2. *Афанасьєва О.Ю., Дурняк Б.В.* Дослідження семантичних параметрів, що використовуються в графіці // Зб. наук. праць. ІПМЕ НАН України, N3, 2007.
3. Такеути Г. Теория доказательств. - М.: Мир, 1978.
4. *Борсуков В.С.* Стеганографические технологии защиты документов, авторских прав и информации // Обзор специальной техники. N 2, -2000.
5. *Акимов О.Е.* дискретная математика: логика, группы, графы, фракталы. - М.: Издатель АКИМОВА, 2005.
6. *Капітонова Ю.В., Кривий С.Л., Летичевский О.А., Луцький Г.М., Печурин М.К.* Основи дискретної математики. - Київ: Наукова думка, 2002.
7. *Стрижалюк Т.Г., Коновалова Н.Р.* Диференціальні рівняння. - Київ: Світ, 1997.

Поступила 11.02.2010р.

УДК 683.05

Б.Дурняк, К.Павелек

ОРГАНИЗАЦИЯ И ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ, ДЛЯ ФОРМИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ И ИССЛЕДОВАНИЕ ОТДЕЛЬНЫХ АСПЕКТОВ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ

Информационая технология, использующая семантику информационных компонент, позволяет создавать достаточно гибкие системы защиты авторских прав благодаря следующим факторам:

- семантика естественного языка, который используется, для описания информационных компонент системы, позволяет достаточно легко согласовывать информационные потоки между отдельными носителями системы защиты, например, между системой связанной с введением, считыванием и интерпретацией *CWZ* с подсистемой реализующей процедуры реагирования,
- поскольку в рамках системы *SZ* неизбежно участие социальных подсистем, то не требуется преобразования интерпретации выходных данных компьютерных подсистем и входных данных социальных подсистем, что не требует адаптации последней к используемой информационной технологии,
- поскольку продуктами интеллектуальной собственности, которые представлены в цифровой форме, могут быть не только продукты касающиеся информационных технологий, но и касающиеся художественных произведений, то использование текстовых представлений информационных компонент, позволяет достаточно легко отображать все аспекты функционирования *SZ* в форме доступной любому учаснику процесса защиты авторских прав, включая распространителей цифровых продуктов интеллектуальной деятельности,

- в процессе функционирования SZ может возникать необходимость во введении дополнительной информации, которая непосредственно связана с процессом функционирования SZ, как правило, такая дополнительная информация в своем исходном виде представлена на естественном языке, тогда, для ее ввода в SZ, достаточно только нормализовать форму представления этой информации, что не предполагает изменения ее интерпретации,
- семантические параметры, которые вводятся и используются в системе SZ, сформированы таким образом, чтобы они в минимальной степени зависили от предметной интерпретации, которую соответствующие информационные компоненты описывают, что позволяет минимизировать влияние субъективных факторов на процессы формирования и модификации новых информационных компонент, которые характерны для систем оперирующих с объектами, для описания которых используются естественные языки пользователей соответствующей системы.

Рассмотрим методы формирования системы защиты SZ из компонент информационной технологии, которая описывается в работе. Для примера выберем наиболее распространенную цель защиты, которая, в тоже время, является наиболее полной с точки зрения необходимости использования максимального количества подсистем и преобразований в процедуре противодействия фактам нарушения авторских прав. Такую цель составляет следующая совокупность требований:

- выявление производителя несанкционированых цифровых продуктов,
- выявление объемов изготовленных не авторских экземпляров цифровой продукции,
- определение вличины потерь собственника авторской продукции в результате распространение нелегальных экземпляров,
- компенсация потерь автору, которые он понес вследствии распространения нелегальных экземпляров,
- предотвращение возможности дальнейших подделок, продукции, которая принадлежит владельцу, обратившемуся за услугой по защите авторских прав, которое характеризуется определенными параметрами, например, объемами подделки, интервалом времени, в течении которого такая подделка продукции не будет осуществляться и т. д.

Выполнение условий, которые описывают цель функционирования системы защиты и приведены выше, требуют максимального количества функциональных преобразований и участия в SZ всех основных подсистем, включая и социальные подсистемы. Рассмотрим на качественном уровне способы обеспечения всех требований, сформулированных в цели функционирования SZ.

Прежде всего отметим, что процесс функционирования SZ инициируется только в том случае, когда появляется заказ на предоставление

услуг по защите авторских прав на определенный продукт интелектуальной деятельности. В состав формируемой системы SZ входит часть подсистем и блоков, которые используются всегда, независимо от конфигурации системы защиты, к ним относятся:

- подсистема мониторинга рынка распространения нелегальной цифровой продукции,
- система идентификации нелегального продукта, которая функционирует в основном на основе используемой информации, размещаемой в форме CWZ,
- минимальная версия подсистемы реагирования на нарушение авторских прав.

Подсистема мониторинга распространения цифровой продукции является достаточно сложной и включает в себя подсистемы социального характера. Необходимость использования социальных подсистем обусловлена тем, что права на проведение контролирующих операций регулируются юридическими нормами, которые предписывают такие права. В рамках подсистемы мониторинга решается целый ряд специфических задач, которые характерны исключительно для системы мониторинга. К таким задачам относятся:

- задачи формирования траектории мониторинга, поскольку рынки распространения цифровых продуктов распределены в пространстве,
- задачи формирования графика проведения мониторинга, если необходимо выявить весь объем нелегальной продукции и предотвратить возможность изготовления нелегальной продукции на заданный период времени,
- задачи определения величины интервалов времени, которые могут быть затрачены на отдельный шаг проверки и выявления нелегальной продукции, поскольку, в противном случае один цикл мониторинга может растянуться на неопределенный период,
- задачи оценки эффективности мониторинга, поскольку основной процедурой контроля является выявление нелегальной продукции, которая является подделкой по отношению к легальной продукции, а качество подделки может иметь различный уровень, что влияет на используемые методы выявления подделаных продуктов,
- задачи формирования стратегий проведения мониторинга рынка распространения и выявления нелегальной продукции, основной целью которой является выявление новых методов идентификации продуктов, анализ юридических особенностей, которые регламентируют процессы и методы выявления нелегальных продуктов, целью стратегии осуществления мониторинга также является решение задач прогнозирования осуществления подделок различных видов продуктов, представленных в цифровой форме и т. д.

Исходя из выше перечисленных задач подсистемы мониторинга можно

заключить , что эта подсистема, сама по себе является достаточно сложной и затратной. Поэтому подсистемы мониторинга не должны представлять собой узкоспециализированные структуры, которые ориентированы на осуществление мониторинга только одного вида продукции. Это означает, что системы защиты авторских прав на цифровые продукты могут пользоватся системами мониторинга, которые уже существуют и используются для контроля рынка других продуктов. В этом случае системы SZ должны только расширять возможности универсальных подсистем мониторинга специфическими процессами идентификации цифровых продуктов, основывающимися на использовании цифровых водяных знаков. Принимая во внимание изложенное выше, в данной работе не исследуются принципы организации систем мониторинга рынка распространения CP. В качестве следующей подсистемы, которая тоже является одной из ключевых, следует отнести систему идентификации CP на предмет ее происхождения. Решение этой задачи в общем случае, является достаточно проблематичным, поскольку ее решение зависит от целого ряда факторов:

- от информации, которая размещается в CWZ и составляют суть соответствующего сообщения,
- от способов подделки оригинального CP, который используется несанкционированным изготовителей нелегальных екземпляров CP,
- от секретных параметров CWZ и в целом параметров носителя, как физического объекта, которые используются, при расширении CWZ и являются ключевыми, параметрами противодействующими попыткам подделки оригинального CP,
- от структуры средств защиты, которые представляют собой текстовое сообщение, ряд дополнительных информационных кодов, которые включаются в состав CWZ и имеют специфическую интерпретацию, что позволяет усложнить возможные процессы подделки оригинального CP и т.д.

В соответствии с решением задачи защиты легального CP средствами, которые основываются на использовании CWZ, средствами подсистемы идентификации решается задача распознования поддельного CP. Исходя из приведенных выше примеров, возможные факторы, которые влияют на способ решения задачи формирования CWZ и защиты авторских экземпляров цифровых продуктов, и принимая во внимание, что в каждом отдельном случае, авторы средств защиты могут разработать новые способы их использования в рамках идеологии CWZ, то становится совершенно очевидным, что задачи создания подсистемы идентификации представляют собой отдельную проблему, решение которой требует специальных исследований. Тем не менее текстовая составляющая CWZ, при любых способах реализации защиты CP, всегда будет существовать в силу следующих обстоятельств:

- в сообщении, которое размещается в CP в виде CWZ, должна размещаться информация, которая, при несанкционированном выявлении CWZ, будет информировать всех учасников, связанных с использованием CP и CWZ, о факте защиты продукта с указанием данных, которые позволяют верифицировать факт реализации санкционированной защиты, поскольку, последняя может быть фальсифицирована, с целью усложнения процесса распознования подделки,
- не вся часть сообщения может составлять тайну используемых методов защиты от подделок, часть информации сообщения M_i из CWZ будет, в рамках CWZ, открыто использоваться системой защиты SZ и, поэтому, такая часть M_i должна, в соответствии с принятым подходом, записываться в виде текста на выбранном естественном языке,
- методы защиты CP на основе использования CWZ могут не предполагать использования автоматизированной защиты, основывающейся на соответствующей информационной технологии, такие методы могут реализоваться, в простейшем случае, отдельными специалистами, которые могут иметь юридические полномочия, для решения вопросов защиты, которые таких полномочий требуют, необходимость обеспечения такой возможности обуславливается тем, что услуги по защите CP предоставляются на комерческой основе и потенциальный пользователь должен иметь возможность выбора альтернативных методов решения задачи защиты, даже если они основываются на использовании CWZ, в этом случае сообщение размещаемое в CWZ должно полностью формироваться в виде текста на естественном языке потенциальных пользователей,
- если в защищаемом CP используются хотябы фрагменты, которые отображаются на естественном языке, то методы защиты CP можно строить таким образом, что информация, размещаемая в сообщении M_i, будет связана с текстовыми фрагментами самого CP, в этом случае, использование естественного языка, для отображения сообщений, которые размещаются в CWZ, являются неизбежными.

Можно было бы привести достаточно много факторов, которые продемонстрировали бы необходимость использования естественного языка, для отображения сообщения, размещаемого в CWZ, но достаточно отметить тот факт, что во всех открытых информационных системах, особенно в тех, которые ориентированы на участие в их в работе специалистов, одной из ключевых задач, которые решаются в таких системах, является задача создания интерфейсов, ориентированных на обеспечение связи системы с пользователем с использованием естественного языка пользователя в наиболее благоприятный для него форме [1,2].

Следующей подсистемой является подсистема, в рамках которой осуществляется следующие функциональные преобразования:

- семантический анализ типа или способа подделки CP, что можна

рассматривать как анализ типа атаки на защищаемый CP,

- анализ данных CWZ с целью выбора или формирования процедуры реагирования на нарушение авторских прав,
- анализ результатов осуществления операций реагирования и формирование оснований, для выбора методов модификации сообщения в CWZ.

Ключевой функцией подсистемы реагирования и противодействия нарушению авторских прав является анализ сообщения CWZ с целью выбора процедуры анализа, реагирования и противодействия нарушению, которая сокращенно была обозначена ARN. Примем, что цель защиты некоторого CP содержит следующие требования:

- обнаружение производителя нелегальной продукции и объемов ее нелегального производства,
- обеспечение компенсации потерь автора из-за несанкционированного распространения подделаных продуктов,
- обеспечение пресечения возможности несанкционированного распространения нелегальной CP.

Очевидно, что размещать в M_i, которое размещается в CWZ полное описание всех требований не имеет смысла. Поскольку, в SZ предпологается использование нормализованых фраз на естественном языке, а в словаре S_c содержится описание интерпретационного расширение отдельных слов и используемых фраз, которые характерны для предметной области SZ, то в качестве примера M_i в части описания цели, фрагмент M_i из CWZ можно привестиследующую текстовую информацию:

< ОБНАРУЖЕНИЕ ПРОИЗВОДИТЕЛЯ, КОМПЕНСАЦИЯ ПОТЕРЬ, ПРЕСЕЧЕНИЕ ДАЛЬНЕЙШИХ ПОДДЕЛОК.

Кроме текстового описания защиты цели защиты, в CWZ размещаются атрибуты, которые позволяют решать задачу идентификации нелегального производителя поддельных CP. Прежде чем описывать решение этой задачи отметим, что использование системы защиты в рамках данного подхода предполагает более широкое представление о участках процесса защиты, к которым, традиционно относят некоторую систему защиты, готовый продукт потребителя услуги по защите авторских прав. Прежде всего, в рамках данного подхода учасником мероприятий по защите авторских прав является производитель промышленного тиража цифровых продуктов. Это означает, что соблюдаются следующие условия, связанные с функционированием SZ:

- автор или владелец авторских прав защищает не продукт, который является промышленным товаром, а продукт интелектуальной деятельности, который подготовлен для дальнейшего промышленного производства (в случае использования носителей CD, соответствующий продукт может представлять собой информационную систему записанную в ограниченом

количестве экземпляров в электронную память или на цифровой носитель информации),

- вопросы связанные с промышленным изготовлением той или иной партии продуктов, за исключением финансовых вопросов, решаются совместно системой защиты в лице социальной структуры, которая использует соответствующую информационную технологию, и производителем промышленной партии соответствующего продукта,

- промышленный производитель, который производит соответствующую продукцию, обязан, независимо от заказчика соответствующего продукта, получать от системы защиты сертификат на производство *CP* ,этот сертификат определяет способ идентификации каждого изготовленого товара без специального обращения к *SZ* перед началом производства заказанного типа цифрового продукта произвольным заказчиком.

Таким образом, задача идентификации производителя любого цифрового продукта становится тривиальной. Каждый автор, который обращается за услугой по защите авторских прав, получает из *SZ* персональный тайный ключ, который присваивается системой и остается в *SZ* , а, для идентификаций соответствующего продукта, автор получает открытый ключ, который предъявляется изготовителю. Изготовитель на основе сертификата генерирует уникальный номер, шифрует его открытым ключом и вводит в состав сообщения *CWZ* . Сертификат, который получает для производства цифровой продукции изготовитель, реализован в виде, который похволяет реализовать алгоритм формирования уникального номера продукта. Этот алгоритм может основываться на принципах формирования цифровой подписи фрагмента защищаемого продукта, в котором предполагается размещать соответствующий *CWZ* . Использование цифровой подписи [3,4] позволяет воспользоваться юридическими нормами, которые последнюю определяют, как форму подписи, которая имеет юридическую силу традиционных способов идентификации документов, например, личной подписи автора документа, с исползованием зарегистрированной печати и т.д. Сертификат легального призводства *CP* , который получает от *SZ* производитель, расчитан на определенное количество тиражей или партий продукции. В случае исчерпания соответствующего количества тиражей, полномочие сертификата истекает и производитель должен обращаться в *SZ* для получения нового сертификата.

При формировании уникального номера издания *CP* , кроме выбора фрагмента *CP* , в котором предполагается размещать соответствующий экземпляр *CWZ* , используются и другие параметры изделия, которые в силу своей физической природы могут являться в определенной мере уникальными [5], например, характеризовать сам носитель информации.

В рамках разработанного подхода, тесная связь между производителем CP и системой SZ не должна приводить к тому, что автор, желающий издать свой CP и не требующий услуг по защите авторских прав, не мог бы оставаться анонимным по отношению к SZ. В этом случае, при изготовлении партии или тиража CP, заказанного автором, в среде CP не формируется CWZ, а открытым способом в технологически определенных местах носителя CP размещаются данные о сертификате на право выполнения работ по изданию CP и информация о его полномочиях.

Как следует из изложенные выше, предложенные методы защиты являются, по своей природе, пассивными. Алгоритмы анализа цифровых продуктов позволяют идентифицировать авторские издания. Если CP не идентифицирован, как авторский продукт, то соответствующий продукт определяется, как поддельный. Если он произведен на сертифицированом производстве, то задача выявления нелегального заказчика соответствующего продукта переходит в правовую сферу, поскольку, каждый легальный производитель, в этом случае обязан передавать все сведения о заказчике в SZ.

Проблема идентификации подделаного продукта с его оригиналом в рамках данного исследования не рассматривается в целом и решается только на уровне анализа комплекта CWZ, которые размещаются в различных фрагментах защищаемого продукта. Для реализации всех $P_i(x_i m_i)$, которые включены в PR_i, в CWZ включаются и другие данные, например,размеры тиража, дата изготовления и т.д. Если в рамках SZ реализация процессов защиты приводит к появлению противоречивости, тогда средства SZ эту противоречивость переводят в ранг сбалансированной противоречивости. Примером такого противоречия может быть ситуация, когда авторские права на данное изделие в той или иной форме были переданы другому лицу и, таким образом, возникло два претендента на авторские права по отношению к одному CP и т. д.

1. *Гринченко Т.О., Стогний А.О.* Машинный интеллект и новые информационные технологии. - Киев: Манускрипт, 1993, -164с.

2. *Девятков В.В*. системы искуственного интелекта - М.: МГТУ им. Н.Э.Баумана, 2001.-352с.

3. *Pierryk J.,Hardjono T., Seberry J.* Teoria berpiecrenstwa systemow Komputerowych Gliwice, HELION, 2003,-595s.

4. *Stallings W.* Ochrona danch w sieci i intersieci w teorii i praktyct. Warsrawa, WNT, 1997, -473s.

5. *Sklyarov D.* Lamanie zabezpieczen programow. Warsrawa, RM, 2004, -210s.

Поступила 15.02.2010р.