

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГЛОБАЛЬНЫХ СЕТЕЙ.

Сергей Дзюба, Евгений Ерофеев, Владимир Петров.

Как ни привлекателен тезис о беспредельности информационного пространства, производители и потребители информации почти всегда теряются в нем из-за неуправляемости многих информационно-энергетических процессов. Американцы в начале пятидесятих годов с целью управления глобальными разведывательными системами создали довольно громоздкое управление национальных оценок (ОНЕ). Вслед за ними японцы объявили информационно-интеллектуальный продукт товаром и весьма успешно прогрессируют в этой сфере. В целом мир задолго до Интернета стал не только объектом информационного переустройства, но и ареной информационных войн, которые наплодили огромное количество диверсионного оборудования и спецсредств электронной и комплексной атаки. И только к концу девяностых годов реально сформировался рынок комплексных средств безопасности (КСБ) информации. Таким образом, два совершенно различных сегмента рынка информационных технологий (ИТ): продуктовый и КСБ, - стали резко выделяться в общей схеме товарно-денежных отношений. Различные «секретки» уже не могут системно контролировать эти потоки, поэтому в начале нового века возникли корпоративные системы экспертизы и консалтинга по ИТ. Современное обеспечение защиты сетей можно представить таким образом:

Необходимо, чтобы системы и сети КСБ имели согласованную архитектуру;

Достаточно, чтобы все данные, находящиеся в системе и сетях КСБ, были защищены в соответствии с их степенью секретности и важностью для выполнения задачи;

Нужны гарантии защиты от отказов в работе всех сетей важных для выполнения и обеспечения задачи;

Следует сделать сети "прозрачными" для обеспечения безопасности и мониторинга;

Надо обеспечить проведение операций по реагированию и восстановлению работы систем и сетей после вторжения или других инцидентов в режиме ЧС;

Необходимо, чтобы инфраструктура не конфликтовала с сетями и системами других организаций;

Следует поддерживать гибкость линейных связей и быстрое реагирование на угрозы, вплоть до изменения стратегии.

Во вновь переизданной как учебное пособие нашей книге «Информационная безопасность России» (Москва, 2003) нами предлагается программа всеобуча по КСБ, которая теперь закреплена в «Методике информационной безопасности» (Москва, 2004). Она официально признана как основа организации государственной системы защиты информации. Нормативно-правовые, психологические и технические приемы ее обеспечения впервые открыты для широкого круга пользователей и общественности. Не зря Президент РФ Владимир Путин в этой связи потребовал создания общественной палаты независимых экспертов, в т.ч. и

по ИТ. Считаю нелишним напомнить, что информация каналов Интернет (анализ за 2003-2004) позволяет сделать вывод о дисбалансе затрат и результативности мероприятий по КСБ для тех же США. Действия китайских хакеров по отношению к беспроводным системам США, России, Японии и, особенно Индонезии и Австралии, явно опережают антитеррористические мероприятия в этой сфере всех национальных институтов по защите ИТ. Можно рассмотреть российский вариант. Практически все администрации субъектов федерации оснащены достаточными средствами защиты информации (защитные устройства - ЗУ). Существует четыре технологии, межсетевые экраны, криптографическая защита, активный аудит, виртуальная частная сеть (VPN). Тем не менее, все эти технологии дублируются бумажным документооборотом (почта, телефакс, фельдъегерская связь). В результате большой административный орган оказывается заведомо пораженным, тем более он не является экспертом в области защиты информации. На практике это выражается в отсутствии ответственности за принимаемые решения, девальвации конституционности и волюнтаризме местного руководства. Задача общественных палат как раз состоит в том, чтобы Президент имел четкие статистические выкладки по каналам быстрого реагирования по тем или иным действиям всех уровней управления государством. На возражения о тоталитарности такого контроля можно предложить следующее: мы все приватизировали в стране, кроме ответственности. Собственник ИТ - это, прежде всего, первое лицо государства. Президент единолично отвечает за интеллектуальный потенциал страны, правительство, народ. При нем должен существовать системный интегратор ИТ, тем более пять лет назад именно действующим Президентом была подписана Доктрина информационной безопасности России. Гостехкомиссия к настоящему моменту перестала ее сопровождать и превратилась, по сути, в сеть региональных коммерческих инспекций по ЭВТ. Мы полагаем, что через системный интегратор должно производиться трехуровневое обследование всех участников экономического и политического управления РФ, согласно Концепции «Защиты в глубину».

Во-первых - это анализ бизнес-процессов (информационные потоки документов, уровня конфиденциальности, аудит серверного парка и сетевого оборудования, проверка шифров входящей и исходящей информации).

Во-вторых - инфраструктурный уровень экспертиз (власть - бизнес, централизованные и муниципальные системы, антикоррупционные мероприятия в сфере принятия решений).

В-третьих - уровень корректив (приложений, исправлений всех видов информационных ошибок по ветвям власти и экономическим предпочтениям, корпоративным компенсациям в случае форс-мажора или террористических действий).

С учетом различного рода аномалий естественного (гео, космического) и техногенного характера сейчас приходится решать более сложные задачи КСБ -

энергоинформационная защита и подготовка человека к существованию в условиях глобализации интеллекта и корпоративности использования информации. Энергоинформационная безопасность базируется на исторически и тектонически сложившихся условиях формирования ноосферы, при которых человечество вплотную приблизилось к порогу самоуничтожения из-за неверного использования интеллекта. Технизм, в т.ч. энергоинформационный, привел к деградации души и духа, нивелированию ценностей и псевдопотребностям. Алчность властолюбцев поработила все страны и народы и антропогенно ведет их к информационному безумству. Энергоинформационные процессы подобно проникающей радиации имеют минимум преград, действуют избирательно, а, резонируя, способны разрушить любую аппаратуру и человека. Энергетика инициативы много меньше энергетики восприятия и этот мультиэффект пока еще не изучен в достаточной мере. Общеизвестны психофизические результаты такого действия на биосистемы, а клиника классических недугов непредсказуема. Освоение космоса, например, привело к тому, что низкоорбитальный «мусор» стая поражать не только ЭВТ, но и рефлекторные центры человеческого организма. СВЧ и КВЧ-излучения в настоящее время весьма популярны в период избирательных кампаний и нефтедолларовых акций. Они применялись и на украинском выборном «пяточке», когда энергоинформационные системы спутникового контроля «стянули» со всей страны и «отфильтровали» для «Площади незалежности» достаточную оранжевую массу манифестантов. Глобальная разведывательная сеть «Эшелон», используя и воздействуя на сотовую и радиорелейную связь, способна преобразовывать не только потоки информации, но и поля энергии. Кстати, джихад довольно успешно освоил технологии «возмездия», маркируя объекты нападения информационно-энергетическими матрицами. В мирных целях эта процедура сейчас используется для кодирования автомобилей сотрудниками дорожно-постовых служб. Таким образом, космическое энергоинформационное оружие «спустилось» на землю и приземленные функции КСБ, возможно, сгладят многие проблемы бытия.

Беспроводные антенные комплексы КВЧ в свою очередь также являются мишенью более мощных энергоинформационных систем. Здесь следует уточнить понятия информационно-энергетические - это в основном процессы, расчеты, решения; энергоинформационные - аппаратные комплексы, полевые структуры, материализованные проекты. Например, в случае с экономической безопасностью объекта, когда информация и энергия соединена таким образом, что чрезмерное наполнение фондов (потенции) зачастую приводит к тому, что утечка любого количества информации превращает объект в стратегическую цель. Так было с экономикой пятилеток, фондами СЭВ и теперь происходит с аналитическими центрами управления СНГ. Дело в том, что эти центры не защищены шифрами и не оборудованы в части таможенной, налоговой, бухгалтерской и других видов дисциплин.

Формализованные функции управления такими системами в своей сути не являются рыночными. Они традиционно указательно-распорядительны и не

рассчитаны на агрессию, присвоение информации, удержание интеллекта и, наконец, владение интеллектуальной собственностью. В России за последнее время создана «Академсеть» в составе проекта «Европейские математические сети» - EmNet. Президент РФ Владимир Путин распорядился об организации технопарков на базе ИТ-ВТ разработок отечественных ученых. Однако и здесь КСБ отводится не слишком много внимания. Правительство РФ настаивает на агрегатно-строительном способе формирования технопарков (ТП). Даже предлагаются варианты научно-технических и производственных решений. Мы считаем их не до конца корректными именно в части обеспечения КСБ. Аргументы следующие:

1. Ни один стационарный блок не может быть идеально защищен, так как он, во-первых - объект недвижимости, во-вторых - объект повышенных гео- и техногенных угроз в силу непредсказуемости последних. Геоаномалии по-прежнему, несмотря на множество предупредительных и экспериментальных мер, слабо изучены и проектировщиками зачастую просто игнорируются.
2. На сегодня совершенно несекретный комплекс защиты Москвы на Воробьевых горах бездействует и сам является источником энергоинформационных угроз, так как большинство его объемов представляют из себя вакуум-сферы, т.е. полигоны для вторжения и хранения любых энергетических концентраций, с последующим их распределением по команде извне. А ведь этот комплекс мог бы контролировать всю инфраструктуру подмосковных технопарков.
3. Нам представляется, что технопарки без указанных нами в Интернет инфодромов -специальных полигонов, мгновенно концентрирующих или распределяющих энергии, информацию по точкам сборки (ИТ-ВТ), в т.ч. под водой и в космосе, становятся малоподвижными технологическими монстрами, своего рода динозаврами. В нашем случае конечный продукт должен стать максимально недоступным, пока не станет собственностью России, а в ряде случаев и лично Президента.
4. Мы предлагаем использовать и соединить разработки по радиоэлектронике, нейрокомпьютерным системам и космоэнергетике в поляризованный комплекс, например, (Карелия - Приамурье) - два мощных блока (минуя Москву) по диагонали охватят основное стратегическое пространство России посредством инфодромов. Для этого необходимо особым распоряжением Перзидента РФ закрепить специальные территории за независимыми президентскими службами КСБ. Эти службы предложат от генплана до проекта детальной планировки систем информационно-энергетического обеспечения технопарков и спецзащиты глобальной инфраструктуры (ИТ-ВТ) в частотах блока Хутта и космоэнергетических программ академика В. Петрова. Возможно развитие треугольника (Карелия - юг России - Приморский край) с опорными базами в известных местах силы. Сочетание антенных (в режиме КВЧ) полей со структурами мест силы и космоэнергетической защитой этих объектов предполагает также

развитие и мониторинг контринформационных и блокирующих энергию средств защиты ноу-хау (ИТ-ВТ).

5. По матричному принципу (аналогично таблице Менделеева) возможно формирование Международного корпоративного портала (проект «Интерпартнер» - Александра Гроза). Правила вхождения и пользования информацией портала обеспечивают поуровневые потребности в ней с учетом карьеры менеджера-сетевика. Пятиуровневые системы одновременно являются достаточно защищенными от дезинформации, так как пользователи и производители модульной информации имеют ряд льгот и бонусов, которые стимулируют их карьерное развитие. Эта технология зафиксирована нами в Международном реестре глобальной информации и многочисленных авторских разработках. Практика показала, что в качестве одного из элементов КСБ, она с успехом может быть предложена и для технопарков. Сам Международный корпоративный портал (МКП) также может использоваться в качестве координационно - правохранительного инструмента в информационных процессах.

Основополагающим принципом в космоэнергетике является наличие частичного диапазона существования, как отдельных органов и тканей, так и всей энергоинформационной структуры организма в целом. Направленные изменения частотных характеристик - это и есть энергоинформационная сонастройка. Практическим путем удалось выяснить, что человеческая энергоинформационная структура способна воспринять не менее 6000 сонастроек в пределах диапазона жизнедеятельности, из них не менее 200 сонастроек уже имеют практическое применение в целительстве и в получении информации.

Конечно, многие из найденных сонастроек не являются уникальными и известны человеку уже давно и были доступны в результате других техник. Это еще раз подтверждает истину о том, что знание едино, разные только пути его достижения. Именно пути достижения знания и его передачи в новой системе доведены до совершенства, что говорит об актуальности космоэнергетики для современного общества. Вечно занятый вопросом собственного благосостояния современный человек вряд ли найдет время и желание для долгого аскетического ученичества.

Большинство недугов имеют отношение к низким частотным уровням. Поэтому смещение основных частот жизнедеятельности от грубых энергетических уровней к более тонким и информативным делает организм космоэнергетата вообще не восприимчивым к заболеваниям. При этом на продвинутых этапах может начинаться естественная деградация иммунной системы. Все недуги - закономерные явления, - это мощные факторы развития, призванные стимулировать переход от грубых материальных вибраций к тонким духовным.

Не только человек, но и любое живое существо, а также информационное поле неживых предметов и механизмов оказываются чувствительным к основным сонастройкам. Все это открывает для космоэнергетики поистине безграничные

возможности практического применения. Действительно, опытные космоэнергеты могут взаимодействовать с окружающим нас информационным полем, как живой, так и неживой природы, восстанавливать нарушения и искажения в нашей среде обитания. Это так называемая энергетическая чистка, которой может быть подвергнута и вода, и пища, и дома. Все это оздоравливает среду нашего обитания, восстанавливает естественный информационный баланс.

Возможность предупреждения заболеваний, повышение жизненного тонуса, восстановление сексуального либидо, решение проблемы депопуляций - это тоже вполне решаемые проблемы. Восстановление естественной энергетики размножения - только часть решения проблемы, другая часть — создание благоприятных энергоинформационных условий для развивающихся эмбрионов, обеспечение нормального течения беременности и роста ребенка. Имеющиеся в арсенале современной космоэнергетики средства позволяют значительно повысить жизнеспособность как эмбриона, так и матери. Если человек не может обойтись без внедрения технологий ЭКО и клонирования, то энергоинформационные биотехнологии могут помочь и здесь. Повышение жизнеспособности эмбриона только малая часть оказываемых на него воздействий.

Мы можем создавать здоровое полноценное потомство, контролируя этот процесс на всех стадиях онтогенеза, вернуть естественную энергетику всем процессам жизнедеятельности, особенно репродуктивным.

Новые технологии не имеют ограничений к применению:

Микробиология, вирусология, ветеринария, агрономия, зооинженерия. Человек сможет интенсифицировать сельскохозяйственное производство, восстановить численность природных эксплуатируемых популяций, подавить рост численности опасных болезнетворных микроорганизмов.

Подобные технологии уже нашли место в нашем обществе. Но социализация, подчинение космоэнергетики логике антиполя не идет ей на пользу. Космоэнергетика призвана менять природу человека и вместе с тем менять и гармонизировать наше общество. Это слишком мощное оружие, чтобы использовать его в рамках современного социума. Причина этого в низком уровне самосознания, ответственности и самоконтроля современного человека. Поэтому человек оказывается слишком слаб перед новыми безграничными возможностями, новые способности буквально сводит его с ума. Множество примеров подобного сумасшествия можно наблюдать на страницах современных рекламных сборников. Но это также является еще одним подтверждением того, какое мощное оружие оказалось в руках современного человека.

Современные энергоинформационные технологии - это шанс для человечества, возможность сгладить все негативные последствия технического прогресса, возможность подготовиться к катастрофическому изменению внешних условий. Космоэнергетика несёт для нас прогрессивные черты, которые всегда отбирались в

ходе эволюции Земли. Это увеличение энергоинформационного пространства жизнедеятельности.