РОССИЙСКАЯ АКАДЕМИЯ НАУК

МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ, НАУКИ И ТЕХНОЛОГИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВСЕРОССИЙСКИЙ ИНСТИТУТ НАУЧНОЙ И ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ (ВИНИТИ)

НАУЧНО • ТЕХНИЧЕСКАЯ ИНФОРМАЦИЯ

Серия 1. ОРГАНИЗАЦИЯ И МЕТОДИКА ИНФОРМАЦИОННОЙ РАБОТЫ

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ СБОРНИК

Издается с 1961 г. № 3 Москва 2004

ОБЩИЙ РАЗДЕЛ

УДК 001.102:004.056.5

А. В. Нестеров

Философия защиты информации

Публикации по защите информации страдают тем же, что и публикации по информации, — отсутствием концептуального определения информации. Рассматривается системный подход к защите информации и безопасности информации.

Защите информации, в том числе полиграфической продукции, всегда уделяется много внимания [1]. Деятельность, связанная с изготовлением защищенной от подделок полиграфической продукции [2], возможна только по лицензии. В соответствии со ст. 17 [3] под лицензирование попадает большой перечень видов деятельности, связанной с разработкой, распространением, использованием шифровальных средств, средств защиты конфиденциальной информации. Подробный анализ защиты полиграфической продукции от фальсификации приведен в [4], а в [5] рассмотрены вопросы лицензирования и сертификации в области защиты информации, однако, несмотря на большое количество как научно-практической литературы, так и правовых и нормативных актов [6–9], проблема защиты информации еще далека от разрешения, в том числе и с концептуальной точки зрения. Например, сложно найти ответы на следующие вопросы. Необходимо ли защищать защиту информации? Где та защита, которая защищает ту защиту? Можно ли защищать нематериальную информацию и что на самом деле защищается? Если модификация есть изменение содержания или объема информации на ее носителях, то что такое содержание информации? Каким термином необходимо именовать изменение открытой информации без согласия автора или владельца информации? Чем отличается сообщение от сведений и как раньше называлось то, что теперь называется информацией с легкой руки Шеннона? Возможна ли абсолютная защита информации или идеальная подмена информации? В чем отличие и сходство понятий *значение, содержание, сущность* и *смысл информации* и что необходимо защищать?

В цели данной статьи не входил анализ всех публикаций по защите информации, поэтому автор приносит свои извинения всем, чьи публикации не упомянуты.

Данная статья рассчитана на широкий круг читателей, в том числе и на неподготовленных пользователей информационных систем, т. е. получателей информации.

Под "защитой информации" [6] понимается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, где под "утечкой информации" понимается неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получение защищаемой информации разведками, а под "несанкционированным доступом" понимается получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации, прав или правил доступа к защищаемой информации.

В соответствии со ст. 20 [7], к целям защиты информации относят предотвращение утечки, хищения, утраты, искажения, подделки информации, а также предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокировке информации.

На наш взгляд, под защитой данных можно понимать деятельность, направленную на предотвращение нарушения целостности, сохранности и подлинности защищаемых данных, а также непосредственно саму защиту как объект, включающий в себя средства и способы защиты, и наконец, создание таких условий для защищаемых данных, при которых гарантированно обеспечивается целостность, сохранность и подлинность данных.

Литература по защите информации страдает тем же, что и литература по информации, — отсутствием концептуального определения информации. Поэтому начнем с краткого анализа понятия *информация*.

В первую очередь мы должны рассмотреть информацию с системных позиций. Информация является продуктом, который продуцируется продуцентом и сопродуцентом. В этой связи можно выделить некоторое средство, которое продуцирует сведения (продукт) по некоторым каналам для получателей. Особенностью информационного средства и канала, как некоторой среды, является то, что эта среда одновременно может передавать и получать сведения, т. е. осуществлять обмен или перемещать их в геометрическом пространстве, а также хранить эти сведения (транспортировать во времени) и, наконец, выполнять какие-либо логические операции в логическом пространстве. Эта особенность сведений заключается в том, что они представлены в виде данных и могут содержать не только собственно данные, но и инструкции по выполнению операций над данными (программы). Получатели также обладают таким свойством и представляют собой целеустремленные индивиды (субъекты — физические лица либо некоторые программно-аппаратные средства), поэтому они выступают не только в роли получателей, но и продуцентов сведений. Мы умышленно не используем термин "информация" по причинам, указанным ниже.

В связи с тем, что мы разделяем понятия "данные, информация, знания" [1], будем использовать термин "данные" для обозначения "информации", нанесенной (внесенной) на (в) информационный носитель. Кроме того, под "носителем" будем понимать не только вещественный носитель, но и материальный, например, в виде электромагнитного процесса (волны). В этой связи при рассмотрении вопросов защиты информации будем различать понятия "данные", "носитель" (конструкцию, материалы) и "технология" (с помощью которой осуществляются операции с информацией и носителем).

Выше был использован термин "сопродуцент", который обозначает, что продуцирование продукта осуществляется продуцентом совместно с сопродуцентом или сопродуцентами. К ним относят поступающие сведения, материалы, энергию и т. п. Понятие "продукт" условно, так как сопродуцент может быть продуктом другого продуцента, однако можно выделить, что существуют два принципиальных контура: информационный — основной — и обеспечивающий, связанный с энергией, материалами и т. п.

В этой связи защита информации является одним из элементов системы безопасности. Можно выделить три составляющие данной системы: подсистема обеспечения безотказности, подсистема обеспечения доступности и подсистема защиты информации. Кроме того, в литературе отмечают, что необходимо иметь систему (подсистему) защиты от угрозы раскрытия параметров подсистемы защиты информации [10]. На наш взгляд, подсистема защиты должна включать данную подподсистему, обеспечивающую маскировку (скрытие) и, при необходимости, имитацию (подмену истинных сведений ложными).

Нельзя согласиться с трактовкой понятия "безопасность информации" в [11], так как в этом случае безопасность сводится только к защищенности (защите) и только состояния информации. Кроме состояния можно, например, выделить условия, в которых находится информация, поэтому защита информации (защищенность информации) должна удовлетворять требованиям норм, в которых определены свойства, правил, в которых определены процедуры (состояния), и условий. Аналогичным требованиям должна удовлетворять и безопасность информации.

Под безопасностью данных (документов) будем понимать не только деятельность по обеспечению защиты данных, безотказности технологии и организации контролируемого окружения, но и мониторинг неконтролируемого окружения. Кроме того, необходимо выделить законодательный аспект, с помощью которого задаются обязательные требования к информационной защите (безопасности) данных в технических регламентах, аспект создания качественных информационных технологий и аспект сертификации (подтверждения) соответствия установленным требованиям защиты данных.

Обычно под безопасностью элемента понимают такие условия, при которых данный элемент не подвергается опасности или степень влияния угрозы минимальна.

Поэтому под безопасностью данных также будем подразумевать защищенные условия существования данных на всех этапах их жизненного цикла, т. е. создания, движения во времени (хранения), в геометрическом пространстве (передачи) и в логическом (элементном) пространстве (оборота) и использования, включая архивирование и утилизацию, при которых обеспечивается их защита от

воздействия по нарушению целостности, сохранности и подлинности.

Обычно выделяют три этапа жизненного цикла продукта: создание, обращение, использование. Обращение продукта подразумевает не только перемещение в пространстве или во времени (хранение), но и оборот, в том числе смену владельца продукта.

Кроме того, необходимо отметить, что к данным как продукту можно отнести носители данных, а также технологии их обращения и оборота, в частности все виды режимов поставки, ремонта, обслуживания программно-аппаратных средств и способов (методов) существования данных.

Безопасность обычно оценивается тремя показателями: вероятностью предотвращения угроз; временем, в течение которого обеспечивается определенный уровень безопасности; вероятностью обнаружения (распознавания) защищенного информационного объекта.

Защита информации является не только пассивной защитой, но и активной защитой, в ее арсенале имеются средства информационного анализа и атаки, т. е. вскрытия защиты (охраны) сведений, информации, программ, данных, которые могут быть или являются опасными или вредными для безопасности информационной системы. Злоумышленники и злоупотребители, в отличие от естественных угроз безопасности информационной системы, применяют средства маскировки и имитации, в том числе имитируют свои следы нарушения безопасности естественными сбоями, отказами, помехами.

Лица или средства, которые пытаются или нарушили безопасность информационной системы (продуцента), могут это совершить путем атаки на: канал обмена сведениями между получателями и продуцентом (нарушение доступности), сам продуцент (нарушение защиты информационной системы) и средства обеспечения (нарушение безотказности). В данной работе мы будем рассматривать только проблемы защиты информации.

В связи с тем, что защита представляет собой материально-вещественный элемент, она должна защищать материально-вещественный объект, а так как информация является идеальным объектом, то термин "защита информации", на наш взгляд, является не корректным, а исторически сложившимся. Как правило, на практике защищают документы, носители информации, отображения (данные), зафиксированные на материально-вещественных элементах, технологии доступа к данным носителям и источникам информации, а также другие свойства информации.

С появлением электронного документа и электронной цифровой подписи данная проблема еще более обострилась, так как электронный документ может быть чисто цифровым, а отношение к нему у многих остается как к традиционному аналоговому документу, при этом подразумевается, что защищать нужно не документ, а информацию. В этой связи, на наш взгляд, объектом защиты является документ (данные), а предметом защиты — сведения, в том числе и информация.

Любая информация (данные) должна (ы) защищаться, однако открытые данные защищают только от естественных воздействий, данные с ограниченным копированием защищают от несанкционированного копирования, а закрытые данные — от любого воздействия.

По открытости данные можно классифицировать на: общедоступные; открытые, защищаемые законодательством, например копирайтом; закрытые данные, которые защищает их собственник, владелец [12]. К закрытым данным относят секретные, коммерческие, служебные, конфиденциальные данные. Закрытые данные защищаются наиболее серьезно и дорогостояще, иногда стоимость защиты достигает 500% стоимости данных. Однако стоимость защиты данных, имеющих коммерческую значимость, как правило, не превышает 50–75% от цены этих данных на рынке. Становится выгоднее приобрести эти данные, чем заниматься вскрытием защиты или приобретать нелегитимные данные. Если защита данных используется многократно и непрерывно, то затраты на ее создание быстро окупаются, поэтому защита данных используется практически во всех сферах человеческой деятельности.

Некоторые авторы [10] считают, что существует три вида угроз автоматизированным системам информации и информации: угроза нарушения конфиденциальности или "утечка информации", когда осуществляется несанкционированный доступ; угроза нарушения целостности — предусматривает умышленное или случайное (несанкционированное) изменение информации; угроза отказа в санкционированном доступе к информации из-за действий злоумышленника или случайных воздействий на информацию.

Термин "утечка информации" стали использовать по аналогии с утечкой электрического тока, газа и т. п., т. е. утечка основного потока через плохую изоляцию от внешней среды в естественных условиях и за счет недостаточной защиты основного потока от воздействия злоумышленников, которые специально организовывают каналы "утечки информации".

Целостность открытых данных отличается от целостности защищенных данных. Под целостностью открытых данных или просто данных (сообщений, информации, сигналов и т. п.) обычно понимают неискажаемость данных под действием случайных помех, сбоев и отказов. Методы защиты целостности, которые обеспечивают целостность данных от случайных помех, сбоев и отказов, не создают защиту от целенаправленных действий злоумышленников. При случайном нарушении целостности данных вышеуказанные методы только восстанавливают целостность, но не фиксируют случаи и способы попыток нарушения целостности данных. Для защищенных данных защита целостности должна предусматривать не только определенный уровень защиты, но и фиксировать следы нарушения защиты (попыток ее нарушения), а также обеспечивать дальнейшую защиту конфиденциальности данных.

На наш взгляд, необходимо классифицировать угрозы не для общедоступных данных, а для защищенных данных, так как защиту данных организовывают для закрытых данных, т. е. по определению защищаемых данных, например, даже обычное письмо помещают в конверт. В этой связи под целостностью необходимо рассматривать целостность защиты информации, а не самой информации.

Далее, необходимо отметить, что нарушение целостности защиты еще не является нарушением целостности информации, содержащейся в данных,

или конфиденциальности. Например, если к двум субъектам попадает конверт с данными (шифрами и кодами счетов в банке), то один из них может просто не понять, о чем эта информация, а другой может тут же пойти и нелегально снять деньги.

Существует много классификаций угроз безопасности информации и информационным системам.

По природе возникновения угрозы делят на: естественные, вызванные природными процессами, независящими от человека; искусственные, вызванные деятельностью человека, а последние разделяются на непреднамеренные и преднамеренные, при этом преднамеренные могут маскироваться под непреднамеренные и естественные. По месту положения угрозы делят на: внутренние; контрагентные, т. е. от того, кому предназначено сообщение; внешние, т. е. от элементов окружающей среды, у которых имеется возможность принять сообщение. По среде, в которой распространяется сообщение, угрозы делят на воздействующие на: передатчик, канал связи и приемник. По элементам среды угрозы делят на: действующие на аппаратные средства, программы и документы (базы данных). По элементам сообщения угрозы делят на действующие на носитель, данные, информацию. По степени влияния их делят на воздействующие на: инструкцию, информацию, мотивацию.

Далее рассмотрим, как извлекает субъект информацию из данных. Если исходить из того, что сведения (данные) необходимы лицу, принимающему решение, т. е. находящемуся в целеустремленном состоянии для принятия конкретного решения, а не ради самого процесса получения сведений (чтения ради чтения) или неопределенной цели познания действительности, то данное лицо может измерить (оценить) количество полученных сведений (информации) по их приросту (относительному или удельному) путем определения меры его приближения к определенной цели.

Наличие получаемых абсолютно истинных сведений, показывающих отклонение от цели, безукоризненных решений на основе этих сведений, безупречных исполнений привело бы данное лицо к цели за один цикл. Однако в реальной действительности такие условия не соблюдаются. Формулировка цели обладает ошибкой, измерение отклонения от цели осуществляется с погрешностью, решение и исполнение также грешат неточностью, изменяется среда, происходит самосовершенствование и старение лица, принимающего решения, и т. п., поэтому приходится многократно собирать сведения и принимать решения, что приводит к непрерывности данного процесса.

На наш взгляд, механизм извлечения информации из данных связан со свойствами окружающей нас Вселенной. Элемент универса Вселенной может отражать сам себя, т. е. свойства, объективно присущие ему, либо отражать свойства другого элемента данного универса или другого универса, т. е. отображенные свойства, неприсущие ему, либо отображать свойства, которые приписывает субъект, получающий данное отображение от этого элемента универса Вселенной.

Здесь под Вселенной понимается такое окружение (неопределенная совокупность элементов) элемента и универса, при котором изменения в последних в конечном счете не влияют на Вселенную, а под универсом понимается такое окружение (конечная совокупность элементов) элемента, при котором изменения в последнем приводят к изменениям в универсе данного элемента.

Данные утверждения необходимо дополнить тем, что окружение не входит в элемент или универс и изменения в окружении могут влиять на элемент или универс, при этом понятия элемента и универса относительны, так как элемент можно рассматривать как универс, а универс как элемент, чего нельзя сказать о Вселенной.

Если субъект или индивид, в том числе целеустремленный программно-аппаратный элемент, принадлежит универсу изучаемого элемента, то он может не только получить рассматриваемое отображение, но и понять (усреднить) его и, наконец, не только понять, но и использовать. Если же универс воспринимающего субъекта только пересекается с универсом рассматриваемого элемента, то субъект может принять отображение, но не понять его и не использовать. В этой ситуации отображенное свойство, например знак, будет восприниматься как символ, т. е. знак знака, значение которого неизвестно (например, нерасшифрованное сообщение).

Субъект, использующий информацию, сам отражается в рассматриваемом элементе универса и это отражение также отображается в виде приписываемых ему свойств, например, когда субъект назначает цену данному элементу на аукционе, то свойство цены элемента определяет прагматический смысл его отображения.

При этом, чем больше пересекаются универсы воспринимающего и рассматриваемого элементов, тем больше информации может извлечь субъект из воспринятого отображения (данных) и, наоборот, если эти универсы не пересекаются, то субъект вообще не извлечет информацию из данных.

На эту особенность обратил внимание Ю. А. Шрейдер [13], в частности количество информации, извлекаемой субъектом из данных, или количество семантической информации, извлекаемой субъектом из информации сообщения, можно измерить степенью изменения его тезауруса, т. е. структурированных знаний, представленных в виде понятий и отношений между ними. Для передачи информации тезаурусы должны пересекаться, если таковых нет, то субъекты, обменивающиеся данными, не смогут извлечь из них информацию, так как не поймут ее. Семантическая информация (содержащая сущность) есть продукт абстрактного мышления человека или обобщения (усреднения) чувственных данных, получаемых от датчиков целеустремленных искусственных систем, и отображает как элементы универса Вселенной, так и создаваемые ими (субъектами, индивидами) образы и модели.

Объем данных, отображающий какой-либо элемент универса Вселенной, зависит от точности чувствительных элементов воспринимающего индивида, в том числе используемых измерительных устройств. В [14] показано, что количество данных можно определить по формуле $J = X/\Delta X$, где X — измеряемая величина, ΔX — разрешающая способность измерителя.

В реальных условиях показано [14], что количество получаемых данных $J_k = R_k M_k$ меньше отражаемых элементом универса Вселенной — M_k за счет наличия информационной проницаемости

среды — R, которая характеризует условия отражения. Относительная информационная проницаемость среды определяется $R_k = \Delta y/\Delta X$, где Δy — минимальный диапазон существования материально-вещественного свойства.

Следующее за чувственным отражением логическое отражение позволяет понять полученные данные и выделить усредненные данные, т. е. формировать понятие на основе данных или логическую информацию, которая определяется как $H = R\Sigma\ (M_k/n) = R_{\text{ср}}M$, где n — число охватываемых понятием объектов, $R_{\text{ср}}$ — средняя характеристика относительной информационной проницаемости.

На основании логической информации формируются образы и понятия, где образ — индивидуализированное множество структурных свойств и связей между ними, на которые откликается субъект [15]. Например, усредненная информация о стадах одногорбых и двугорбых верблюдов дает абстрактного верблюда с нецелым количеством горбов, что не соответствует реальности, но дает образ всей популяции в целом. Понятие есть индивидуализированное множество функциональных свойств и связей между ними, на которые откликается субъект [15]. Мы можем не иметь образа Бога, но многие имеют понятие о Боге. В этой связи необходимо верифицировать логические данные, т е. проверять их на логическую непротиворечивость.

Наблюдаемая нами действительность не только объективна, но и субъективна, так как у нас нет 100% уверенности, что наши наблюдения не организованы другим субъектом. Поэтому $M_{\text{к}} = M_{\text{о}} + M_{\text{с}}$, а $J_{\text{к}} = J_{\text{о}} + J_{\text{с}}$, где $J_{\text{о}} = M_{\text{о}}R_{\text{о}}$ (объективные данные), $J_{\text{с}} = M_{\text{с}}R_{\text{с}}$ (субъективные данные), $R_{\text{о}} = \Delta y/\Delta x$, а $M_{\text{с}} = M_{\text{и}} + M_{\text{п}} + M_{\text{ох}}$. Обнаружение объекта при $R_{\text{с}} > R_{\text{ср}}$ может указывать на наличие $M_{\text{с}}$. Однако другой субъект может среди $M_{\text{к}}$ создавать условия, когда $R_{\text{с}} \approx R_{\text{ср}}$. Обнаружение охраны (защиты) $M_{\text{ох}}$ (в том числе функции самоуничтожения) будет однозначно свидетельствовать о наличии субъективной составляющей $M_{\text{с}}$. Снятие охраны и исправление искажений $M_{\text{и}}$, а также выявление подмены $M_{\text{п}}$ может позволить получить $J_{\text{с}}$ и даже значение (сущность) $J_{\text{с}}$, однако еще необходимо уяснить содержание (смысл) данного значения.

Если наблюдаемый элемент универса Вселенной представляет собой субъект, который противодействует воспринимающему субъекту, то данный элемент может стараться уменьшить информационную проницаемость среды, маскироваться (прятаться) в среде и тем самым ухудшать логическое понимание воспринимающего субъекта или имитировать какие-либо свои свойства, например, "чужой" может представиться "своим". Если воспринимающий субъект воспринимает такие данные как истинные, то он приписывает эти свойства к "своему" универсу. Степень адекватного (достоверного) восприятия, т. е. содержание (смысл) данных — С связаны с понятием данных — Н следующим соотношением С=КН, где К — степень адекватности содержания информации отражаемому элементу.

Отражение от противодействующего субъекта определяется как $I = \Sigma I_{\text{К}}$ или в предельном случае $I = \int_S O_{ds}$, где $O = dJ/ds$ — вектор плотности потока отражения снимаемой с отражающей поверхности S, замкнутой вокруг данного объекта [14]. Отсюда следует, что данный субъект адекватно отражается пространством и может быть полностью восстановлен по суммарному информационному потоку отражения сквозь произвольную поверхность, замкнутую вокруг некоторого материально-вещественного элемента отражения. Таким образом, если наблюдаемый субъект представляет ложное (мнимое) отражение несуществующего элемента или скрывает в "тумане" части существующего элемента, то он не может это сделать полностью. В этой ситуации наблюдатель может собрать полный поток отражения и выявить наличие неадекватности. Далее необходимо рассмотреть ценность информации или прагматическую информацию, так как от нее зависит, что необходимо защищать.

Данные в соответствии с [15] могут нести инструкции, информацию и мотивацию. Инструкции, если они предназначены для программно-аппаратных средств, представляют собой программу, назначение которой для целеустремленного индивида заключается в изменении объективных вероятностей достижения цели, т. е. в эффективности. Инструктировать — это значит наделять способностью управлять, когда она отсутствует. Мотивация предназначена для того, чтобы увеличить ценность результата для индивида либо выявить ее для него. В [15] под информацией понимается вероятность выбора индивидом каждого из доступных способов действия в целеустремленном состоянии, т. е. информация прямо связана с управлением и фактически оценивается мерой ценности. Полученное сообщение (данные) влекут изменение целеустремленного состояния получателя, при этом ценность данных определяется разностью ценности начального состояния и ценности измененного после управления конечного состояния индивида. В [15] ценность состояния индивида определяется функцией $V = \sum_{i=1}^{m}\sum_{j=1}^{n} P_i E_{ij} V_i$, где P_i — мера информации, E_{ij} — мера инструкции, V_i — мера мотивации. Ценность данных для отправителя, получателя и третьей стороны может отличаться. Например, обращение родителя к ребенку по поводу прекращения шума может увеличить ценность состояния родителя, но уменьшить ценность состояния ребенка.

Таким образом, "защита информации" должна осуществляться в виде защиты сведений, имеющихся в информации, инструкциях (программах, приложениях) и мотивации. Особенностью мотивации является то, что она может оказывать воздействие на субъекта на подсознательном уровне. Каждый вид данных сведений требует своего подхода к защите, например, программный продукт на лазерных дисках необходимо защищать от клонирования.

В литературе, посвященной защите информации, используются такие понятия, как "целостность", "сохранность" и "подлинность". Рассмотрим их более подробно. Если данные защищены, то несанкционированное ознакомление с ними приводит к нарушению целостности защиты, а стало быть, и к так называемой "утечке информации", при этом данные могут потерять свою конфиденциальность, а их значение отражается в мозгу субъекта, который несанкционированно с ними ознакомился. Если этот субъект смог не только озна-

комиться, но и скопировать эти данные на носитель, то такое действие можно квалифицировать как незаконное копирование (документирование); если этот субъект несанкционированно вмешивается в технологию создания, обработки данных, то такое действие можно квалифицировать как незаконное нарушение целостности данной технологии (процедуры), могущее привести к нарушению сохранности защищенных данных.

Целью незаконного (противоправного) "взлома" защиты данных является: корысть; получение преимуществ, например, политических, военных и т. п.; самоутверждение взломщика, который ограничивается только взломом и при этом не осуществляет ни ознакомление, ни копирование, ни какие-либо другие действия с данными, т. е. только нарушает целостность защиты, либо носителя, либо технологии.

Под сохранностью данных (документа) будем понимать не только сохранность защищенных данных, но и носителя этих данных и технологии их создания, обработки и т. п. Несанкционированное умышленное искажение защищенных данных или несанкционированное изъятие носителей этих данных, в том числе из легального оборота готовой продукции, полуфабрикатов и материалов, а также несанкционированное воздействие на технологию изготовления, конструкцию и материалы должно квалифицироваться как правонарушение. При этом "хищение информации" возможно только в виде хищения носителя информации.

Под искажением будем понимать скрытие, уничтожение, внесение или комбинации из этих действий, где скрытие (утаивание, блокировка) есть действия по уменьшению уровня восприятия данных, при этом информация не теряется, но ее невозможно воспринимать имеющимися средствами, например, залитая чернилами запись; уничтожение есть действия по полному устранению (стиранию) данных, приводящие к невозможности восстановления информации, а внесение есть действия по нанесению данных на поверхность носителя или в его тело или процесс, в том числе и распространяющийся в виде волн в полевой среде.

Под нарушением подлинности защищенных данных будем понимать несанкционированную умышленную подмену носителя данных, самих данных с помощью незаконной (нелегальной) технологии их изготовления.

Скрытие (затуманивание) — операция, позволяющая затруднить обнаружение объекта, которую можно разделить на три вида: маскировка — снабжение объекта свойствами, похожими на свойства окружающей среды (фона); уменьшение размеров объекта до размеров, позволяющих их спрятать (уменьшение Δx — порога восприятия); прикрытие — экранирование объекта каким-либо образом, например, непроницаемым экраном, который делает его невидимым (уменьшает информационную проницаемость среды до нуля).

При подмене используют имитацию (миражирование, дезинформирование) — операцию, позволяющую осуществить подмену истинной информации на ложную, которую можно разделить на три вида: фоновая дезинформация, при которой ложная информация создается с ложным фоном, чтобы затруднить выявление ложного; достоверная дезинформация — подразумевает представление истинной информации за исключением защищаемой истинной информативной ее части; правдоподобная дезинформация, представляющая собой истинную информацию, но уводящая в сторону от истинных целей.

Для имитации или распознавания имитации используют информационную модель. Информационная модель — совокупность элементов, связей и отношений между ними, отображающая свойства носителя, значение (сущность) и содержание (смысл) сообщения.

В случае, когда данные представлены в виде сигналов, при скрытии данных используют некоторые свойства этих сигналов, в частности, для видимой части спектра для сигналов существуют две характеристики: яркость, которая определяется отношением уровня сигнала к уровню помехи, и контрастность, которая определяется уровнем сигнала к уровню фона.

Элемент может скрываться либо в помехах, либо в фоне среды, либо с помощью определенного скрывающего средства (свойства — $X_а$), делающего его невидимым в среде. Последнее скрытие возможно выявить по другому свойству — $X_в$. Однако бывают ситуации, когда $X_в$ недостаточно для выявления X, тогда пытаются выявить еще одно свойство $X_с$. Обычно данные свойства называют необходимыми и достаточными свойствами (свойство объекта — как минимальной совокупности из двух свойств), а также используют еще одно свойство — связности — X_D. Как правило, если данные свойства являются информативными, то их бывает достаточно для выявления скрытого элемента.

Для случая фальсификации полиграфической продукции под фальсификацией полиграфической продукции можно понимать преднамеренное (сознательное, умышленное) нарушение целостности (несанкционированное ознакомление с конфиденциальными или иными защищаемыми данными); сохранности (искажение данных, в том числе носителя данных, в частности, несанкционированное изъятие из легального оборота излишков готовой продукции (полуфабрикатов), материалов путем несанкционированного воздействия на технологию изготовления, конструкцию и материалы полиграфической продукции; подлинности, т. е. осуществление подмены (нелегальное, нелегитимное), изготовление полиграфической продукции с корыстной (коммерческой, преступной) целью на всех этапах ее жизненного цикла (использование, разработка, производство, изготовление, переработка, хранение, транспортировка (перевозка, пересылка, ввоз, вывоз), обработка, отпуск, реализация, сбыт, распространение, предложение, утилизация, уничтожение, архивирование и т. п.). В данной ситуации незаконное изъятие полиграфической продукции не является только хищением, так как изымаются излишки неучтенной продукции, которые образовались за счет фальсификации с элементами материалов, конструкции и технологии изготовления.

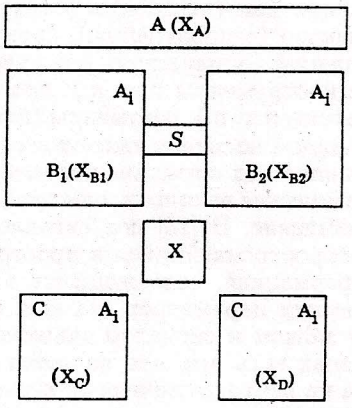
Обычно под формами защиты информации понимают уровень сложности и доступности идентификации наличия защиты, при этом выделяют три формы: 1) объявленные защиты, 2) сертифицированные защиты, 3) скрытые защиты. В соответствии с [4] сертифицированные средства защиты представляют собой комплекс технических мер от фальсификации, применение которых известно только участникам контролируемого окружения обращения полиграфической продукции. Наличие и описание таких защитных мер, равно как

и метод их идентификации, описываются в сертификате или декларации защищенности.

В связи с тем, что заказчик защиты информации не всегда обладает достаточной квалификацией для проверки качества защиты, необходима сертификация защиты третьими лицами, например, органами по сертификации защиты данных (информации). Кроме того, среди участников, имеющих отношение к защите данных, можно выделить экспертов-криминалистов, которые осуществляют экспертное исследование документов, в том числе и защищенной полиграфической продукции.

Окружения, в которых распространяются отображения, документы, данные обычно делят на неконтролируемое, контролируемое и профессиональное окружения, где профессиональное окружение подразумевает окружение, в котором со 100% гарантией будет выявлено нарушение защиты данных, контролируемое окружение подразумевает наличие в нем подготовленных субъектов и условий, позволяющих тестировать защищенные данные, неконтролируемое окружение подразумевает субъектов, практически не имеющих опыта по обнаружению нарушения защиты данных. Последним обстоятельством широко пользуются злоумышленники.

Рассмотрим модель косвенного общения в неконтролируемом окружении при отсутствии взаимного доверия сторон (рисунок).



A — производитель аппаратуры, программ, баз данных, услуг связи, защиты и т. п.; A_i — аппаратура, программы, базы данных, процессы услуг, защиты и т. п.; B_1 — отправитель сообщения (данных); B_2 — получатель сообщения (данных); C — доверенное лицо (сертификационный центр, нотариус); D — арбитр, привлекающий экспертов; X — злоумышленник; X_{A_i}, X_{B1}, X_{B2}, X_C, X_D — злоупотребители; S — сообщение (данные)

В данной структуре возможны следующие способы нарушения целостности, сохранности и подлинности защищенных данных:

1) X получает доступ к S, нарушает целостность защиты K, искажает S или (и) подменяет (имитирует) S и отправляет B_2 от имени B_1. При этом ему могут помогать X_{B1} и X_{B2} или они сами могут выступать в роли X;

2) B_1 выступает в роли X_{B1} и отправляет искаженное S в B_2, при этом заявляя, что данное сообщение не отправлялось или отказывается от авторства S, т. е. заведомо искажает или подменяет (имитирует) S;

3) B_2 выступает в роли X_{B2} при получении S от B_1, заявляя, что данное S не получал или получил, но искаженное S, т. е. подменяет (имитирует) отсутствие S либо намеренно искажает полученное S;

4) X получает доступ к S, нарушает целостность защиты K, копирует K и S, при этом он может восстановить целостность K или маскировать (имитировать) нарушение целостности за счет воздействия естественной природы;

5) X получает доступ к A_i и организовывает непрерывную посылку S от имени B_1 и B_2 и наоборот, тем самым имитируя непрерывный сбой, что приводит к отказу A_i выполнять истинные задания.

В задачи доверенной стороны — C входит предоставление официальной информации о состоянии средств и методов, используемых в информационной среде, чтобы в случае спора между B_1 и B_2 относительно целостности, сохранности и подлинности сообщения представить необходимые документы в арбитраж. Задача арбитра — D заключается в разрешении спора между B_1 и B_2 с возможностью привлечения эксперта. В этой связи большое значение приобретают такие понятия, как идентификация и аутентификация. Аутентификация есть проверка принадлежности субъекту предъявленного им идентификатора. Идентификация есть присвоение (наложение) средств идентификации (идентификатора) элементу (объекту, субъекту и т. п.) и проверка идентификатора по списку присвоенных идентификаторов. Идентификатор — некоторые уникальные данные, позволяющие различать индивидуальные элементы (пользователей, объекты и т. п.) в системе идентификации. Кроме того, в системах идентификации используют пароли. Пароль — некоторые секретные данные, известные только элементу парольной системы и самой парольной системе и позволяющие парольной системе осуществлять идентификацию и аутентификацию элементов, предъявляющих идентификатор и пароль. Для аутентификации субъектов еще применяют индивидуальные биометрические характеристики, например, рисунок папиллярного узора пальца. В современных системах защиты используются трехфакторные защиты, состоящие из электронного ключа — идентификатора, пароля и криптографического файл-ключа. Если же субъект после идентификации должен получить доступ к осуществлению некоторых действий с программно-аппаратным средством, то запрос на такие действия и проверка субъекта (разрешение) еще называется авторизацией.

В последнее время для защиты данных широко используется электронная цифровая подпись. Электронная подпись выполняет три основные функции: обеспечивает путем шифрования защиту от нарушения целостности, сохранности и подлинности данных [16]. Она является гарантом, что данные не будут подвергнуты изменениям за счет естественных воздействий, а также искажениям злоумышленниками, и, наконец, гарантирует юридическое авторство документа. Цифровая подпись представляет собой функцию от содержания документа и секретного ключа, при этом цифровая подпись может передаваться отдельно от документа. Как правило, цифровой ключ формируется из двух частей: секретного ключа и известного всем абонентам проверочного (открытого) ключа. Любой получатель, имеющий проверочный ключ, может аутентифицировать сообщение по цифровой подписи. Общедоступные контрольные ключи (комбинации) должны быть удостоверены доверенным лицом, чтобы потом контрагенты не могли от них отказаться.

Кроме криптографии для наиболее важных данных используется стеганография, которую стали применять даже ранее криптографии. Способы скрытия либо факта наличия данных, либо истинного смысла в этих данных называют стеганографией (тайнописью), например, запись невидимыми чернилами либо встраивание секретных данных в нейтральное сообщение. При криптографии смысл данных неизвестен, но известен либо факт наличия, либо само шифрованное сообщение.

Обычно используют следующие виды взлома защит [17], которые мы рассмотрим на примере лазерных дисков: "кряк", с помощью которого в код защищенной программы вносятся изменения, т. е. нарушается подлинность; эмуляция, с помощью которой удается имитировать защиту, т. е. нарушается подлинность; клонирование, с помощью которого удается нарушать целостность защиты данных.

Защита лазерных дисков базируется на установке: 1) некоторой метки на носителе, которая не копируется или не эмулируется (воспроизводится) программными средствами; 2) некоторой программы в защищаемую программу, которая проверяет наличие некоторой метки; 3) в некоторой виртуальной среде — Интернете — некоторых узлов продуцента — серверов, с помощью которых легальный пользователь регулярно расширяет возможности продукта и получает сервис.

Если рассматривать в качестве носителя лазерный диск, то каждый диск можно снабдить уникальной физической меткой, которая его идентифицирует, однако в неконтролируемом окружении с помощью клонирования данная защита обходится. Клонирование — копирование защищенных данных, включающих программы, в результате которого получается копия программы, которую можно исполнить на аппаратных средствах. Поэтому на лазерный диск наносится лазерная метка, несущая данные об уникальных характеристиках, присущих только конкретному носителю. Данная метка не копируется, а поэтому диск не клонируется. Ее можно только эмулировать, но для этого необходимо научиться определять физические характеристики каждого конкретного диска, а это аналоговые данные, которые трудновоспроизводимы.

Программная часть защиты, как правило, это резидентная программная часть, способна идентифицировать метку на носителе или характеристику носителя, с которого она была запущена. Обычно программная защита защищает саму себя и защищаемую программу. При этом данная защита должна позволять разработчикам защищаемой программы встраивать защиту в тело программы. Наиболее перспективным способом защиты является написание данных программ на специальных уникальных языках, вспомним клинопись, которая была расшифрована только с появлением глиняного фрагмента на трех языках. Все эти мероприятия противодействуют хакеру, который стремится полностью удалить защитный модуль либо создать эмулятор, который обманет защиту. Здесь мы не рассматриваем случая, когда хакеры получают незаконно доступ: либо к ключу защиты, либо к незащищенной программе, которая затем была защищена.

Далее отметим, что необходимо различать источник и носитель информации. Некоторые сведения, нанесенные на лист бумаги (документ), представляют собой источник информации, а бумага — носитель. Однако, если бумага обладает определенными свойствами, например, водяным знаком, то она в этом случае также является источником информации.

Поэтому обычная копия документа является носителем информации, но лишена свойства источника информации, а клон лазерного диска с программным продуктом является источником информации, в смысле инструкции, и позволяет запускать программу с контрафактного диска.

К свойствам носителя относят основные свойства элемента универса Вселенной: вещественные свойства (свойства веществ, из которых сделан носитель — вещь), материальные свойства (свойства процессов и полей, с помощью которых существует носитель) и свойства отношений, например, элементные (видовые) свойства, с помощью которых можно выделить элемент среди других, например, форма. Данные свойства носителя еще называют демаскирующими признаками, в которые входят внешний вид, излучаемые им поля, внутренняя структура и химический состав, содержащихся в нем веществ [18].

Среди вещественных носителей выделяют локальные носители, например, компьютер; отчуждаемые носители, например, дискета; распределенные носители, например, провода линии связи. Обычно выделяют субъективные и объективные носители данных. К субъективным относят человека, а к объективным — вещи, процессы взаимодействия.

Среди источников данных как объектов защиты выделяют субъективные (человек) и объективные: материалы, энергию (сопродуценты); продукты и отходы; продуценты (аппаратура (оборудование, измерительные инструменты и т. п.), программы (алгоритмы, методы и т. п.), документы (данные)).

Отдельным видом носителя являются сигналы. В радиоэлектронике под сигналом понимается изменяющаяся физическая величина, однозначно отображающая сообщение. В [18] под сигналом подразумевают распространяющийся в пространстве носитель с информацией, содержащейся в значениях его физических параметров. На наш взгляд, разница между знаком и сигналом заключается в том, что если знак есть все, что является продуцентом отклика на нечто, отличное от него самого (вещь или ее свойство, связь между вещами или ее свойство), то сигнал есть такой знак, который отображается не вещным носителем, а материальным носителем, не имеющим вещной формы.

В [4] выделяются два основных метода подделки полиграфической продукции: 1) аналоговая, 2) "цифровая" фальсификации. Аналоговая фальсификация построена на непрерывном способе представления объектов и подделка осуществляется теми же методами, что и производство оригинала, или технологией, максимально приближенной к оригинальной, т. е. используется аналогичный метод. При цифровой фальсификации, как правило, используются методы цифрового (компьютерного) репродуцирования, в основе которых лежит способ дискретного представления объекта. Современные информационные технологии, применяемые совместно с настольными издательскими системами ДТР, позволяют осуществлять правдоподобные фальсификации защищенных документов не только на уровне полиграфии, но и на уровне постпечатных защитных технологий.

В заключение, необходимо остановиться на вопросе о возможности "идеальной" фальсификации данных. В [19] отмечено, что для аналогового метода фальсификации принципиально невозможно

создать идеальную фальшивку в силу непрерывного способа представления объектов, в котором используется практически бесконечное количество элементов объекта. С цифровым представлением объектов дело обстоит значительно сложнее. Если оригинальные данные были созданы в цифровом виде, то принципиально возможно создать идеальную, т. е. точную цифровую копию данного объекта.

Особенностью цифрового документа является принципиальная возможность создания тождественного цифрового документа, который ничем не будет отличаться, кроме естественного времени его производства, при этом цифровой (электронный) документ уже не имеет фиксированного места, а представляет собой некоторый дискретный, но процесс [19].

Исходя из того, что любая защита принципиально преодолеваема, наиболее важные защиты организуют в виде нескольких рубежей, а саму защищаемую информацию обеспечивают системой экстренного уничтожения или подмены на ложную в случае преодоления злоумышленником последнего рубежа. Поэтому можно считать, что существуют практически непреодолимые защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Нестеров А. В. Некоторые соображения по поводу "Доктрины информационной безопасности РФ" // НТИ. Сер. 1 .— 2001 .— № 4 .— С. 1–5.
2. Положение о лицензировании деятельности по изготовлению защищенной от подделок полиграфической продукции // Постановление Правительства РФ от 11.11.2002 № 817.
3. Федеральный закон РФ "О лицензировании отдельных видов деятельности", № 128-ФЗ от 08.08.2001.
4. Коншин А. А. Защита полиграфической продукции от фальсификации.— М.: Синус, 2000 .— 157 с.
5. Снытников А. А. Лицензирование и сертификация в области защиты информации.— М.: Гелиос АРВ, 2003 .— 192 с.
6. ГОСТ Р 50922-96. Защита информации.
7. Федеральный закон РФ "Об информации, информатизации и защите информации".
8. Система обнаружения подделки документов // Патент 5432506 США, 1995.
9. ГОСТ Р 51141-98. Делопроизводство и архивное дело. Термины и определения.
10. Девянин П. Н. и др. Теоретические основы компьютерной безопасности.— М.: Радио и связь, 2000 .— 192 с.
11. Защита от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России // www.rnt.ru.
12. Нестеров А. В. Компьютерные методы и средства глубокой обработки, анализа и синтеза общедоступных документов.— Новосибирск, 1991 .— 214 с.
13. Шрейдер Ю. А. О семантических аспектах теории информации // Информация и кибернетика.— М.: Сов. радио, 1967.
14. Денисов А. А. Введение в информационный анализ систем.— Л.: ЛПИ, 1988 .— 52 с.
15. Акофф Р., Эмери Ф. О целеустремленных системах.— М.: Сов. радио, 1974 .— 272 с.
16. Федеральный закон РФ "Об электронной цифровой подписи".
17. Новичков А. Анализ рынка средств защиты программного обеспечения от несанкционированного копирования // www.wall.tms.ru.
18. Торокин А. А. Основы инженерно-технической защиты информации.— М.: Ось 89, 1998 .— 336 с.
19. Конявский В. А., Гадасин В. А. Системное отличие традиционного и электронного документа // www.accord.ru.

Материал поступил в редакцию 23.12.03.

УДК 001.5:001.891.57

Ю. В. Нефедов

О подходе к схематическому моделированию развития научной мысли

Лавинообразный рост научных знаний во всех сферах диктует необходимость разработки общепринятых подходов для представления развития научной мысли наглядно и в динамике. Рассматривается ряд подходов, применяемых в информационном моделировании и управлении для решения смежных задач. С их учетом предлагается новый подход, основанный на противоречии как исходном элементе причинно-следственной связи, приводящей к появлению новых знаний. Получаемые схемы просты, наглядны и могут быть интерактивными, в том числе с помощью гипертекстовых технологий. Вместе с тем, подход требует многочисленных экспериментов по применению.

Продолжающийся уже почти полвека взрывообразный рост научных знаний ставит все новые задачи перед исследователями. В 1970–1980 гг. существенной проблемой был поиск необходимой публикации. Так, в середине 1970-х гг. даже возник парадокс: некоторые химические соединения быстрее было синтезировать заново, чем найти статью, где синтез уже описан. Появление глобальных компьютерных сетей, поисковых систем и баз данных в 1990-е гг. в целом разрешили проблему поиска, но на смену ей пришла новая проблема: "пропускной способности" исследователей. Ясно, что количество публикаций, которые исследователь может прочитать и осмыслить в единицу