вывода. Используя эту конструкцию можно создать программу **V** для любой **Машины Тьюринга**, и эта программа будет программой утечки в том случае, если она сможет произвести несанкционированный ввод/вывод информации, т. е. в том случае, когда **Машина Тьюринга** завершает свою работу на фиксированном для программы **V** входе или, что тоже самое, если программа **P** печатает единицу для данной **Машины Тьюринга** и данного входа. Предположим, что существует **Машина Тьюринга**, способная обнаруживать все факты несанкционированной утечки информации, т. е. такая **Машина Тьюринга T**, которая читает код программы ввода/вывода и печатает **1**, если в коде этой программы содержится код несанкционированного вывода (утечки), и печатает **0**, если этого кода нет нет. Применим машину **T** к программе **V**. Если **T** печатает **1**, значит программа **P** и соответствующая ей **Машина Тьюринга** завершают свою работу на некотором входе **B**. Если **T** печатает **0**, значит программа **P** и соответствующая ей **Машина Тьюринга** никогда не завершит свою работу на некотором входе **B**. Учитывая, что вход **B** и эмулируемая программой **P** **Машина Тьюринга** могут быть любыми, получаем, что **Машина Тьюринга T** способна для любой **Машины Тьюринга** и любого входа определить,

завершит ли данная **Машина Тьюринга** работу на данном входе. Однако мы знаем, что это невозможно. Полученное противоречие доказывает теорему.

Заключение.

Из вышеизложенного видно, что используя различный математический аппарат нами получен эквивалентный вывод о неразрешимости абсолютного определения факта несанкционированной утечки информации через периметр абстрактного наперёд 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.

Л и т ер а т у р а

1. Материалы статьи «Модели безопасности информационных технологий критичных информационно-измерительных систем (часть 2 Модели дискреционного доступа)» [Электронный ресурс] – Режим доступа: http://itzashita.ru/publications/modeli-bezopasnosti-informacionnyx-texnologij-kritichnyx-informacionno-izmeritelnyx-sistem-chast-2.html.
2. Материалы статьи «Модели безопасности информационных технологий критичных информационно-измерительных систем (часть 3 Модели мандатного доступа)» [Электронный ресурс] – Режим доступа: http://itzashita.ru/publications/modeli-bezopasnosti-informacionnyx-texnologij-kritichnyx-informacionno-izmeritelnyx-sistem-chast-3.html.
3. Материалы статьи «Формализм Ф. Лейтольда». [Электронный ресурс] – Режим доступа: http://ra32.ru/