Захист інформації

УДК 316.776:351.741:34:65.0128

И.А. Громыко

Харьковский национальный университет имени В.Н. Каразина, Харьков

ОБЩАЯ ПАРАДИГМА ЗАЩИТЫ ИНФОРМАЦИИ: НОСИТЕЛИ И СРЕДА РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ

В статье изложен новый подход к таким информационным терминам, как «носитель информации», «среда распространения» и «технический канал утечки информации», что позволяет устранить размытость и неоднозначность их трактовки при подготовке кадров для системы ТЗИ.

Ключевые слова: *информация, защита информации, носители информации, среда распространения, канал утечки информации.*

Введение

Подготовка, переподготовка и повышение квалификации кадров является неотъемлемым требованием, предъявляемым к высшим учебным заведениям Украины, как к субъектам системы технической защиты информации (ТЗИ) [1].

Постановка проблемы. Анализируя в течении 10 лет процесс получения теоретических базовых знаний обучаемыми (студентами, слушателями, курсантами и др.) в области ТЗИ можно заметить, что при переходе от школьной программы к изучению научных основ нормативно-правовых актов Украины в области ТЗИ, наблюдается некоторое снижение качества усвоения материала. Это выявляется в процессе опросов, выполнения контрольных - летучек, модульных контрольных работ, зачётов и даже экзаменов. Отлично успевающие студенты просто – напросто переходят к элементарной «зубрёжке» терминов и определений, оставляя «понимание физической сущности процессов «на потом»», причём для части остальных обучаемых эти знания остаются неким пробелом, который постепенно заполняется в процессе их трудовой деятельности.

Во время поиска и изучения причин такой ситуации выяснилось следующее. Выпускники физико-математических лицеев и колледжей, придя в аудитории высших учебных заведений, имеют за спиной багаж знаний профилирующих дисциплин, которые были сформированы и выкристаллизованы человечеством из интегрального многовекового сплетения жизненно важных наук. В этих дисциплинах установлены чёткие границы событий и причинно-следственных связей между ними. Термины и определения не размыты и следуют в логической последовательности один за другим, что нельзя сказать о некоторых существенно важных терминах и определениях системы ТЗИ. Это является одной из причин слабой усваимости данного материала.

Анализ последних исследований и публикаций. Рассмотрим в качестве примера пункты 3.3 и 3.4. Государственного стандарта Украины № 3396.0-96 «Защита информации. Техническая защита информации. Основные положения» [2].

Известны научные постулаты о том, что:

– любая информация (и открытая, и с ограниченным доступом – ИСОД) может существовать исключительно только на носителе информации (далее, носитель);

– информация и её носитель всегда материальны;

– материя существует в двух основных видах: поле(1), вещество (2).

Однако в пункте 3.3, выше упомянутого стандарта сказано, что носителями информации могут быть физические поля (1), химические вещества (2), которые создаются в процессе информационной деятельности, производства и эксплуатации продукции разного назначения и … сигналы (3).

Задаётся вполне резонный вопрос:

1. Если носители информации материальны и существуют как материя в двух видах, то о каком третьем виде материи – СИГНАЛЕ (3) говорится в ДСТУ 3396.0-96 пункт 3.3 ?».

Обучаемый, анализируя дальнейшее содержание ДСТУ 3396.0-96, находит, что в пункте 3.4 говорится о существующих линиях СИГНАЛизации, видимо созданных для прохождения через них СИГНАЛов, а пункт 4.1.3 сообщает, что есть каналы специального воздействия, в которых формируются СИГНАЛы с целью разрушения системы защиты или нарушения целостности информации. Воображение обучаемых из полученных сведений о СИГНАЛе может построить мысленно всё что-угодно. Но далеко не всегда это построение соответствует истине. Здесь как раз приходит на помощь преподаватель, и драгоценное учебное время расходуется отнюдь не на познание основ информационной безопасности. Ссылка на то, что у неправильно понимающих студентов слабый тезаурус,

как запас знаний предыдущих курсов обучения, здесь не принимается, так как после п. 3.3 в данном стандарте следует негативная информация показывающая образ СИГНАЛа, как «разрушителя информации».

Дальнейшее изучение стандартов из этой серии позволяет обучаемому найти в пункте 6.2 ДСТУ 3397.2-97 определение не сигнала, как такового, а информативного сигнала, но уже без разрушительных свойств: «Информативный сигнал – это … физическое поле и химическое вещество, содержащее информацию с ограниченным доступом» [3].

Если преподаватель не потратил время на ответ по первому вопросу обучаемого, то в аудитории поднимается рука и задаётся уже два вопроса:

1. Информативный сигнал это некая промежуточная форма материи, обладающая, как квантовый дуализм фотона, свойствами и поля, и вещества одновременно?

2. Информативные сигналы содержат только ИСОД или могут содержать в себе открытую информацию?

Здесь уместно напомнить, что речь идёт о государственном стандарте и:

- «термины, регламентированные в стандарте обязательны для применения во всех видах организационной и нормативной документации, а также для работ по стандартизации и рекомендованы для применения в справочной и учебно-методической литературе сферы ТЗИ;

– термины стандарта являются обязательными для использования предприятиями и учреждениями всех форм собственности и подчинения, гражданами – субъектами предпринимательской деятельности, министерствами (ведомствами), центральными и местными органами государственной исполнительной власти, воинскими частями всех воинских формирований, представительствами Украины за границей, которые владеют, используют и распоряжаются информацией, которая является государственной или другой, предусмотренной законом тайной или является конфиденциальной информацией, которая принадлежит государству» [2, 3].

Далее, в пункте 3.4 ДСТУ 3396.0-96 говорится о том, что «средой распространения 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 т.д.

У обучаемых возникают вопросы:

1. Среды делятся на техногенную и естественную (природную), а здесь всё перемешано. Почему?

2. Если взять обыкновенное письмо в бумажном конверте, то ЧТО(?) является здесь носителем информации, а ЧТО средой распространения информации?

3. Может являться носителем информации электрический ток? - Ведь из пункта 3.4 следует, что электрический ток не является носителем информации, а является лишь «частью» среды распространения этой информации, которая переносится неким полем, как мы знаем, - сквозь линии связи, заполненные электронами проводимости. Тогда, например, по логике следует, что на приёмном конце линии связи на подвижную катушку мембраны громкоговорителя воздействует сила, порождённая магнитными полями, которые в свою очередь порождены, не электрическим током, а неким полем и провода (проводники) здесь не нужны. Если же провода есть, то тогда электронам проводимости отводится роль некоего «катализатора» процесса преобразования этой совокупности полей. Как это связать с выводами из уравнений Максвелла?».

Понятно, что такое изложение физической сущности «носителей информации и сред распространения» требует от студентов глубоких специализированных знаний на университетском физико-математическом уровне, а изучение основополагающих документов области ТЗИ нужно отодвинуть на последний семестр обучения. Но ведь эти документы являются базовыми и с ознакомления с ними начинается процесс становления работника системы ТЗИ. И если в изложенных выше примерах есть сложности, которые можно разъяснить, то уникальная фраза из статьи 6 Закона Украины «О государственной тайне» далека от диалектических основ теории защиты информации: «…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 [4]. Видимо, ещё не всем известен тот факт, что информация существует только на носителях и в данном случае её нельзя отобрать в своё пользование у собственника без изъятия носителей.

В связи с этим, **целью статьи** является показ парадигмального подхода к трактовке некоторых терминов и определений в системе ТЗИ, что позволяет показать их чёткие границы и устранить неоднозначность их понимания обучаемыми.

Основная часть

Следует указать, что приведенное выше свободное обращение с терминами и определениями не обязательно может быть порождено низкой грамотностью авторов, редакторов или корректоров. При-

чина в том, что невозможность объяснения некоторых явлений иногда заставляет людей непродуманно применять термины или идеализировать ситуацию и искать причину в каких-либо потусторонних силах. Так было и в недалёком прошлом. Например, многие природные и техногенные явления, относимые человечеством к разряду мистических, в середине прошлого века были объяснены открытием такого носителя информации, как электромагнитные волны. Сейчас в 21-веке людей ждут новые открытия неизвестных ныне носителей. И поэтому, с научной точки зрения диалектического материализма, нужно корректно обращаться с текстами законов, гостов и других основополагающих документов. К примеру, неуместно применять такие фразы как «искра божья», «осенило», «чуйка (интуиция)» и пр.

Можно ещё привести множество примеров, когда статьи законов и стандартов не соответствуют как логической последовательности процессов, так и основам диалектического материализма. Не удивительно, что обучаемые видят, что имеют дело с построением прекрасного, надёжного здания государственной системы технической защиты информации на некотором нестабильном грунте-плывуне. Многие термины и определения расплывчаты и служат для людей, познающих основы информационной безопасности, некими логическими преградами на пути становления грамотного специалиста области ТЗИ.

Избежать этой ситуации позволяет подход к носителям информации и средам её распространения с точки зрения общей парадигмы защиты информации, которая гласит, что «***информация считается защищённой, если при её перемещении соблюдается режимная адекватность коммуникабельных носителей информации***» [5 – 8].

Общая парадигма защиты информации впервые была опубликована в Украине и России в 2002-2003 гг. Там же и было приведено определение термина «информация», как «***зафиксированное на носителе представление о предметах, процессах, событиях, природных явлениях и т.д.***». При этом в качестве носителя информации может выступать поле или вещество. В некоторых случаях в качестве носителя информации может рассматриваться человек [9].

Прошло не более 10 лет и в новой редакции Закона Украины «Про информацию» появилась новая трактовка термина «информация», как «***будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді***». Здесь сравнение с парадигмальной трактовкой термина «информация» показывает фактически полную синонимальность этих трактовок.

И если в данном случае мы имеем ситуацию с более или менее благополучным законодательным исходом, то с каналами утечки информации дело обстоит по-прежнему. Как и 20 лет назад о канале утечки информации говорят не конкретно, а вообще. Например, как о «потенциальных направлениях несанкционированного доступа к информации». Понятно, что для обывателя такая терминология наиболее усвояема и уместна, но она никак не пригодна для специалистов области ТЗИ.

Также, определение технического канала утечки информации в ДСТУ 3396.2-97, как «***совокупности носителя информации, среды его распространения и средства технической разведки***», в какой-то степени приближено к правильному пониманию процесса на физическом уровне. Но оно несколько отдалено от основных задач, которые решают работники системы ТЗИ в процессе выполнения служебных обязанностей.

В парадигмальном понимании, - носители информации (поле и/или вещество) делятся на два класса (типа): основные и вспомогательные (дополнительные, промежуточные).

Если рассмотреть канал связи, то 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 несанкционированно владельцем, (в частности, источником, автором), 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 в канале связи от источника к получателю. Если в числе промежуточных носителей информации находятся преобразователи, то информация может распространяться носителями как полевого, так и вещественного вида, а также «перемещаться» с одного на другой. Например, акустическая волна сжатия и разрежения смеси химических веществ, находящихся в газообразном состоянии (воздух), преобразуется микрофоном в изменение величины электрического тока на участке цепи или частоты колебательного LC-контура. И здесь в зависимости от носителя скорость распространения информации изменяется, примерно, от 330 м/с до 300000000 м/с. Такое изменение скорости распространения информации носителем-преобразователем в парадигме называется качественным изменением параметра.

Где же здесь среда распространения информации? С парадигмальной точки зрения термин «среда распространения» заменяется на термин «среда влияния», что говорит о воздействии некоторых элементов 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. Например, водорода, воды и т.д.

И если в неживой природе о необходимости введения или сохранения термина «среда влияния» можно ещё спорить, 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 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 техническим средством разведки».

Вывод

Учитывая, что надуманные в ДСТУ 3396.0-96 «среды распространения» носителей информации на практике реально представляют собой последовательные, параллельно - последовательные и параллельные цепочки вспомогательных носителей информации, через которые в процессе информационной деятельности перемещается информация, необходима на государственном уровне разработка реестра носителей информации. При этом в паспорт каждого носителя информации должны вноситься сведения о его **коммуникабельности** в различных **режимах** применения (эксплуатации, работы, хранения, его защиты и пр.).

Список литературы.

1. Указ Президента України "Про Положення Про технічний захист інформації" № 1229/99 від 27 вересня 1999 року // Офіційний вісник України. - 1999. - №39. - Ст. 1934.

2. Державний стандарт України № 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення".

3. Державний стандарт України № 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення."

4. Закон України «Про державну таємницю» від 21 січня 1994 р. № 3855-XII // Відомості Верховної Ради (ВВР), 1994, N 16, ст.93.

5. Общая парадигма защиты информации / П. Орлов, И. Громико, В. Носов, Н. Логвиненко, Е. Громико // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – К.: НТУУ "КПІ", 2002. – № 5. – С. 84 – 86.

6. Громыко И.А. Общая парадигма защиты информации / И.А. Громыко // 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 // Системи обробки інформації. – Х.: ХУПС, 2006. – Вип. 9 (58). – С. 3 – 9.

8. Громыко И.А. Общая парадигма защиты информации. Определение терминов от носителей до каналов утечки информации / И.А. Громыко // Защита информации. – 2008. – № 1. – С. 12 – 18.

9. Нормативный документ ТЗИ 1.1 – 002 – 99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. Нормативный документ ДСТЗИ СБ Украины. Киев, 1999 г.

Поступила в редколлегию 14.05.2015

Рецензент: д-р экон. наук, доц. С.В. Кавун, Харьковский институт банковского дела Университета банковского дела НБУ (Київ), Харьков.

ЗАГАЛЬНА ПАРАДИГМА ЗАХИСТУ ІНФОРМАЦІЇ: НОСІЇ ТА СЕРЕДОВИЩЕ ПОШИРЕННЯ ІНФОРМАЦІЇ

І.А. Громико

У статті викладено новий підхід до таких інформаційних термінів, як «носій інформації», «середовище поширення» і «технічний канал витоку інформації», що дозволяє усунути розмитість і неоднозначність їх трактування при підготовці кадрів для системи ТЗІ.

Ключові слова: *інформація, захист інформації, носії інформації, середовище поширення, канал витоку інформації.*

GENERAL PARADIGM OF INFORMATION PROTECTION: STORAGES AND INFORMATION DISTRIBUTION MEDIUM

I.A. Gromyko

The article describes a new approach to information terms such as "information storage", "distribution medium" and "technical channel of information leakage" that can eliminate fuzziness and ambiguity of their interpretation by personnel training of technical information protection system.

Keywords: *information, data protection, information storage, distribution medium, the information leakage channel.*