УДК 001.6+004

Общий закон защиты информации

И. А. Громыко

Харьковский национальный университет имени В.Н. Каразина, Украина

В статье сформулирован «Общий закон защиты информации» на основании требований «Общей парадигмы защиты информации», государственных стандартов Украины в области информационной безопасности и новой редакции Закона Украины «Про информацию».

Ключевые слова: *защита информации, парадигма и закон защиты информации.*

В статті сформульовано «Загальний закон захисту інформації» на підставі вимог «Загальної парадигми захисту інформації», державних стандартів України в галузі інформаційної безпеки і нової редакції Закону України «Про інформацію».

Ключові слова: *захист інформації, парадигма і закон захисту інформації*

An author proposed the "General Law of data protection". The law is based on: the requirements of the "General paradigm of data protection", state standards of Ukraine in the field of information security and the new edition of the Law of Ukraine "On information".

Keywords: *data protection, General paradigm of data protection, General Law of data protection.*

1. Введение.

Первая попытка сформулировать общий закон защиты информации была предпринята в начале 21-го века, когда стало очевидным, что в молодом государстве Украине, принявшем новую Конституцию и закон «Про информацию», существует необходимость развития теории информационного права, выработки нового и коррекции устоявшегося информационного понятийного аппарата [1-3].

Разработанная в 2002 году «Общая парадигма защиты информации» (далее, - Парадигма), опубликована в научных изданиях, апробирована на отечественных и международных научных конференциях, а также на протяжении 10 лет использована в учебном процессе при подготовке специалистов области технической защиты информации (ТЗИ) [4-10].

В первую очередь Парадигма предложила устранить существующую некорректность в определениях носителей и сред их распространения. На фоне множества существующих классификаций носителей информации было рекомендовано разделить их на две группы: основные носители и дополнительные (вспомогательные). Аналогично стилю всемирно известных критериев надёжности компьютерных систем («Оранжевая книга») [11], в Парадигме к носителям предъявлены общие требования, выполнение которых позволяет считать информацию защищённой при ее перемещении от источника к получателю. Кроме того, предложено заменить словосочетание «среда распространения информации» на словосочетание «среда влияния» (на носители информации). Скорректировано смысловое значение определения термина «сигнал».

Сформулировано определение термина «информация», которое существенно отличалось от первичного определения, установленного в 1992 году Законом Украины «Про информацию».

Парадигма явилась отправной точкой для выполнения ряда дальнейших исследований общенаучного и прикладного значения. В формулировках технических каналов утечки информации (ТКУИ) «среда распространения» была заполнена множеством реальных носителей информации, с их режимными «адекватностью и коммуникабельностью».

В дальнейших работах отдельное внимание было уделено такому носителю информации, как «источник угроз», контроль за возникновением которого позволяет создавать эффективные системы защиты информации упреждающего типа. Аналитическим центрам служб безопасности государств и бизнес-структур было доказательно рекомендовано перейти из статических режимов пассивного аналитического созерцания атак на информацию в активные динамические режимы циклического типа «разведка-прогноз-коррекция системы ТЗИ-разведка» [12,13].

Результаты парадигмальных исследований использованы за рубежом для решения конкретных проблем обеспечения информационной безопасности типовых объектов, в составе которых функционируют информационно-телекоммуникационные системы, имеющие признаки ключевых систем информационной инфраструктуры органов государственного управления [14,15].

Работа по Парадигмальной тематике, в плане коррекции информационного понятийного аппарата, в 2008 году привела к выявлению источников угроз, завуалированных в многозначности административно-правовой терминологии. Была показана излишествующая административная многозначность определений в многочисленных статьях «Кодекса Украины об административных правонарушениях», содержащих информационные угрозы: утечка информации - 13 статей, нарушение целостности информации - 60 статей, блокирование информации - 86 статей. Проведенная информационная фильтрация административных правонарушений служит основанием для разработки в Украине «Кодекса об информационных правонарушениях» [16].

С момента опубликования Парадигмы, в области защиты информации произошло множество положительных сдвигов, позволяющих более эффективно решать задачи по обеспечению информационной безопасности объектов и систем информационной деятельности. Так, в Украине, в законодательной базе, относящейся к области безопасности информационных систем и технологий, претерпели изменения ряд Законов Украины (например, существенно изменено содержание Закона Украины «Про информацию» и др.). Реорганизованы и обновлены руководящие структуры (например, «Держспецзв’язок»), обновлена аппаратурная и элементная база технических средств защиты информации.

Однако, несмотря на общее желание государств повысить уровень информационной безопасности, оказалось, что новые законы, инструкции и, как ни парадоксально, - увеличение объёма финансирования, существенно не изменили ситуацию в этой области. Задав поисковым системам общедоступного Интернета словосочетания «утечка секретных сведений» и/или «утечка данных»

можно получить разворот негативного положения дел. Поисковые системы по данной тематике предлагают сотни наглядных примеров, позволяющие сделать вывод о том, что и в Соединённых Штатах Америки, и в Украине, и в Японии, и в России, и в Германии (и т.д.) – ситуация с защитой информации находится на одинаковом, недостаточно высоком уровне [17].

На множестве конкретных примеров практика доказывает, что «чего-то не достает» (каких-то элементов или действий) в системах защиты информации. Не учитываются некие «факторы сред влияния». Эти факторы, которым изначально не придают существенного значения, в реальных ситуациях начинают превалировать по значимости над применёнными методами и средствами защиты информации. В результате, - угрозы информации «успешно» реализуются конкурентами, разведывательными службами иностранных государств и др.

Необходимость разрешения этой проблемы диктует дальнейшее совершенствование «Общей парадигмы защиты информации» до уровня «Общего (основного) закона защиты информации».

2. Постановка проблемы в общем виде, её причины и связь с важными научными или практическими заданиями.

Прежде всего, необходимо показать причины, которые привели к возникновению самой проблемы. Таковых, например, в Украине, - минимум, две: объективная причина и субъективная.

Объективность кроется в том, что в период 90-х годов прошлого столетия на государственном уровне необходимо было крайне срочно разработать правовые, организационные и технические основы информационной безопасности, провести их экспертизу и корректировку на согласованность и соответствие мировым стандартам в области защиты информации. Вновь созданным государственным органам системы ТЗИ ставились экстренные задачи защиты информации в технических средствах создания, приёма, передачи, обработки, хранения информации и т.д.

Субъективность заключается в том, что по своей сути в форс-мажорной ситуации не всегда удавалось учитывать на первый взгляд незначительные моменты, относящиеся в какой-то степени к рутинным философским высказываниям и рассуждениям. При этом некоторые базовые элементы основ теории защиты информации остались нетронутыми и их несовершенство легло в основу причин, породивших проблемы в системах защиты информации.

3. Анализ последних исследований и публикаций источников

Одним из основных законов, который в 1992 году ознаменовал рождение в Украине информационного права и начало разработки языка информационного законодательства, явился Закон Украины «Про информацию».

Считается, что информация (informatio, - лат.) это абстрактное понятие, которое может иметь такие значения, как: разъяснение, изложение фактов и событий, истолкование, представление, понятие, знакомство, просвещение, определение и др. Наиболее общее определение информации представлено в философии, где её понимают, как отражение реального мира. С расчётом на

тезаурус «среднестатистического» гражданина, более доходчивое определение термина «информация» приводится в законодательных базах различных стран мира.

Однако и здесь встречаются некоторые неточности. Так в первой редакции (1992 г.) Закона Украины «Про информацию» информация трактуется, как «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі». Подробный анализ данного определения показал, что используемые в нём термины выражаются, в конечном итоге, сами через себя.

В 2002 году была предложена следующая Парадигмальная формулировка: «Информация – это зафиксированное на носителе представление о предметах, процессах, событиях, природных явлениях и т.п.».

В 2011 году в новой редакции Закона Украины «Про информацию» под этим термином было установлено понимать «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» («какие-либо сведения и/или данные, которые могут быть сохранены на материальных носителях или отображены в электронном виде»). Практически, такое определение является синонимальным отражением определения, приведенного в Парадигме [4-6].

Однако, при тщательном рассмотрении выявляется, что и новая формулировка в законе «Про информацию» содержит некоторые неточности. Говоря об информации, как о «каких-либо сведениях и/или данных, которые «могут быть сохранены» на материальных носителях или отображены в электронном виде», логически разделяется информация и носители информации.

Так, например, у людей, познающих основы информационной безопасности, после прочтения словосочетания «могут быть» возникает вопрос о местонахождении информации до того момента, когда эти «сведения и/или данные» будут сохранены. Ответ прост: «Информация всегда находится на носителе – и, в том числе, до того, описанного в законе момента, когда её сохранят на другом носителе информации». Таким образом, группа из двух словосочетаний «…могут быть сохранены… + …или отображены…» применена здесь неуместно, так как она не исключает рассуждений о сохранении (расположении, нахождении) каких-либо сведений и/или данных на чём-либо другом, отличающемся от носителей информации.

Кроме того, в данном определении закон добавил ещё один вариант нахождения информации в пространстве и времени. Оказалось, что информация может:

1 - находиться на материальных носителях с целью сохранения;

2 - отображаться в электронном виде.

При этом в законе эти два свойства строго разделены - «или так, или иначе».

Тогда, находится ли информация в момент отображения в электронном виде на каком-либо носителе? – Да, находится.

Но в законе этот момент определён так, что не исключается суждение о том, что при отображении в электронном виде информация не находится на материальном носителе. Такое высказывание некорректно, так как:

1 - объединяет статический процесс (например, - при хранении информации) с динамическим процессом перемещения информации (например, по проводникам в линиях связи или в линиях систем обработки информации);

2 – «реанимирует» устаревшие требования двух важнейших (но «не совсем корректных») формулировок (они будут рассмотрены ниже) одного из основополагающих государственных стандартов Украины в области технической защиты информации – ДСТУ 3396.0-96.

В данном стандарте, без определения и раскрытия свойств терминов «носитель» (п. 3.3) и «среда распространения» (п. 3.4) информации, в отношении носителей информации было обобщённо сказано, что «носителями информации могут быть физические поля, химические вещества, которые создаются в процессе информационной деятельности, производства и эксплуатации продукции разного назначения и сигналы».

Понимая, что носители информации материальны, а материя существует в пространстве и времени в виде полей и вещества, некорректным оказался показ «сигналов» в виде некоей третьей формы существования материи. Возможно поэтому, далее, понятие «сигнала» оказалось завуалированным, получив информационную окраску. Так (в этом пакете стандартов) ДСТУ 3396.2-97 в пункте 6.2 установил определение «информационного сигнала» (ТЗІ), охарактеризовав его, как «физическое поле и(или) химическое вещество, которые содержат информацию с ограниченным доступом». И если можно в какой-то степени допустить тавтологию в словосочетании «информационный сигнал», то продолжает оставаться открытым вопрос принадлежности самого «сигнала» без добавки – «информационный». Понятно, что с материалистической точки зрения и то, и другое может относиться либо к полю, либо к веществу, либо, как в случае дуализма, - и к тому, и другому одновременно. В Парадигме (в отличие от показанной путаницы) термину «сигнал» дано скорректированное определение.

Далее, согласно ДСТУ3396.0-96, средой для носителей информации «могут быть линии связи, сигнализации, управления, энергетические сети, конечное и промежуточное оборудование, инженерные коммуникации и сооружения, оградительные строительные конструкции, а также прозрачные для света элементы зданий и сооружений (проёмы), воздушная, водная СРЕДА, грунт, растительность и так далее».

В данных формулировках, к примеру, отсутствует электрический ток (направленное движение носителей зарядов) который, с одной стороны, – порождает несколько видов вышеупомянутых физических полей, и, с другой стороны, – может быть образован в проводниках, полупроводниках, диэлектриках, плазме (и др.) под влиянием этих полей. Также, при выяснении сущности таких носителей информации как «сигналы», возникает множество противоречивых ситуаций, с которыми можно ознакомиться в [18].

Здесь виден материалистический диссонанс формулировок ДСТУ 3396.0-96 и отсюда берут начало такие дальнейшие не совсем корректные формулировки как «отображение информации в электронном виде» [2], в которых не видно информации, как таковой, а существует её отображение. Не говорится об

электронах, частицах-носителях зарядов или электрическом токе в целом, а предлагается «электронный вид», в котором может быть отображена информация.

Чтобы понять предложенную формулировку нужно выяснить значение терминов «отображение», «вид», «электронный вид». “Отображение”, как термин широко применяется в математике. Отображение, как «параллельное проектирование одной плоскости на другую», понятия «функция», «оператор», «преобразование», - всё это правильно, но дифференцируемые и конформные отображения тяжело вписываются в тезаурус не только обывателя, но и студентов младших курсов ВУЗов. Если же под отображением понимать установление некоего соответствия элемента **x** из множества {A} элементу **y** из множества {B}, то понятно, что не все пользователи смогут здесь понять физическую сущность «информации» в её новом изложении Закона Украины «Про информацию».

При запросе в поисковой системе “Google” слова «отображение» (в кавычках) мы получаем 17 миллионов 300 тысяч вариантов толкований и словосочетаний по данной тематике.

“Вид” - определенная категория, в большей степени применяемая к живой среде. “Электронный вид” – данному словосочетанию соответствует 30 миллионов 200 тысяч вариантов толкований, а если подойти более строго к интерпретации данного термина на государственном языке Украины, то мы получим 800 000 вариантов. Так, «Практическое руководство кадровой службы местной государственной администрации» утверждает, что «Электронный вид» - это информация на магнитных или флеш-носителях [17].

Закон Украины «Об электронных документах и электронном документообороте» не даёт определение «электронному виду», но раскрывает смысл электронного документа, как документа, информация в котором зафиксирована в виде электронных данных, включая обязательные реквизиты документа. Электронный документ может быть создан, передан, сохранен и преобразован электронными средствами в визуальную форму. Визуальной формой представления электронного документа является отображение данных электронными средствами или на бумаге в форме, пригодной для восприятия его содержания человеком.

Поиск словосочетания “відображення в електронному вигляді” («отображение в электронном виде») позволил найти всего четыре источника. В списке найденного, первым было приведено в разделе «Проблемы права интеллектуальной собственности» исследование кандидата юридических наук, доцента Киевского университета права НАН Украины, разъясняющего «что же имели ввиду» авторы закона Украины «Про информацию» под словосочетанием «отображение в электронном виде», сопрягая его с общепринятыми информационными терминами и определениями [19]. Три других документа с данным словосочетанием оказались идентичными рефератами, поясняющими, что документы Internet предназначены для отображения в электронном виде на языке HyperTextMarkupLanguage.

Всё вышеизложенное нагромождение разъяснений некорректности нового определения термина «информация» в последней редакции Закона Украины,

показывает, что недостаточное знание основ диалектического материализма и недопонимание философского и физического смысла слов лексикона, применяемого в таких документах, как Законы Украины, Кодексы, Государственные стандарты и т.п. приводит к неоднозначностям в их формулировках и усложнению восприятия их смыслового значения.

Ярким примером вышесказанного может служить фраза из ст.6 закона Украины «О государственной тайне», в котором указано следующее: «Якщо власник секретної інформації або її матеріальних носіїв відмовляється від укладення договору чи порушує його, за рішенням суду ЦЯ ІНФОРМАЦІЯ АБО ЇЇ МАТЕРІАЛЬНІ НОСІЇ можуть бути вилучені у власність держави за умови попереднього і повного відшкодування власникові їх вартості». Здесь строго указано, что может быть изъята в собственность государства исключительно (эта) информация, или могут быть забраны её носители. То есть, не учитывается тот факт, что информация всегда существует только на носителях и её невозможно отобрать в своё пользование у собственника без изъятия носителей. Здесь уместно показать, что согласно указаниям нормативного документа ДСТЗИ Службы Безопасности Украины человек является носителем информации [17].

4. Выделение нерешённых ранее частей общей проблемы, которым посвящена данная статья

Как было показано выше, в результате несовершенства информационного понятийного аппарата и других объективных и субъективных причин оказались искажёнными изложения физических сущностей части информационных процессов с последующей неверной расстановкой акцентов при решении задач, стоящих перед работниками области информационной безопасности.

5. Формулирование цели статьи

Целью данной статьи является формулирование «Общего закона защиты информации» на базе диалектически скорректированного понятийного аппарата изложенного в новой редакции Закона Украины «Про информацию» (2011 г.), государственных стандартов Украины: 3396.0-96, 3396.1-96, 3396.2-97 и «Общей парадигмы защиты информации».

6. Изложение основного материала исследования с полным обоснованием полученных результатов

Анализ множества источников информации, раскрывающих смысловое содержание цели защиты информации и, в частности, - технической защиты информации, показывает, что, прежде всего, это «защита от утечки информации», как первоисточника всех последующих правонарушений.

Согласно тезису о том, что «защита информации должна упреждать появление самих источников угроз», необходимо, прежде всего, скрывать от потенциального правонарушителя факт наличия информации с ограниченным доступом (ИсОД) и её местоположение. Рано или поздно конкурент заинтересуется причинами экономического процветания физических или юридических лиц, которые занимают с ним одну нишу на рынке товаров и

услуг. Понятно, что эта ситуация неизбежна. Но, чем позже конкурент совершит атаку на защищаемую ИсОД, тем лучше.

Далее, в зависимости от возможностей правонарушителя и его целей, последуют попытки реализации угроз типа: нарушение конфиденциальности информации, её целостности и доступности.

Под правонарушителем мы будем понимать органы и сотрудников зарубежных спецслужб, конкурентов, криминал и любых других людей, которые незаконным путем пытаются добыть, изменить и даже уничтожить информацию или затруднить к ней доступ законных владельцев или санкционированных пользователей.

Практически все доступные автору источники информации, после ссылки на утечку ИсОД, говорят о каналах утечки информации, и о необходимости их выявления и блокирования (устранения, ликвидации и пр.).

ДСТУ 3396.2 – 97 устанавливает:

- канал утечки информации (технический - ТКУИ) представляет собой совокупность носителя информации, среды его распространения и средства разведки;

- самопроизвольный (технический) канал утечки информации; непреднамеренный канал утечки информации - технический канал утечки информации, в котором носители информации и (или) среда их распространения формируются самопроизвольно.

Из первого определения следует один из постулатов разведки о том, что канал утечки информации может быть (а в разведке, - должен быть) создан заранее, и в его состав изначально может и не входить источник информации. Это означает, что при появлении информации на каком-либо промежуточном носителе, который заблаговременно или «постфактум» подключён к носителю-источнику, образуется действующий канал утечки информации.

Из второго определения следует, что в ТКУИ «носители информации и (или) среды его распространения могут формироваться самопроизвольно». Очевидно, что невозможно и нереально самопроизвольное формирование (см. п. 3.4 ДСТУ 3391.0 96) линий связи, …, оборудования, воздушной и водной сред, грунта, растительности (и пр.). Это является неопровержимым проявлением идеализма в ДСТУ 3396.2 – 97.

Носители информации являются реальными материальными объектами, а «среды распространения» информации являются чисто надуманными словосочетаниями, опустошающими и нейтрализующими смысловое наполнение существующих проблем информационной тематики настолько, что о них начинают пространно рассуждать дилетанты и обыватели.

В Парадигмальном понимании, - основные носители информации это: источник информации и получатель. Получателю санкционировано получение информации и, согласно вида информации и границ санкции, получатель в дальнейшем может сам являться источником данной информации.

Если получение информации несанкционировано владельцем, (в частности, - источником, автором, разработчиком и т.д.), то получатель является нарушителем права собственности (авторских прав и пр.) - правонарушителем.

Вспомогательными носителями информации являются поля и вещества, через которые, и благодаря наличию которых, информация распространяется от источника к получателю. Если в числе них находятся преобразователи, то информация может распространяться носителями как полевого, так и вещественного вида, а также «преобразовываться» с одного в другой.

Например, акустическая волна сжатия и разрежения смеси химических веществ, находящихся в газообразном состоянии (т.е. - воздух), преобразуется микрофоном в изменение величины электрического тока (на участке цепи) или частоты колебательного LC-контура. Здесь в зависимости от носителя скорость распространения информации изменяется, примерно, от 330 м/с до 300000000 м/с. Такое изменение носителем-преобразователем скорости распространения информации называется качественным изменением параметра.

Где же здесь среда распространения информации? С Парадигмальной точки зрения термин «среда распространения» заменяется на термин «среда влияния». Это говорит о воздействии некоторых факторов окружающей среды на носители информации, в результате чего изменяются их параметры и характеристики. Например, если носитель информации – воздух, то при неравномерном изменении его плотности под влиянием солнечной радиации воздушная масса перемещается. Перемещающаяся в пространстве масса воздуха называется ветром, который оказывает на процесс распространения акустических волн влияние, отличающееся от влияния массы воздуха, находящейся в покое. Если воздух движется от получателя к источнику сообщения, то фронт акустической волны отклоняется от прямолинейного пути распространения и получатель может не услышать говорящего, хотя уровень затухания энергии звука не настолько велик, чтобы получатель не смог услышать источник сообщения. Также, акустические параметры воздуха изменяются под влиянием процентного содержания в нём тех или иных химических веществ.

И если в неживой природе о необходимости введения или сохранения термина «среда влияния» можно дискутировать, то в социуме такой термин вполне уместен и целесообразен. В обоих случаях информация подвергается угрозам нарушения её целостности, конфиденциальности и доступности к ней.

В отношении технических каналов утечки информации Парадигмальное определение этого термина устраняет идеалистические и пространные рассуждения о некоем физическом пути от источника к правонарушителю и становится конкретным:

«**Технический канал утечки информации** это паразитная (нежелательная) цепочка носителей информации, один или несколько из которых может быть правонарушителем или его техническим средством разведки».

Парадигма конкретизирует абстрактное представление о среде в следующей трактовке. Информация, в виде сигналов распространяется по цепочкам (последовательной, последовательно-параллельной и др.) носителей информации от источника к получателю. Среде (окружающей среде) отводится исключительно роль влияния на параметры носителей информации (рисунок 1).

Под действием факторов окружающей среды изменяются те или иные параметры носителя информации вплоть до видоизменения самого носителя. Например, H_2O: «пар – жидкость – лед».

Рис.1. Обобщенная структурная схема канала утечки информации

Под фактором понимается причина, движущая сила какого-либо процесса, явления, что определяет его характер или отдельные его черты. Окружающая среда включает естественную (природную) среду и искусственную (техногенную) среду. Таким образом, "среда это:

1. Вещество и/или поле, окружающие объект (в нашем случае, - окружающие носитель информации. – авт.).

2. Природные тела и явления, с которыми организм человека находится в прямых или непрямых взаимоотношениях.

3. Совокупность физических (природных), природно-антропогенных и социальных факторов жизни человека".

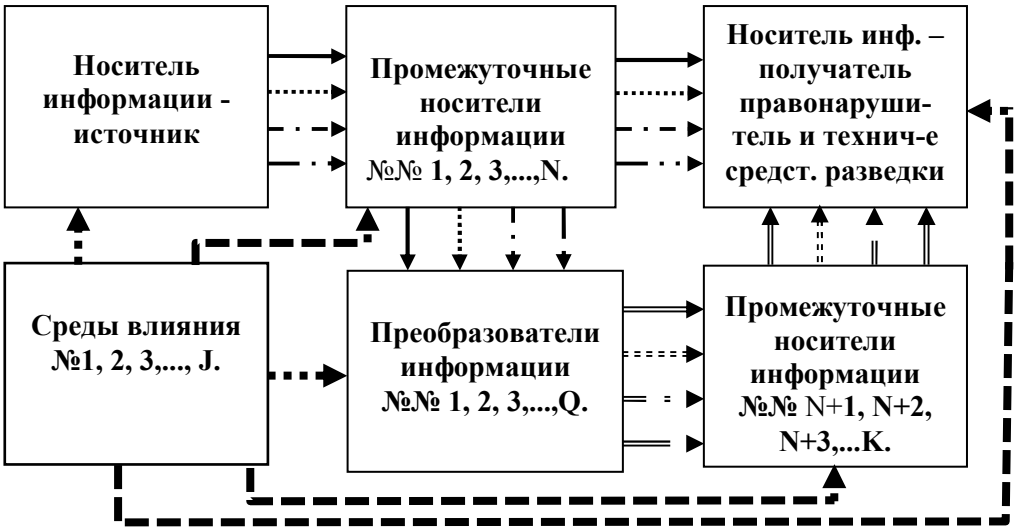

Рис.2. Структурная схема (вариант) ТКУИ

На структурной схеме технического канала утечки информации (рисунок 2) одинарными и двойными стрелками показаны направления распространения сигналов. Двойные стрелки - направления распространения сигналов после преобразования. Толстыми стрелками показано влияние факторов среды на параметры носителей информации.

Следует учесть, что приведен упрощенный вариант технического канала утечки информации, в котором не показаны обратные связи, наличие которых строго обосновано в научных трудах [17].

Таким образом, **процессом образования канала утечки информации** называется образование паразитной (нежелательной) последовательности (цепочки) носителей информации, один (или несколько) из которых может быть правонарушителем или его специальной аппаратурой.

7. Преобразование Парадигмы в «Общий закон защиты информации»

Из материала, приведенного выше, следует, что в первую очередь при создании систем защиты информации нужно предъявлять жёсткие требования к носителям. Они при перемещении информации должны обладать режимной адекватностью и коммуникабельностью. Смысл требований раскрыт в [4-10].

Рассмотрим, существует ли возможность расширения прав Парадигмы до уровня Общего закона защиты информации. Для этого сопоставим в Таблице 1 смысл термина «парадигма» и самого определения Парадигмы.

Табл.1. Определение «Парадигма» и её смысловое значение.

Термин «Парадигма» (энцикл.)	Определение в Парадигме.
Парадигма это исходная концептуальная схема, модель постановки проблем и их решения, методов исследования, господствующих в течении определенного исторического периода в научном сообществе [17].	Информация считается защищенной, если при её перемещении соблюдается режимная адекватность коммуникабельных носителей информации.

Следует отметить то, что для самого существования Парадигмы, как закона, необходимо наличие среды влияния - «научное сообщество» (наличие высокоинтеллектуального социума). Без этой среды влияния говорить о Парадигме бессмысленно.

В отличии от парадигмального значения, - законы свободны от этого недостатка. К примеру, «Закон всемирного тяготения» действителен всегда и не зависит от каких-либо дополнительных условий типа «наличие социума» и пр.

Вторая характерная особенность Парадигмы заключается в том, что она охватывает только процесс «перемещения информации». И если информация, к примеру, - на бумажном носителе, предназначена для длительного хранения и помещена в специальное хранилище, то действие Парадигмы распространяется исключительно до момента помещения носителя с информацией на полку хранилища. Далее можно рассуждать лишь о диффузии (под действием факторов среды влияния) молекул красителя, применённого в качестве чернил на листах бумаги, а также о замыслах и действиях такого носителя информации, как обслуживающий персонал хранилища.

В новой редакции Закона Украины «Про информацию» раскрыты виды информационной деятельности, исследуя которые мы можем сказать о том,

«находится ли информация в состоянии перемещения или её координаты и носитель не меняются в течение какого-либо промежутка времени».

Основными видами информационной деятельности является: создание, сбор, получение, хранение, использование, распространение, охрана и защита информации [2 - ст.9].

Следует отметить, что в отличии от формулировки закона, Парадигма допускает по отношению к информации такие расплывчатые рассуждения, как «какой-либо промежуток времени», «непродолжительно», «кратковременно» и пр. При трансформировании Парадигмы в закон, такой подход недопустим. Должна быть конкретизация по времени, либо сопоставление (сравнение) с продолжительностью каких-либо процессов во время информационных взаимодействий носителей информации.

Под информационным взаимодействием двух и более носителей информации понимается процесс создания, передачи, приёма, преобразования и/или уничтожения информации, представленной в любой материальной форме (полевая, вещественная) и виде (символы, графика, анимация и пр.). При этом могут быть реализованы: обратная связь между носителями, запросно-ответная форма с использованием паролей, выбор вариантов содержания информации и режимов работы с ней и др.

Анализируя предложение «информация считается защищённой, если при её перемещении», определим, существуют ли случаи, когда информация не меняет свои координаты в пространстве (Таблица 2) [2].

Табл.2. Преимущественное состояние координат информации при осуществлении различных видов информационной деятельности.

Вид информационной деятельности	Изменение координат
Создание информации	Да.
Сбор информации	Да.
Получение информации	Да.
Хранение информации	Нет.
Использование информации	Да.
Распространение информации	Да.
Охрана информации	Нет.
Защита информации	Нет.

В некоторых случаях изменение координат информации может отличаться от состояния, приведенного в Таблице 2. Но это не отрицает факта возникновения ситуаций в процессе информационной деятельности, когда при хранении, охране и защите информации Парадигма частично не соответствует статическому состоянию координат нахождения информации и при возникновении таких ситуаций не исключены моменты, когда отсутствует необходимость в обязательном наличии среды влияния типа «научное сообщество».

Таким образом, преобразование Парадигмы до уровня, охватывающего те состояния, когда информация (а фактически, - её носитель) не меняет свои координаты, позволяет трансформировать её в закон защиты информации.

Для этого в формулировке Парадигмы необходимо исключить ограничения, сужающие диапазон распространения её влияния до уровня перемещающейся информации.

8. Выводы данного исследования и перспективы дальнейших исследований в данном направлении

1. Таким образом, без промежуточных рассуждений, логических и математических выкладок о статических и динамических процессах при информационных взаимодействиях носителей информации, формулировка «Общего закона защиты информации» выглядит следующим образом:

«ИНФОРМАЦИЯ СЧИТАЕТСЯ ЗАЩИЩЁННОЙ, ЕСЛИ ПРИ ОСУЩЕСТВЛЕНИИ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В ЦЕПЯХ ИНФОРМАЦИОННЫХ ВЗАИМОДЕЙСТВИЙ НОСИТЕЛЕЙ ИНФОРМАЦИИ СОБЛЮДАЕТСЯ РЕЖИМНАЯ АДЕКВАТНОСТЬ И КОММУНИКАБЕЛЬНОСТЬ».

2. Информационные взаимодействия носителей информации, как важный с точки зрения ТЗИ процесс, сопровождающийся созданием, передачей, приёмом, преобразованием и/или уничтожением информации, порождают необходимость их графического отображения на принципиально новых информационно-логических схемах, которые должны войти в комплект документации, при создании и аудите систем защиты информации на объектах информационной деятельности и пр.

ЛИТЕРАТУРА

1. Конституція України від 28 червня 1996 р. //Відомості Верховної Ради України. – 1996. - №30. – Ст. 141.
2. Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. - №48. – Ст. 650.
3. Скакун О.Ф. Теория государства и права/ О.Ф. Скакун // Учебник. – Харьков: Консум; Ун-т внутр. дел, 2000. – 704 с.
4. Громыко И.А. Общая парадигма защиты информации / П.И. Орлов, И.А.Громыко, В.В.Носов, Н.Ф. Логвиненко, Е. И. Громыко // Збірник "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. НТУУ "КПІ". - 2002. - №5. - С. 84-86.
5. Громико І.О. Загальна парадигма захисту інформації / І. О. Громико // В науково-практичному посібнику «Інформація та інформатизація». 2-е видання, доп. й перероб. – Харків: Вид-во. НУВС, 2003 р. - 724 с.
6. Орлов П.И., Громыко И.А., Носов В.В., Логвиненко Н.Ф., Громыко Е.И. Общая парадигма защиты информации // Конфидент.- 2003 - №1 (49).- с. 14-26.
7. Громико І.О. Загальна парадигма захисту інформації: визначення термінів від носіїв до каналів витоку інформації. / І.О.Громико // . Вид-во ХУПС, - Вип.9. – 2007р.

8. Громико И.А. Общая парадигма защиты информации. Определение терминов от носителей до каналов утечки информации/ И.А. Громыко // Информ.-метод. журнал. Защита информации ІНСАЙД.–2008.-№1. - с.12-18.
9. Громико І.О. Загальна парадигма захисту інформації: визначення термінів. / І.О.Громико // НТТУ "КПІ".- Вип. 2. – 2007р.
10. Громико І.О. Визначення середовища поширення інформації та технічних каналів витоку/ І.О.Громико //Системи обробки інформації. – 2009. – Вип.. 7(79). – с. 16-19.
11. Department of defense standard. Trusted computer system evaluation criteria. National Security Institute - 5200.28-STD. December 1985. 116p.
12. Громыко И.А. Будущее за упреждающими системами защиты/ И.А. Громыко, С.Ю. Кильмаев, Е.Я. Оспищев // Защита информации. INSIDE. – 2007.- №2 (14) март-апрель 2007 г. – с. 14 – 18.
13. Громико І.О. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам / І.О. Громико, Т.І. Саханчук // Право України. - 2008. - №8. - с.130 – 134.
14. Шивдяков Л.А. Проблемы обеспечения информационной безопасности в ключевых системах информационной структуры органов государственного управления. Модель угроз безопасности информации в КСИИ/ Л.А. Шивдяков // Ж-л "Безопасность информационных технологий" №1 МОН РФ - 2008 - С.107 111.
15. Шивдяков Л.А. Проблемы обеспечения информационной безопасности в ключевых системах информационной структуры органов государственного управления. Модель угроз безопасности информации в КСИИ/ Л.А.Шивдяков //Ж-л "Безопасность информационных технологий" №№ 2, 3 МОН РФ - 2009 - С.82-91.
16. Громико І.О. Інформаційна обумовленість адміністративних правопорушень / І. О.Громико, О. І. Громико // Право України. – 2008. - №12. – с. 52 – 58.
17. Общий закон защиты информации. Полный перечень источников информации. [Электронный ресурс].– Режим доступа: http://www.ex.ua/view_storage/600448122943
18. Громыко И.А. Общая парадигма защиты информации: носители и среда распространения информации/ И.А.Громыко // Системи обробки інформації. – Х.: ХУПС, 2012. – Том 2., Вип. 4 (102). – С. 23-26.
19. Нерсесян А.С. Інформаційний вимір результатів творчої діяльності та право інтелектуальної власності./ А.С. Нерсесян // Часопис Київського університету права. Проблеми права інтелектуальної власності. Вип.3 - 2011 р.- С. 201-205 [Електронний ресурс]. – Режим доступу: http://kul-lib.narod.ru/bibl.files/index-2011_3/201.pdf

Надійшла у першій редакції 03.11.2012, в останній – 01.12.2012.