УДК 004.056.53:347.211

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФАКТОР ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В КИБЕРПРОСТРАНСТВЕ

В.М.Левыкин, Т.В. Гавриш.

Харьковский национальный университет радиоэлектроники.

Рассмотрена проблема охраны интеллектуальной собственности в киберпространстве. Исследована специфика защиты программных продуктов и баз данных как объектов интеллектуальной собственности в условиях выхода информационных систем в Internet. Обоснована необходимость сочетания правовых методов охраны с технологиями защиты данных и сетевой безопасности.

Ключевые слова: *интеллектуальная собственность, электронный бизнес, информационная безопасность, глобальная сеть, программный продукт, база данных, авторское право,, патент.*

Введение

Основным фактором экономического развития современного общества является интеллектуализация, одним из проявлений которой следует считать повсеместное использование информационных технологий, рост сети Internet и, как следствие, формирование информационной среды, охватывающей все сферы деятельности человека, в том числе и бизнес. Конкурентоспособность бизнеса непосредственно связана с применением современных IT-технологий. Последнее объясняется тем, что конкуренция требует от бизнеса большей степени открытости и гибкости, адекватности и оперативной реакции на все изменения внешней среды.

Выполнение этих требований возможно только при условии использования информационных систем и современных средств телекоммуникаций, формирующих среду для информационного обмена между всеми структурными подразделениями пространственно распределенных бизнес-структур.

Примерами такого обмена можно назвать связь головной организации с удаленными офисами, посещение Web-сайтов с размещенной на них рекламой, выполнение запросов менеджеров предприятий при заключении торговых сделок и проведении финансовых операций и пр. Использование информационных систем в качестве одного из основных инструментов управления бизнесом и возможность доступа к информационным ресурсам киберпространства, обусловленная интеграцией локальных и корпоративных сетей предприятия в глобальную сеть, привели к трансформации традиционных форм бизнеса в электронные.

Однако появление электронного бизнеса наряду с неоспоримыми преимуществами (экономия времени на контакты с деловыми партнерами и сотрудниками, более совершенная система документооборота, снижение расходов на организацию и поддержание инфраструктуры предприятия, уменьшение стоимости рекламы, новые возможности для маркетинга) актуализировало задачу обеспечения его информационной безопасности (ИБ). Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий, которые могут нанести ущерб владельцам или пользователям информации [1]. Причем, последствия от нарушения ИБ можно рассматривать как в правовом поле, так и с точки зрения финансовых потерь предприятий.

Следует отметить, что несмотря на интенсивное развитие IT-технологий, уязвимость современных информационных систем и компьютерных сетей существенно не снижается [2]. Поэтому проблемы обеспечения информационной безопасности привлекают внимание как разработчиков информационных систем, так и многочисленных пользователей, включая предприятия, работающие в области электронного бизнеса.

Цель работы

Одним из аспектов указанной проблемы является то, что подавляющая часть ресурсов, размещенных в информационных системах, является интеллектуальной собственностью, охране которой в настоящее время уделяется большое внимание. К указанным ресурсам, являющимся объектами интеллектуальной собственности, относятся де-юре базы данных (БД) и программные продукты (ПП), а де-факто – доменные имена, служащие для адресации Web-сайтов. Экстерриториальность киберпространства, постоянно растущее число пользователей глобальной сети, а также мобильность и виртуальность природы информационных объектов определяют необходимость дальнейшего развития проблемы охраны объектов интеллектуальной собственности в условиях их размещения в информационных системах и сетях.

Специфика защиты интеллектуальной собственности в информационном пространстве

Сложность решения указанной проблемы обусловлена следующим:

- информация, распространяемая через Internet, становится доступной всем пользователям глобальной сети. В то же время правовая защита объектов интеллектуальной собственности осуществляется на территориальной основе, т.е. согласно национальным законодательствам, которые далеко не всегда идентичны. Данное обстоятельство позволяет считать одно и то же нарушение противоречащим правовым нормам одной страны и не нарушающим законодательства других. Заключение международных договоров с целью правового регулирования распространения информации в Internet с участием всех стран мирового сообщества в настоящее время нереально;

- использование процедуры правовой защиты объектов интеллектуальной собственности требует достаточно убедительного доказательства факта нарушения прав и защиты интересов авторов и/или владельцев этих прав. Однако, учитывая неовеществленный и динамичный характер информации как таковой (речь не идет о физическом носителе), и делокализованную природу Internet, зафиксировать место и время нарушения прав фактически невозможно;

- большинство информационных объектов, будучи результатом творческого труда, имеют статус интеллектуальной собственности. В частности, правовая защита компьютерных программ и БД осуществляется нормами авторского права. Однако анализ сведений, содержащихся в БД информационных систем предприятий и организаций позволяет заключить, что многие из них представляют собой коммерческую тайну. Неправомерный доступ к этим сведениям и их последующее использование можно трактовать как недобросовестную конкуренцию. Отсюда следует, что защита размещенной в БД конфиденциальной информации должна выполняться не только нормами авторского права, но также законодательством об охране коммерческой тайны и защиты от недобросовестной конкуренции;

- в законодательствах многих стран (в том числе Украины) отсутствует однозначная трактовка понятийной базы и терминологии, относящихся к защите интеллектуальной собственности.

Таким образом, вышеизложенное позволяет заключить, что достаточно надежную защиту объектов интеллектуальной собственности, размещенных в информационных системах, имеющих выход в Internet, обеспечить только существующими в настоящее время правовыми методами невозможно. Следует также констатировать, что стремительное развитие IT-технологий и глобальной инфраструктуры привело к заметному отставанию действующей нормативно-правовой базы по части охраны интеллектуальной собственности от реальных потребностей в этой области. Данное отставание можно сократить, выполняя соответствующие мероприятия по следующим направлениям:

- создание в информационных системах условий, позволяющих повысить эффективность использования существующей нормативно-правовой базы в области защиты интеллектуальной собственности;

- выработка более действенных правовых норм по охране интеллектуальной собственности, учитывающих специфику информационной среды;

- применение одновременно с правовыми нормами криптографических методов, в большей степени учитывающих специфику информационных ресурсов как объектов интеллектуальной собственности и некритичных к различиям национальных законодательств по ее охране.

Анализ правовых аспектов защиты программных продуктов как объектов интеллектуальной собственности

С позиции разработчиков информационных систем наиболее действенными механизмами защиты интеллектуальной собственности в настоящее время является совокупность методов и средств, обеспечивающих информационную безопасность этих систем. Однако используемые криптографические методы защиты информационных объектов должны также учитывать их правовой статус как интеллектуальной собственности. В этой связи представляется целесообразным рассмотреть суть правовой защиты, предоставляемой объектом интеллектуальной собственности в киберпространстве.

Наиболее уязвимыми интеллектуальными ресурсами современного бизнеса являются базы данных и программные продукты. Их охрана закреплена нормами авторского права в Берн-

ской конвенции, членом которой является Украина, и на национальном уровне осуществляется согласно закону «О авторском праве и смежных правах». Однако следует отметить, что защита современных ПП только нормами авторского права далеко не полностью удовлетворяет интересы их разработчиков [3]. Это объясняется тем, что авторское право направлено исключительно на предотвращение нелицензионного использования программ, но не на устранение возможного плагиата принципов и идей, заложенных в их алгоритме. В то же время наиболее творческие аспекты создания ПП остаются вне правовой защиты. Это подтверждается произошедшими изменениями в технологиях разработки программных средств, чему способствовали следующие обстоятельства:

-появление специализированных средств разработки программных продуктов с готовыми типовыми модулями;

-возможность использования фрагментов уже существующих программ и отсутствие контроля новизны и уникальности при регистрации вновь создаваемых продуктов;

-появление большого числа программ-аналогов по выполняемым функциям;

-сокращение срока жизни программ до 5-7 лет.

Всё это ставит под сомнение правомерность использования для защиты ПП только института авторского права в существующей его трактовке. Наиболее целесообразной системой защиты компьютерных программ следует считать такую, которая бы объединила экспертную проверку, необходимую при патентной охране, с существующей практикой защиты ПП нормами авторского права. Основными трудностями на пути осуществления данного подхода являются [4]:

-необходимость согласования нормативно-правовой базы в странах, использующих коммерческие ПП;

-отсутствие квалифицированных экспертов-патентоведов со знаниями в области программирования;

-необходимость создания специализированной базы данных с текстами уже существующих программ в выходных кодах.

Хотя данные условия в настоящее время в полном объёме не могут быть выполнены, необходимость патентной защиты компьютерных программ осознана и реализована в ряде экономически развитых стран (США, Япония, страны-участники Европейского патентного ведомства).

В практике борьбы с компьютерным пиратством существует ряд рекомендаций относительно доказательства фактов нелегального использования ПП [5]. Это, прежде всего, проведение проверок установленного на компьютерах программного обеспечения с целью определения законности его приобретения и использования.

Однако трудности осуществления таких проверок и неоднозначность определения нарушителей авторских прав на ПП усложняют на практике привлечение субъектов правонарушения к ответственности, в первую очередь юридических лиц. Только немногие из компаний-производителей программного обеспечения доводят дело до судебного рассмотрения, хотя и оканчивается оно, как правило, в пользу правообладателя.

Недостаточная эффективность правовых методов защиты компьютерных программ привела к появлению чисто технических способов предотвращения их копирования и несанкционированного использования. К этим методам относится введение паролей, необходимость получения файлов-ключей, ограничение срока действия программы, ограничение функциональности незарегистрированных копий. Однако данные методы могут затруднить, но не исключить возможность копирования и незаконного использования компьютерных программ.

Наибольшие экономические потери от нарушения авторских и патентных прав несут компании-производители программных продуктов. Не следует также забывать об ущербе, который наносит стране высокий уровень компьютерного пиратства. Это, прежде всего, экономические потери, к которым следует отнести недополучение валового внутреннего продукта и соответственно уменьшение налоговых поступлений, потери на таможенных сборах и платежах, снижение инвестиционной привлекательности страны, а также международные экономические санкции. В основном речь идет об экономических потерях стран, в которых имеется достаточно мощный парк компьютеров и практически отсутствует рынок лицензионного программного обеспечения.

Несколько в ином аспекте следует рассматривать последствия компьютерного пиратства относительно некоммерческих программ. Они, в отличие от коммерческих, разрабатываются по заказам отдельных предприятий в процессе проектирования или реинжиниринга их информационных систем и предназначены для работы сравнительно небольшого числа сотрудников этих предприятий.

Использование указанных ПП позволяет реализовать информационную поддержку вновь создаваемых бизнес-процессов и повысить уровень эффективности уже существующих, получить новые возможности оперативной связи с деловыми партнерами, мониторинга рыночной среды. В результате применения программных средств, адаптированных к конкретному бизнесу, обеспечивается его качественное превосходство над конкурентами.

Не вызывает сомнения, что эти ПП, будучи объектами интеллектуальной собственности их создателей или владельцев бизнесов, должны иметь статус правовой защиты. Его особенность состоит в том, что некоммерческие ПП следует защищать не столь авторским правом, сколь законодательством о недобросовестной конкуренции и об охране коммерческой тайны.

Действенность правовой защиты ПП непосредственно связана с установлением факта их неправомерного использования. Однако установить и юридически обосновать факт незаконного ознакомления и/или копирования ПП чрезвычайно трудно. В связи с этим целесообразно применение методов, предотвращающих или снижающих до минимума вероятность несанкционированного доступа к программному обеспечению информационных систем. К данным методам следует отнести административно-организационные меры, разграничение доступа к программно-информационным ресурсам системы, использование криптографических средств.

Концепция защиты баз данных в условиях электронного бизнеса

Вторым объектом интеллектуальной собственности, размещенным в информационной среде, являются базы данных, которые согласно Бернской конвенции охраняются, как и программы, нормами авторского права. Однако бурное развитие компьютерных информационных технологий и глобальной сети Internet внесли коррективы в трактовку БД как объектов творческого труда и, следовательно, обоснованность их защиты нормами авторского права. Речь идет о размещенных на сайтах международных организаций и государственных учреждений БД с общественно-полезной информацией. Создание и поддержание работоспособных БД требует значительных финансовых инвестиций и трудовых затрат, которые зачастую не являются творческими. Последнее позволяет подобные БД не причислять к объектам интеллектуальной собственности, на которые распространяется охрана авторским правом. Вместе с тем каждый участвующий в создании и ведении БД независимо от их творческого или нетворческого характера заинтересован в адекватном вознаграждении и защите своих экономических интересов.

Отношение к защите авторским правом нетворческих БД неоднозначное. С одной стороны, предоставление охраны нетворческим БД стимулирует их составителей к продолжению деятельности в области накопления и систематизации общественно-полезных знаний, что повышает уровень информатизации различных бизнесов. С другой стороны, оплата информации, размещённой в БД, приведет к удорожанию всех производимых с её помощью товаров и услуг.

На основании вышеизложенного можно заключить, что наиболее вероятной перспективой усовершенствования нормативно-правовой базы стран мирового сообщества является введение института охраны нетворческих баз данных. При этом необходимо обеспечить гарантию доступа к охраняемым БД только при условии соответствующей оплаты информационных услуг. Последнее в условии киберпространства возможно только с помощью технологий информационной безопасности, в частности, организации защищенного доступа удаленных пользователей.

Очевидно, достижение и поддержание баланса интересов потребителей информации и составителей БД является специфической задачей для каждой страны. Например, в европейской практике существует институт особой охраны БД или право на БД, запрещающее использовать без разрешения автора базы данных, созданные даже нетворческим трудом [6]. В США, напротив, сильны традиции свободного доступа к любым незасекреченным информационным ресурсам. Различие в национальных законодательствах в подходах к охране нетворческих БД

приводит к тому, что в условиях киберпространства БД со свободным доступом становятся донорами для конкурирующей информационной индустрии.

Несколько иначе обстоят дела с защитой информации, размещенной в БД бизнес-структур. В этих БД хранятся сведения, касающиеся всех аспектов функционирования предприятия. К этим сведениям можно отнести:

- информацию о производственных процессах (технологии и оборудование, дисциплина поставок, организация сбыта, оценка качества и эффективности и пр.);
- информацию о рынке (цены, отношения с деловыми партнёрами, сведения о конкурентах, анализ текущих продаж и прогноз будущего спроса, условия договоров и пр.);
- информацию об организационной структуре и финансах (кадровая политика, персонал и полномочия, бухучёт, финансовая отчётность и пр.)

Судя по объёму и содержанию указанных сведений, можно считать, что экономическая безопасность предприятия непосредственно зависит от информационной безопасности его БД.

База данных как объект защиты авторским правом отличается от традиционных объектов интеллектуальной собственности. Отличия состоят в следующем:

- информация баз данных в бизнесе предназначена для использования узким кругом лиц;
-информация имеет различный уровень конфиденциальности и предназначена для различных пользователей. Последнее обуславливает необходимость разработки процедуры управления доступом к ресурсам;
-основной ценностью является не форма представления и организации данных, а их содержание;
- несанкционированное ознакомление с информацией БД ставит под угрозу конкурентоспособность предприятия, которому принадлежит эта БД.

Таким образом, можно заключить, что хранящаяся в БД информация (или её существенная часть) непосредственно связана с экономическими интересами предприятия и, следовательно, является коммерческой тайной, которая должна быть защищена законом о недобросовестной конкуренции. Однако данный закон может быть использован только после доказательства факта противоправных действий по извлечению из БД и использованию конфиденциальной информации.

С точки зрения экономических интересов предприятия защита БД должна быть организована так, чтобы исключить или свести к минимуму возможность несанкционированного доступа к сведениям, являющимся коммерческой тайной. Причём фактор правовой защиты, направленный в основном на формирование у потенциальных правонарушителей сознания неотвратимости наказания, не является основным при выборе методов охраны БД.

Это объясняется тем, что существующие технологии позволяют «взломать» БД так, что утечка информации остаётся долгое время (или даже навсегда) необнаруженной. В результате этого экономическим интересам предприятия наносится серьёзный ущерб, его конкурентоспособность падает, в то время как менеджер не может дать правильную оценку причинам спада.

Следует отметить, что во многих случаях руководство предприятий даже при обнаружении неправомерного использования конфиденциальных сведений не спешит обращаться к уполномоченным государством органам относительно нарушения прав на интеллектуальную собственность [7]. Это объясняется следующими факторами:

- правовая форма защиты требует много усилий и времени и даже в случае успешного решения дела не гарантирует полного возмещения убытков;
- факт разглашения утечки коммерческих секретов ставит под сомнение деловую репутацию предприятия.

Это еще раз подтверждает, что защиту БД, размещенных в информационных системах бизнес-структур, только правовыми методами нельзя считать достаточной.

Базовые технологии информационной и сетевой безопасности

Для эффективной защиты интеллектуальной собственности в киберпространстве необходимо объединение правовых методов и криптографических, препятствующих несанкционированному доступу к интеллектуальным ресурсам предприятия.

Для предотвращения утечки экономически значимой информации в условиях функционирования распределенных информационных систем следует использовать базовые технологии информационной и сетевой безопасности. К ним следует отнести:

- криптографическую защиту данных для обеспечения конфиденциальности, целостности и подлинности информации, в результате чего потенциальный противник лишается возможности извлечь информацию, исказить ее смысл или заменить истинное сообщение ложным;
- технологии идентификации и аутентификации, предназначенные для распознавания и проверки подлинности заявленных пользователей, процессов или устройств;
- управление доступом на уровне авторизованных пользователей и защита от несанкционированного доступа к критической для предприятия информации;
- технологии построения виртуальных защищенных сетей VPN, предназначенных для противодействия сетевым атакам и безопасному использованию открытых сетей;
- технологии межсетевых экранов, назначение которых состоит в защите локальной сети предприятия от вторжений из глобальной сети Internet или корпоративной сети Intranet;
- поддержку инфраструктуры управления открытыми ключами PKI, представляющими собой систему цифровых сертификатов и центров сертификации, назначение которых – проверка и идентификация каждой из взаимодействующих сторон;
- технологии защиты от вирусов, реализуемые с помощью антивирусных программ и специализированных комплексов антивирусной защиты и профилактики;
- технологии обнаружения вторжений, предназначенные для исследования защищенности информационных ресурсов и, в первую очередь, для распознавания уязвимостей и реализуемых на их основе атак.

Указанные базовые технологии могут использоваться при проектировании информационных систем или в процессе их реинжиниринга. Выбор конкретных технологий осуществляется по результатам аудита безопасности информационной системы и последующей оценки рисков ее нарушения.

Выводы

1. Существующие механизмы защиты объектов интеллектуальной собственности, размещенных в киберпространстве, не соответствуют их специфике и не учитывают возможности современных информационных технологий по неправомерному доступу и использованию этих объектов.

2. Защиту объектов интеллектуальной собственности (программные продукты, базы данных) с помощью существующих правовых норм нельзя считать достаточной.

3. Для обеспечения защиты интеллектуальной собственности в киберпространстве необходимо объединение правовых методов и современных технологий информационной и сетевой безопасности.

ЛИТЕРАТУРА:

1. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. - М.: ДМК Пресс, 2004. – 616 с.
2. Гульбин Ю. Охраняем ли Интернет? // ИС. Авторское право и смежные права. - 2003. - № 9. - С. 26-34.
3. Скляров І. Комп'ютерна програма та патентна охорона // Інтелектуальна власність. – 2003. - № 5. – С. 7-14.
4. Ермаков М., Попов М. Пути решения проблемы правовой охраны программного обеспечения ЭВМ // ИС. Промышленная собственность. - 2001. - № 6. - С. 48-53.
5. Симкин Л. Новые меры обеспечения доказательств по делам о защите компьютерных программ // ИС. Авторское право и смежные права. - 2003. - № 2. - С. 21-29.
6. Вайшнурс А. Современность и перспективы правовой охраны баз данных в России, США, Европейском союзе // ИС. Авторское право и смежные права. – 2003 - № 11. – С. 4-18.
7. Задірака В.К., Олексюк О.С. Методи захисту фінансової інформації. - Тернопіль: Видав. ОПТВПК „Збруч", 2002. – 456 с.

Левыкин Виктор Макарович, д.т.н., проф., зав. кафедрой Информационных управляющих систем Харьковского национального университета радиоэлектроники, сл. тел. 70-21-451, *iyc@kture.kharkov.ua*

Гавриш Татьяна Валентиновна, к.т.н., доц. кафедры Информационных управляющих систем Харьковского национального университета радиоэлектроники, сл. т. 70-21-451, д.т. 700-69-74.

ваний на порівнянні й виборі найкращого варіанту.
Табл. 1. Іл. 3. Бібліогр.: 5 найм.

УДК 621.315.592:669.791

Модельноорієнтований підхід до функціонального тестування web-базованих інформаційних систем / В.М. Левикін, М.О. Тихенко // Нові технології. – 2007. - № 1-2 (15-16). – С. 82.

В роботі розглянуті проблеми й особливості функціонального тестування сучасних Web-базованих інформаційних систем та існуючі підходи до тестування таких систем. З урахуванням недоліків існуючих підходів запропоновано підхід, що має в основі моделювання вимог до Web-базованих інформаційних систем. Цей підхід складається з етапів: моделювання вимог до системи, автоматизована генерація тестових сценаріїв за допомогою інструментального засобу, виконання тестових сценаріїв, генерація звітів по результатам тестування та їх аналіз.

Іл. 2. Бібліогр.: 4 найм.

UDC 621.315.592:669.791

Model-based approach to web-based information systems functional testing / V.M. Levykin, M.A. Tykhenko // New Technologies. – 2007. - № 1-2 (15-16). – P. 82.

Problems, particular qualities of Web-based information systems functional testing and existing approaches to such systems testing are considered in this work. Taking into account disadvantages of existing approaches, an approach based on a model of Web-based information systems functional requirements is suggested. This approach consists of such stages: modeling system requirements, automated test case generation with a help of special tool, test case execution, report generation and analysis.

Fig. 2. Ref.: 4 items.

УДК 681.3.06; 004.3

Система тестування взаємодії WEB та SQL–серверів / Р.І. Макарчук, В.Я. Ляшкевич, О.Я. Олар, С.В. Мельничук // Нові технології. – 2007. - № 1-2 (15-16). – С. 87.

Розглянуті фактори, які впливають на середній час обробки запиту та потоку запитів. Проведений аналіз існуючих способів розташування серверів в мережі. Запропонована система тестування процесу взаємодії Web та SQL-серверів. За допомогою системи проведено тестування серверів Firebird та MySQL. Результати тестування наведені на рисунках у вигляді графіків та екранних зображень.

Іл. 11. Бібліогр.: 6 найм.

UDC 681.3.06; 004.3

System of testing of the WEB and SQL-servers interaction / R.I. Makarchuk, V.Ja. Lyashkevich, O.Ja. Olar, S.V. Melnichuk // New Technologies. – 2007. - № 1-2 (15-16). – P. 87.

Factors which affect mean time of treatment of a query and stream of queries are considered. The analysis of the existing methods of servers location in the network is performed. The system to test the process of the Web and SQL-servers interaction is offered. By the system proposed Firebird and MySQL servers have been tested. The results of testing are shown in figures in the form of graphs and screen shots.

Fig. 11. Ref.: 6 items.

УДК 621.8

Виявлення спама на основі алгоритмів штучного імунітету / О.І. Михальов, Ю.О. Каліберда // Нові технології. – 2007. - № 1-2 (15-16). – С. 92.

У статті запропонований новий підхід щодо виявлення й фільтрації спама на основі одного з алгоритмів штучного імунітету. Відмінною рисою запропонованого алгоритму є спосіб побудови детекторів, що складаються з сигнатур, що однозначно визначає семантику листа.

Іл. 2. Бібліогр.: 4 найм.

UDC 621.8

spam detecting on the basis algorithms of artificial immunity / O.I. Mikhalev, Yu.O. Kaliberda // New Technologies. – 2007. - № 1-2 (15-16). – P. 92.

In article the new approach for spam detect and filtration on the basis algorithms of artificial immunity. Distinctive feature of the offered algorithm is the way construction of the detectors, consisting of the signatures, unequivocally defining semantics of the letters.

Fig. 2. Ref.: 4 items.

УДК 004.056.53:347.211

Інформаційна безпека як фактор захисту інтелектуальної власності в кіберпросторі / В.М. Левикін, Т.В. Гавриш // Нові технології. – 2007. - № 1-2 (15-16). – С. 95.

Розглянуто проблему охорони інтелектуальної власності в кіберпросторі в контексті інформаційної безпеки електронного бізнесу й електронної комерції. Показано невідповідність існуючих законодавчих норм в галузі захисту програмних продуктів і баз даних як об'єктів інтелектуальної власності сучасним технологіям розробки програмних засобів і рівня *творчого начала у формуванні баз даних. Визначено* тенденції в диференціації підходів до правового захисту комерційних і некомерційних програмних продуктів, творчих і нетворчих баз даних, обґрунтована доцільність захисту інтелектуальних

UDC 004.056.53:347.211

Information security as factor of protection of intellectual property in cyberspace / V.M. Levikin, T.V. Gavrish // New Technologies. – 2007. - № 1-2 (15-16). – P. 95.

The problem of protection of intellectual property in cyberspace in the context of information security of electronic business and electronic commerce has been researched. There has been shown lagging behind of the present legislative basis in the sphere of protection of program products and database as objects of intellectual property from modern technologies of working out of program means and the level of creative work in forming database.The tendencies in differentiation of approaches and legislative protection of commercial and non-commercial program products, creative and non-creative database have been worked out. The necessity to protect