УДК 316.324.8:004

А.И. Куляница
кандидат технических наук, ведущий научный сотрудник Научно-исследовательского института Министерства обороны Украины

О.В. Коломиец
кандидат политических наук, старший научный сотрудник Научно-исследовательского института Министерства обороны Украины

ПАРАДИГМЫ ИНФОРМАЦИОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЦИВИЛИЗАЦИИ

В статье рассматриваются особенности безопасности человеческой цивилизации в третьем тысячелетии. Предложен новый информациологический подход к рассмотрению понятия «безопасность».

Ключевые слова: безопасность, цивилизация, информациология, глобальные информационные системы, теория графов.

Катастрофические события в США в сентябре 2001 года повергли в шок весь мир, напомнив человечеству об обратной стороне технического прогресса. Разрушительные террористические акты, сделанные группой террористов-смертников в Нью-Йорке и Вашингтоне, стали суровым испытанием для всего американского общества. Мир узнал, что США не самая безопасная страна в мире. Почти десять дет Пентагон и НАТО стараются взять реванш в битве с международным исламским терроризмом в горах Афганистана, но на повестке дня возникает вопрос безопасности информационных технологий.

Практически все сферы деятельности человека, в которых применяются информационные технологии, стали зависимые от

их составляющих (байтов, чипов, модемов). Во многих развитых странах сегодня реализована концепция так называемого „электронного управления”. Вместе с тем, далеко не все страны и народы внедряют новый „цифровой” порядок; высокие технологии для многих просто недосягаемые и миллионы голодных людей вообще не знают о том, что есть спутники, персональные компьютеры и Internet.

В ходе расследования террористических актов 11 сентября ФБР установило, что камикадзе готовились к терроризму с помощью доступных программ, имитирующих полет самолета над Нью-Йорком и Вашингтоном, а для передачи инструкций в процессе подготовки и планирования террористической операции по управлению самолетом – электронную почту Internet. Разрушение комплекса домов только в Нью-Йорке, кроме человеческих жертв вызвало за собой закрытие биржи, падение курса акций, потерю десятка тысяч каналов передачи данных, перегрузка трафика в Internet, уничтожение информации в компьютерах сотен фирм и офисов [1].

Для того чтобы лучше осознать масштабы распространения информационных технологий в современном обществе и степень его технологической уязвимости, обратимся к опыту США – страны, откуда пришли высокие технологии вместе с новыми проблемами. США после распада СССР на протяжении последних десяти лет крепко занимают место лидера со статусом мировой сверхдержавы. На земном шаре нет ни одного уголка, который не попадал бы в сферу американских национальных интересов.

Но сегодня американцы целиком реально могут стать жертвами «кибернетического» Перл-Харбора, для подготовки и осуществления которого агрессору не понадобятся, как это было в прошлом, ни ракеты, ни самолеты, ни атомная бомба. Буквально в считанные минуты страна может оказаться парализованной, а через несколько часов стать ареной ужасающих по своим следствиям беспорядком среди населения.

Это все – сценарий Пентагона, американского военного ведомства, в коридорах которого уже более 10 лет разрабатывают возможные сценарии информационной войны, которая нависла над США после войны в Персидском заливе.

За несколько недель до начала ведения боевых действий, специально обученные агенты ЦРУ с помощью портативных компьютеров в Багдаде внедрили программные «вируса-закладки», что в предназначенный день и час отключили телефонные станции и радиолокационные средства, парализовав уже в первые часы ведения боевых действий систему ПВО Ирака. Есть сведения, что истребители „Мираж" иракских ВВС по этой же причине не могли использовать свои бортовые РЛС в ходе отражения налета. Это позволило союзной авиации в первые несколько часов уничтожить основные объекты иракской системы ПВО и через 10 дней завоевать преимущество в воздухе.

Несмотря на то, что еще в начале 90-х годов XX века было принято решение о создании специальных резервных информационных центров в каждом штате на период чрезвычайных ситуаций (аварий, катастроф, стихийных бедствий, террористических актов), власти Нью-Йорка оказались не готовы к такому развитию событий, которые вызвали за собой потерю информации в сфере социального обеспечения, при этом десятки тысяч малообеспеченных, инвалидов и старых оказались в первые недели без пособий. Власти вынуждены были пойти на беспрецедентные меры, обратившись с помощью к добровольцам по сбору, обработке и накоплению утраченной информации. В Конгрессе рассматривается законопроект о создании "национальной сетевой гвардии" (National Emergency Technology Guard), в задачу которой и будет входить предоставление помощи правительства в восстановлении информационных ресурсов в кризисных ситуациях [2].

Незадолго до описываемых событий ученые и специалисты Северной Америки начали бить тревогу по поводу непредсказуемости последствий кризисных ситуаций, связанных с масштабными техногенными катастрофами на объектах инфраструктуры. Суть этой проблемы заключается в том, что сегодня в США практически отсутствует национальный план не только информационных, но и коммуникаций вообще, что становится важнейшим критерием оценки состояния бизнеса, государства, общества.

Наиболее сложным моментом в этой концепции есть определения границ системы как совокупности обычных во времени и пространстве сетевых топологических структур. При этом изначально функционально несвязанные элементы этих структур на каком-то этапе своего развития становятся косвенно зависимыми и при определенных обстоятельствах образуют причинно-следственные цепочки потенциальных техногенных катастроф.

В данное время в США вводится в жизнь государственная программа аудита (учета) всех видов коммуникаций с целью построения многоуровневой топологической модели и определение на ее основе критически важных объектов инфраструктуры, их взаимосвязи с точки зрения прогнозирования характера и степени потенциальных угроз для безопасности общества и государства в целом [3].

С началом массового распространения доступных в цене персональных компьютеров с сетевыми операционными системами начала ухудшаться ситуация с информационной безопасностью. Лавинообразный рост числа локальных сетей и пользователей Internet, среди которых появилось немало авантюристов, хулиганов и преступников, стимулировал поиск новых методов борьбы со взломщиками (хакерами) информационных ресурсов. В связи с активным внедрением доступа к распределенным базам данных по технологии «клиент-сервер» появились операционные системы с

многоуровневой защитой от несанкционированного доступа, начинают широко использоваться методы криптографии для шифрования транзакций, внедряются интеллектуальные аппаратные средства блокирования подключения устройств.

В 1995 году в открытой печати появляются первые газетные и журнальные публикации, в которых проблема информационной безопасности приобретает своего близнеца и антипода – концепцию информационного противоборства и информационной войны.

Новая, сетецентричная (network-centric) парадигма информационной безопасности как концептуальная схема (модель) постановки и решение проблемы вытекает, прежде всего, из повышенных требований к живучести информационных систем, которые характеризуются высокой степенью распределения ресурсов (обслуживанием, логикой, программным и аппаратным обеспечениям, телекоммуникациями) и практически полным отсутствием централизованного управления.

Получив в настоящее время в США концептуальную модель эшелонированной многослойной системы информационной безопасности, национального стандарта ISO/IEC 15408, разработанного в коридорах Пентагона, содержит в себе набор компонентов, которые реализуют функции мониторинга, защиты и адаптации информационных ресурсов, которые в совокупности разрешают поэтапно предотвратить проникновение, найти факт нарушения, локализовать объект влияния, нейтрализовать и удалить нарушителя, восстановить утраченные функции системы [4].

В целом обеспечение информационной безопасности сегодня содержит в себе такие понятия, как целостность (integrity) информации, конфиденциальность (confidentiality) и защищенность от несанкционированного доступа (authentication, non-repudiation) и обеспечение надежности (availability) функционирования системы. Мировой опыт показывает, что эта

задача наболее эффективно решается с помощью методов криптографии в соединении с использованием проверенного и лицензированного программного обеспечения, а также надежными интеллектуальными носителями ключевой информации [5].

В свою очередь, понятие живучести (survivability) системы предполагает ее способность своевременно выполнять свои функции в условиях действия дестабилизирующих факторов (физическое разрушение, частичная потеря ресурсов, отказ и сбой элементов, несанкционированное вмешательство в контур управления). При этом техническая надежность, которая как способность системы работать на заданном отрезке времени в штатной ситуации без отказов, определяет минимальный порог стойкости системы, за которым без наличия системы восстановления утраченных элементов и функций может наступить катастрофа. Итак, живучесть информационных систем имеет определяющее значение для информационной безопасности в целом.

Эффективность такой концепции защиты государственных и коммерческих информационных систем определяет безопасность инфраструктуры государства в целом, а живучесть этих систем – мобилизационную готовность вооруженных сил, промышленности, экономики, народного хозяйства и общества в целом, как к ведению войны, так и к ликвидации последствий террористических актов, стихийных бедствий и техногенных катастроф.

Системы безопасности будущего должны не только и не столько ограничивать допуск пользователей к программам и данным, сколько определять и делегировать их полномочия в корпоративном выполнении заданий, обнаруживать аномальное использование ресурсов, прогнозировать аварийные ситуации и устранять их следствия, гибко адаптируя структуру в условиях отказов, частичной или полной потери продолжительного блокирования ресурсов.

Анализ рассмотренных концепций базируется на научных трудах и публикациях 90-х годов XX столетия русского ученого Юзвишина И.И., который является основателем научного направления – информациология. Философская глубина его концепций информациологической безопасности охватывает комплексную проблему безопасности эволюции земной цивилизации, последствия для неё вследствие нарушения законов информациологии и прогнозирование её процветания при разумном использовании ноотехнологий информациологического развития [6].

Основными принципами, предшествующими и сопутствующими информатизации общества, являются: гуманизация процесса информатизации; сознание не только должно определять бытие, но и должно намного его опережать; экономия материальных и трудовых ресурсов за счет развития информационных; недопущение ядерной и экологической катастрофы – страшной угрозы выживанию человеческой цивилизации; демилитаризация общества; каждый человек должен как бы войти в единое информационное пространство, познавая его информационные процессы, самому участвовать в этих процессах, выполняя свои ежедневные задания [5].

Следует отметить, что многие страны уже значительно продвинулись в направлении создания информационно-сотового общества. Деньгами как таковыми они почти не оперируют, а лишь информационно-кредитными карточками. Тем самым повышается уровень гуманизации общества как первой ступени информатизации и более чем на порядок уменьшается количество краж и других негативных явлений. Заменив информационно-кредитными карточками деньги, сокращая количество денежных банков, некоторые страны параллельно создают информационные банки, их сети и телекоммуникации, вступив на путь создания еще более совершенного постинформационно-сотового интеллектуального (ноосферного) общества [7].

Понятие глобальных информационных сетей (ГИС) вошло в общественно-научный обиход на волне глобализации в 90-е годы, когда процесс формирования центров глобального управления в отдельных сферах человеческой деятельности, в первую очередь, в сфере информации и коммуникации, стал очевидным и начала формироваться американоцентричность в системе отношений между цивилизациями. Слово «сети» отражает разветвленную вширь и вглубь техногенно-институциональную инфраструктуру международных информационных институтов, как бы опутавших планету [8].

Глобальные информационные сети как объект научного исследования относятся к категории так называемых искусственных неорганических систем, выявление сущностного содержания которых требует проведения междисциплинарных исследований. В междисциплинарных исследованиях наука, как правило, сталкивается с такими сложными системными объектами, которые в отдельных дисциплинах зачастую изучаются лишь фрагментарно, а поэтому эффекты их системности могут вообще не обнаруживаться при узкодисциплинарном подходе, а выявляться только при синтезе фундаментальных и прикладных задач в проблемно ориентированном поиске.

Проблемно ориентированный поиск в исследовании сущности глобальных информационных сетей сводится к анализу цивилизационно-культурологического генезиса и на этой основе выявлению их политической сущности, имеющей не только научно-теоретическое, но и практическое значение, поскольку от ее понимания зависит политическая ориентация и общественное поведение больших масс людей в разных масштабах – партии или движения, этнической общности, национального государства, цивилизации, глобального сообщества [8].

В основе ГИС лежат три основных фактора: цивилизационно-культурологический, в рамках которого

проявляется особенность современного этапа мирового общественного развития, собственно глобализация; политический: формирование механизма глобального управления; техногенный фактор, сводящийся к формированию технической инфраструктуры ГИС на уровне современных технологий.

В наиболее общем плане ГИС является продуктом глобализации, частью её исторической «ткани». В связи с этим понимание исторической сущности ГИС, как и других отраслевых сетей, сводится к пониманию сути глобализации как всеобщей тенденции мирового общественного развития.

Главным аспектом в понимании сути глобализации является монетаризм, в эволюции которого отражена вся общественно-политическая и экономическая суть развития нашей цивилизации, являющейся по характеру монетаристской.

Дисгармония взаимовлияния цивилизации и окружающей среды на стадии формирования глобального капитала достигает максимальных пределов, критической точки, что максимально обостряет глобальные проблемы, главной из которых становится антагонизм цивилизация – природа, который объективно обусловливает императив смены модели глобального развития.

При этом основной эволюционный смысл этой смены заключается в восстановлении гармонии развития человеческой цивилизации и природной среды, выход их из режима взаимоуничтожения. Эта проблема в реалиях монетаристского мира нерешаема (в этом смысле патронируемая ООН концепция «устойчивого развития» изначально практически неэффективна и в историческом смысле малопродуктивна). Требуется смена эволюционной мотивации в Мировом общественном развитии, формирование которой будет проходить в направлении перехода от примата рационалистических ценностей, порожденного монетаризмом, к примату

традиционалистических ценностей, создающих условия восстановления гармонии во взаимоотношениях человека с природой. При этом формируется тенденция к смене монетаристской моновариантной модели мирового общественного развития на поливариантную модель, отдельные формы которой уже проявляются в настоящее время. Речь идет о киберпространстве, которое по своей цивилизационно-культурологической сути являет исторически первой формой глобального сообщества, альтернативой монетаристскому реальному миру. Киберпространство как исторически первая реальная форма ноосферы – пространства разума, проистекает из недр монетаризма и является его продуктом, перенимающим эволюционную эстафету.

В процессе эволюции земной цивилизации коэффициент информатизации отдельных государств и регионов значительно увеличивается. Запасы информациологического ресурса, а также развитие компьютерных и телекоммуникационных технологий позволили осуществить переход человечества к созданию искусственной цифровой цивилизации (ИЦЦ), которая в процессе своего развития становится главным атрибутом его существования [9].

Таким образом, наблюдается тенденция взаимозависимости интеллектуальной части человеческой цивилизации от ИЦЦ, которая приняла архитектуру всемирной сети Internet. Далее проанализируем системные информациологические особенности взаимодействия двух систем: человек – ИЦЦ. Поскольку система ИЦЦ эволюционно всё с большей мерой влияет на развитие ОЭФ человеческой цивилизации, то любые нарушения её функционирования могут привести к необратимым информациологическим процессам в развитии земной цивилизации. Глобальная зависимость развития промышленности, экономики, культуры, сельского хозяйства, медицины и т.д. от нормального функционирования интеллектуальной цифровой «монстры» (назовём её для

краткости просто Сеть), подтверждает опасения многих социологов, политологов, философов, информациологов и других ученых о том, что человеческой цивилизации наряду с такими другими катастрофами, как ядерная, экологическая, биологическая, угрожает и информациологическая катастрофа.

Какие катастрофы имеют высший приоритет и какое влияние они окажут на судьбу земной цивилизации трудно предугадать и спрогнозировать. Исходя из фундаментальной теории информациологии, разработанной русским ученым Юзвишиным И., авторам хотелось бы на основании материала, изложенного выше, попытаться обратить внимание на серьёзные последствия для человечества при возникновении информациологических катастроф.

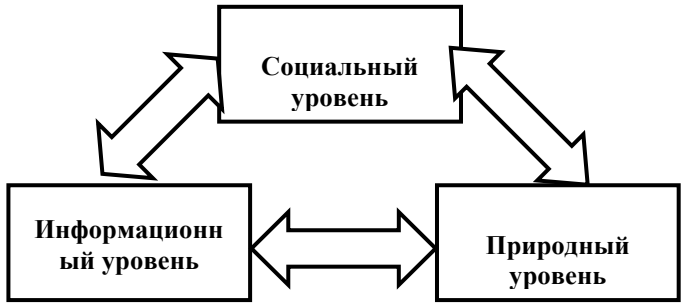

Рис. 1. Модель информациологической триады

На рис. 1 приведена модель информациологической триады, состоящая из трёх уровней: физико-химического (природный), информационного и социального. Информационные процессы трёх уровней диалектически дополняют друг друга, а также системно связаны между собой, например: физико-химические информационные процессы полупроводниковых приборов (первый уровень) составляют информационную основу для создания дискретных элементов информатики (второй уровень), которые, в свою очередь, создают информационные системы на основе компьютеров для

решения научно-технических и социальных задач общества (третий уровень).

Если в качестве информациологической модели рассматривать более простой неориентированный граф G (V,E) 3-го порядка и размера, изображенного на рисунке 2, то его можно будет математически описать с помощью хроматического полинома P (G,x) [10].

Используя лемму теоремы Брукса

$$P(G,x) = P(G_1,x) - P(G_2,x), \quad (1.1)$$

где граф G_1, полученный из G удалением ребра (u,v), а граф G_2 получается из графа G отождествлением вершин u и v.

Используя математический аппарат, найдем этот полином:

$$P(G,x) = x^3 - 3x^2 + 2x. \quad (1.2)$$

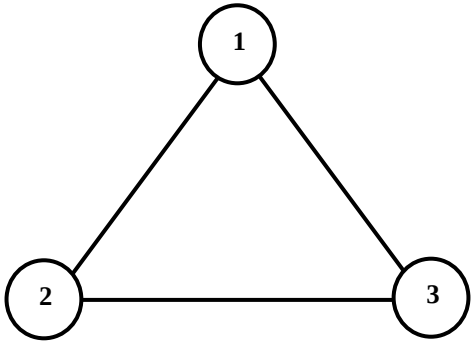

Рис. 2. Информациологическая модель в виде неориентированного графа

Найдем все 8 остовых подграфов графа G. Множество представим в виде трёх графов размера 1, т.е. с одним ребром, трёх графов размера 2, т.е. с двумя рёбрами и двух несобственных графов (пустой граф и граф G).

Учитывая, что ранг подграфа равен 2, получаем ранг-полином [10] рассматриваемого графа

$$P_v(x,y) = x^{3-0}y^0+3x^{3-1}y0+3x^{3-2}y^0+x^{3-3}y^0= x^3 + 3x^2 + 3x + 1. \quad (1.3)$$

Более высокие уровни информациологии созданы человеком в процессе его познания информационных процессов природы и окружающего мира. Соответственно, все три уровня связаны между собой информациологическими законами, которые подтверждают тезис о том, что информационные процессы происходят везде и информация есть основой живой и неживой природы, а также общества.

Литература

1. Гнесотто Николь. Сверхмилитаризация американской внешней политики // Internationale Politik. – 2002. – № 4. – С. 76–81.
2. Жуков В. Взгляды военного руководства США на методы ведения войны // Зарубежное военное обозрение. – 2001. – № 1. – 121 с.
3. Новые приоритеты в информационной безопасности США // Jet Info. – 2001. – № 10. – С. 11–17.
4. Гедмин Джеффри. Америка лидирует. Одна американская самооценка // Internationale Politik. – 2002. – № 4. – С. 6–11.
5. Пахомов Ю.М., Крымский С.Б., Павленко Ю.В. Пути и перепутья современной цивилизации. – К.: Междунар. деловой центр, 1998. – 432 с.
6. Юзвишин И.И. Информациология. – М.: Информациология, 1996. – 220 с.
7. Юзвишин И.И. Энциклопедия информациологии / Под ред. М.А. Прохорова. – М. : Информациология, 2000. – 467 с.
8. Глобальные тенденции развития человечества до 2015 года / пер. с англ. М. Леоновича. – Єкатеринбург : У-Фактория, 2002. – 120 с.
9. Коломиец В.Ф. Информациологическая эволюция и безопасность цивилизации. – К. : А-центр, 2005. – 184 с. : ил.

10. Кирсанов М.Н. Графы в Maple. Задачи, алгоритмы, программы. – М. : Издательство ФИЗМАТЛИТ, 2007. – 168 с.

This article is about peculiarities of human civilization security in the 21st century. A new informatiological approach to the consideration of "security" notion.

Key words: security, civilization, informatiology, global informational systems, graph theory.

У статті розглянуто особливості безпеки людської цивілізації у третьому тисячолітті. Запропоновано новий інформаціологічний підхід до розгляду поняття «безпеки».

Ключові слова: безпека, цивілізація, інформаціологія, глобальні інформаційні системи, теорія графів.