УДК 004.056.5

Богданов А.М., Мохор В.В.

О КИБЕРБЕЗОПАСНОСТИ В ШИРОКОМ СМЫСЛЕ

Анотація:

У статті викладено позицію авторів відносно кібербезпеки як явища сучасного етапу розвитку інформаційного суспільства. При цьому зроблено спробу висвітлення різних аспектів вивчення даного поняття з метою визначення теми можливих дискусій.

Аннотация:

В статье излагается позиция авторов по отношению к кибербезопасности как явлению современного этапа развития информационного общества. При этом сделана попытка освещения различных аспектов изучения данного понятия с тем, чтобы наметить темы для возможных дискуссий.

Abstract:

The article contained the position of the authors regarding cybersecurity as a phenomenon of the present stage of development information society development. It attempts to highlight different aspects of this concept study in order to identify possible topics of discussion.

Актуальность

Временной период существования общества в плане применения в войнах и конфликтах оружия массового поражения может быть условно разделен на два этапа – до 2010 года и после него.

Первый этап характеризуется относительно «мягким» отношением к понятиям «кибероружие», «кибератака», «кибербезопасность» и т.п. Понятие «киберпространство» было введено писателями-фантастами в 1982 году для обозначения входившего в те годы в моду явления – общения людей с помощью компьютеров. Виртуальное пространство понималось как пространство, параллельное обыденному пространству жизни и общения людей.

Второй этап характеризуется появлением компьютерных боевых вирусов типа Stuxnet, Duqu, Flame, Gauss и им подобных. В середине июня 2010 года было обнаружено вторжение вируса Stuxnet в компьютеры иранской атомной станции в Бушере. Вирус состоит из двух частей: первая проникает в систему управления режимом работы центрифуг устройств обогащения урана, потенциально позволяя спровоцировать даже и взрыв этих устройств, а вторая в это время обеспечивает сигнализацию на все устройства контроля (вплоть до оператора станции), что все нормально, все элементы работают в заданных режимах. Величина ущерба, причиненного ядерным взрывом станции окружающей среде, становится соизмеримым с ущербом, который она получила бы при применении в отношении нее обычного ядерного оружия. Поэтому данный вирус можно обоснованно относить к оружию массового поражения.

Анализ рассмотренной ситуации привел к выводу, что Киберпространство – это уже не просто среда общения людей, игры («стрелялки», «догонялки»), хранилища знаний (библиотеки) и т.д. Киберсредства (кибероружие) – это самостоятельный вид вооружений,

способных нанести эффективный удар, сравнимый по результатам с ядерным ударом, и остаться при этом необнаруженным и невидимым для противника.

Другими словами, жизнь показала, что шутки с киберсредствами закончились, и необходим серьезный подход к их изучению. Показала жизнь и то, что сейчас в мире разворачивается настоящая гонка кибервооружений, поэтому промедление в изучении и разработке эффективных мер противодействия кибероружию – истинно «смерти подобно», говоря словами классика.

Последовательность исследований

Для качественно нового изучения кибероружия как новой реальности необходим, прежде всего, и новый качественный подход к нему. Имеющиеся на сегодняшний день представления и модели уже исчерпали себя. Они хорошо описывают киберпространство как пространство коммуникаций людей и технических средств, обмена видеоинформацией, научными данными. Но они не позволяют получить результаты при рассмотрении кибероружия именно как оружия поражения противника, нанесения ему существенного ущерба. Поэтому необходим новый взгляд на киберпространство и на работу в нем.

После разработки нового подхода к анализу киберпространства необходимо будет сконструировать его модель. Это может быть как общая модель, так и частные модели, отражающие специфику функционирования киберпространства в различных ситуациях. Например, стационарное состояние киберпространства, кибератака на киберпространство, защита от внешнего кибервоздействия и др.

После разработки моделей киберпространства, их исследования и оптимизации можно будет получить ответы на многие актуальные вопросы, которые стоят сегодня перед обществом.

Новый подход к изучению киберпространства

Из Википедии следует, что «Киберпространство» (англ. cyberspace) – метафорическая абстракция, используемая в философии и в компьютерах, является (виртуальной) реальностью, которая представляет Ноосферу / параллельный мир как «внутри» компьютеров так и «внутри» компьютерных сетей. Слово «киберпространство» (от кибер-нетика и пространство) в первый раз было введено Уильямом Гибсоном, канадским писателем-фантастом, в 1982 в его новелле «Сожжение Хром» («Burning Chrome») в журнале Омни. Потом оно было популяризировано в «Нейроманте» («Neuromancer»).

Введение этого понятия закрывало «белое пятно» в обозначении реальности, которая появлялась в то время в связи с бурным процессом разработки и внедрения компьютеров и была предвестником появления затем интернета. Но интернет и киберпространство – это не синонимы. Интернет входит в киберпространство своей технической составляющей и может, таким образом, рассматриваться как составляющая киберпространства.

Другая составляющая киберпространства определяется из представления его не как пространства общения, а как пространства точек принятия управленческих решений. Основной посыл здесь идет от перевода с древнегреческого языка слова «кибер» как «кормчий», то есть управитель кораблем (все гребут, а только один – рулит). Термин «кибернетика» (от др.-греч. **κυβερνητιχη**) использовался древними греками как искусство управления кораблем. Впоследствии его исследовал французский ученый А. Ампер [1], а потом через сто лет «вторично открыл» американец Н. Винер [2]. Именно он уже как бы в наше время назвал кибернетику наукой о связи в живых организмах и машинах. Наконец, со-

гласно Толковому словарю Ожегова [3], **КИБЕРНЕТИКА**: наука об общих закономерностях процессов управления и передачи информации в машинах, живых организмах и обществе.

Итак, киберпространство понимается в двух ипостасях:

1. Как пространство для общения технических средств типа компьютеров.

2. Как среда, в которой принимаются управленческие решения. Причем решения могут приниматься как людьми, так и механизмами.

Рассмотрим второе толкование понятия киберпространства (КП). При этом толковании КП состоит из множества точек, в которых принимаются решения о дальнейшем протекании процессов функционирования всего организма (машины) или его частей.

Такие точки могут быть у человека. Например, акупунктурные точки, при воздействии на которые с помощью иглоукалывания можно добиться остановки кровотечения или наоборот его провоцирования, устранения боли или же ее возникновения.

Точки могут быть в государстве, его хозяйстве. Они еще называются критическими элементами инфраструктуры. Это, например, атомные электростанции, Днепровский гидрокомплекс, объекты химической промышленности. При воздействии на эти точки можно значительно повлиять на ход процессов, протекающих в государстве с названием Украина.

Точки могут быть и в системе управления государством. Это так называемые «ЛПР» – лица, принимающие решения. Имеется в виду квалификация управляющих кадров, начиная с прораба и заканчивая президентом страны, а также нравственность, честность этих кадров. Воздействуя на эти точки, также можно серьезно влиять на протекание процессов в государстве.

Таким образом, киберпространство можно представлять как множество точек объекта, в которых принимаются решения о протекании в нем процессов, и при воздействии на которые можно управлять функционированием объекта.

Модель обработки информации объектом принятия решения

Под объектом принятия решения будем понимать как одушевленный объект (ЛПР), так и неодушевленный (автоматизированная система принятия решений). Рассмотрение начнем с одушевленного объекта, а неодушевленный проявится потом как частный случай.

Вопрос о модели восприятия, хранения, обработки и обмена информацией внутри человека, его психики рассмотрим с позиции Достаточно общей теории управления (ДОТУ), разработанной в русле Концепции общественной безопасности (КОБ) [4].

Психику человека в процессе обработки информации и принятия решения в первом приближении можно представить в виде системы из двух блоков – сознания и подсознания (рис. 1).

Прием информации и выдача решения осуществляется сознанием человека, а обработка информации – и сознанием, и подсознанием в комплексе. При этом можно говорить об аналогии такой модели с моделью персонального компьютера. Сознание человека отождествляют с оперативной памятью компьютера, подсознание – с жестким диском (винчестером), а алгоритмику обработки информации – с программным обеспечением. Прием и выдача информации осуществляется с помощью пяти органов чувств человека (слух, зрение, обоняние, осязание, вкус) аналогично датчикам входных устройств компьютера.

Шестое чувство (интуиция, жизненный опыт, предсказание, долговременная память) реализуется подсознанием. Седьмое чувство (воля, разум, различение «Да-Нет») опять же присуще сознанию человека.

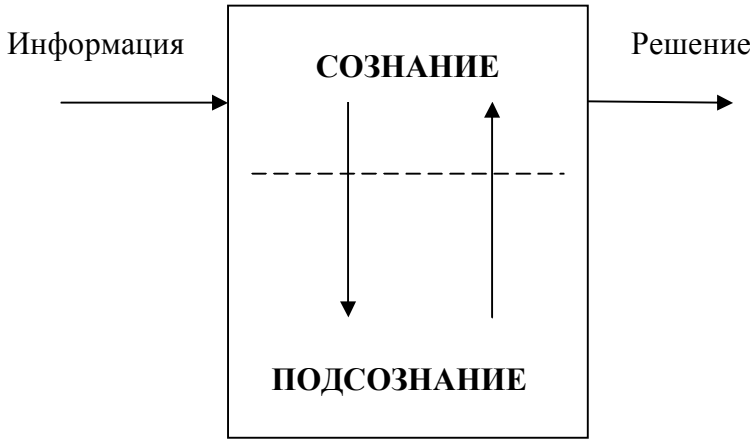

Рис. 1 Структура психики человека

Числовые характеристики обработки информации следующие. Сознание среднестатистического человека способно одновременно анализировать (принимать, выдавать, контролировать) эффективно не более 7-9 каналов информации со скоростью изменения данных в них не больше, чем 15 бит/с в каждом. В подсознании информация обрабатывается со скоростью сотен Мбит/с. Память подсознания практически бесконечна.

Процессы обработки информации в психике человека в некотором роде также аналогичны процессам обработки информации в компьютерах. По своей структуре эти процессы можно разбить на следующие группы:

– последовательные (рис. 2), когда входами одного процесса являются выходы предыдущего, а выходы в свою очередь являются входами для последующего процесса;

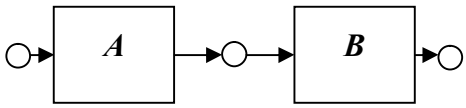

Рис. 2 Последовательные процессы

– параллельные (рис. 3), когда одна и та же входная информация обрабатывается параллельно в разных блоках, имеющих различные назначения. Например, информация об окружающем ландшафте параллельно обрабатывается в каналах слухового, зрительного, обонятельного, осязательного и вкусового восприятия;

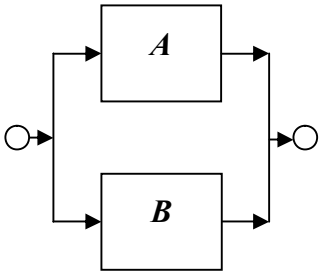

Рис. 3 Параллельные процессы

– условные процессы (рис. 4), которые разветвляются, содержат логические элементы типа «если ***A*** больше или равно ***M***, то надо идти в точку ***X***, а если ***A*** меньше ***M***, то надо идти в точку ***Y***». В этом случае величина ***M*** называется ***мерилом, мерою***, то есть характеристикою психики конкретного человека, которая показывает, по каким путям осуществляется им обработка информации и какое, в конце концов, будет принято решение.

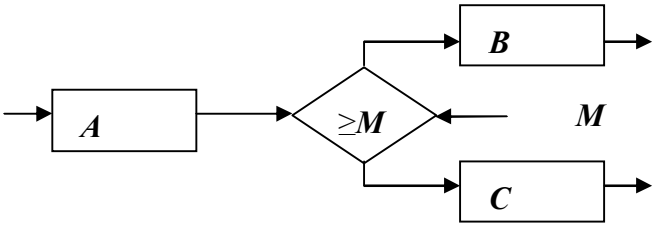

Рис. 4 Условные, ветвящиеся процессы

Величина ***M*** (а реально таких величин целое множество, для каждой точки разветвления психических процессов) является переменной для каждого человека. Она также изменяется в течение жизни человека в зависимости от разных условий. Определяется она **нравственностью** (этикой, совестью, моралью), которая, в свою очередь, зависит от воспитания: как генетического (наследственность от родителей), так и социального (школа, улица, коллектив, общественные идеи).

Что такое **нравственность**? Это бесконечно счетная таблица, в которой в левой части перечисляются различные ситуации (жизненные, технические и др.), а в правой – отношение человека к ним. В простейшем случае это «Хорошо-Плохо». Давайте вспомним стихотворение Владимира Маяковского: «Кроха-сын к отцу пришел и спросила кроха – что такое «хорошо» и что такое «плохо»? Оказывается, сын спрашивал у отца ответ на основной вопрос о смысле жизни!

Возможны ситуации, когда в правую часть таблицы нравственности добавляется еще один столбик – «все равно, по барабану». Тогда нравственность моделируется в троичном коде: «Да-Нет-Нейтрально». Можно определить, что когда нет ответа на какую-либо ситуацию, то это для данной ситуации считается аморальным.

Рассмотрим конкретный пример. Представим себе бизнесмена, который опаздывает на самолет, улетающий в город, где должен быть подписан очень выгодный контракт. Он мчится на автомобиле с огромной скоростью, так как до отлета самолета остаются считанные минуты и секунды. И вдруг на дорогу выбегает котенок! Что делать? Тормозить, спасти котенка, но не улететь? Или пожертвовать чужой жизнью (пускай даже и котенка), чтобы успеть к моменту подписания контракта всей своей жизни? Очевидно, разные люди поступят в данной ситуации по разному, и у каждого будет свое «железное» оправдание. Все будет зависеть от своего внутреннего Мерила.

Понятно, что, воздействуя на мерило человека, можно манипулировать процессом принятия им решения, а воздействуя на мерило целого народа, – поведением этого народа. Особенно эффективно воздействие на мерило лица, принимающего решения в государственном масштабе.

Порог принятия решений (мерило) изменяется в течение жизни человека. При его рождении это одни значения (много чего еще неизвестно, таблица нравственности почти не заполнена, заполнены лишь генетические графы). По мере взросления происходит из-

менение порогов и таблицы нравственности под воздействием окружающей среды. А в конце жизни имеют место уже третьи параметры. Например, если при рождении ребенок не хочет ни курить, ни употреблять алкоголь или наркотики, то в конце жизни этот же человек вполне может стать алкоголиком или наркоманом.

Таким образом, процессы обработки информации при принятии решений человеком в значительной степени определяются его личной таблицей нравственности, что может служить целью осуществления кибератак.

В технической автоматизированной системе принятия решений также можно выделить последовательные процессы обработки информации, параллельные и условные (ветвящиеся). Также можно определить пороговые значения параметров (в киберточках), определяющие дальнейший ход процесса принятия решения. Изменяя эти пороговые значения, возможно управлять системой, заставляя ее принимать нужные решения.

Немного о философии вопроса

Общепризнанным является факт, что современное общество становится информационным, приходя на смену обществу постиндустриальному. При этом по инерции мы пытаемся новые явления информационного общества описать и объяснить старыми понятиями и законами общества постиндустриального, материалистического в своей основе. Один из основных законов материи – закон о ее сохранении. То есть, если где-то прибыло, то где-то должно убыть. В отношении информации это не действует. Преподаватель передает знания учащимся, но при этом количество знаний у них увеличивается, а у него – не уменьшается! Эта нестыковка требует уяснения и исправления.

Одним из выходов может послужить переход от объяснения явлений Бытия в 4-хэлементном базисе «Материя-Энергия-Пространство-Время» (как это делается в материализме) к объяснению их в базисе 3-хмерном «Материя-Информация-Мера». Этот базис подробно рассмотрен в Концепции общественной безопасности (КОБ). С его помощью авторами было проанализировано понятие «Оружие массового поражения» [5] и получено новое, качественно более глубокое толкование этого понятия на современном этапе.

Согласно данной модели все Мироздание (Бытие) состоит из материальных объектов, которые могут обмениваться информацией в определенной мере, изменять в силу этого свое состояние, превращаясь в другие объекты. Все материальные объекты увязаны в многомерную многовариантную статистическую матрицу с различными вероятностями переходов ее в различные состояния. Материя для Информации представляет собой ее носитель. Информация для Материи – образ. Мера для Материи – вероятности переходов матрицы Бытия из одного состояния в другие. Мера для Информации – код, обозначение (включая языки общения людей). В этой системе сочетание «образ плюс его обозначение» – это «понятие», основная категория мыслительной деятельности человека. Совокупность понятий – это суждение, а совокупность суждений – это тезаурус имеющихся знаний.

Суть модели Материя-Информация-Мера поясняется на рис. 5.

Под углом зрения представленной модели были рассмотрены варианты современного оружия массового поражения. Для наглядности была смоделирована и проанализирована ситуация, когда Президент одной очень мощной мировой державы имеет возможность подкреплять свои политические амбиции с помощью нажатия на одну, условно говоря, из трех кнопок – «красную», «синюю» или «зеленую».

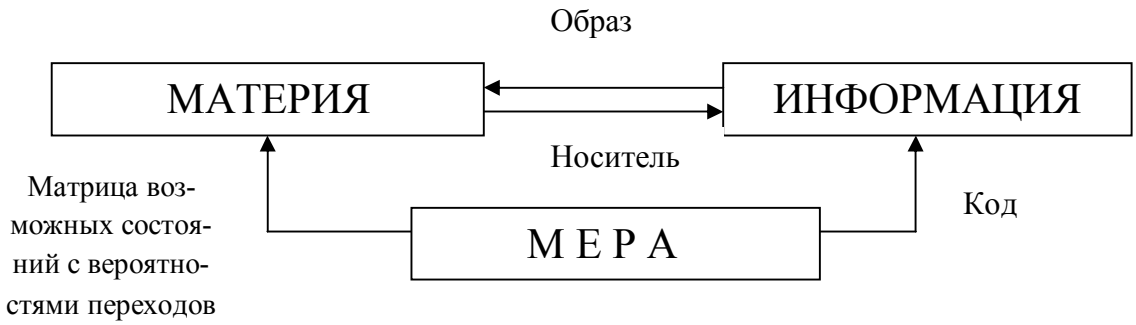

Рис. 5 Система координат Материя-Информация-Мера

При нажатии на «красную» кнопку отдается приказ о применении ядерного оружия в том или ином районе земного шара. При этом материальном воздействии уничтожаются материальные ресурсы противника, а именно – его живая сила и инфраструктура.

Нажатие «синей» кнопки приводит к отключению сети Интернет в том или ином регионе (или в мире в целом), пропаданию спутниковой и сотовой связи, а также активизации заложенных в различных компьютерных устройствах боевых вирусов. Таким образом, нажатие «синей» кнопки приводит к разрушению всех систем управления, нарушению процессов коммуникаций и всеобщему хаосу на территории противника.

Нажатие на «зеленую» кнопку означает, например, девальвацию какой-то валюты, региональной или мировой. Примерами последних лет могут служить:

а) девальвация белорусского «зайчика» в 2010–2011 годах. Это масштаб сравнительно небольшого региона;

б) девальвация и нестабильность евро в Европе. Это континентальный масштаб региона;

в) периодические угрозы Президента США девальвировать американский доллар, если конгресс США не примет определенные законы. Это уже мировой масштаб воздействия.

Таким образом, при нажатии на любую из кнопок Президент рассматриваемой в качестве примера державы может достигать своих политических целей как в отдельно взятом регионе Земли, так и в глобальном масштабе. В одних случаях это будет сопровождаться человеческими жертвами напрямую, а в других – опосредованно, например, по следующей цепи: «разрушение инфраструктуры – голод – бунты – хаос – ввод миротворческих сил для поддержания порядка». То есть, та же оккупация, но без явственных жертв людей.

Анализ приведенной ситуации с позиций системы Материя-Информация-Мера показал, что:

- информационное оружие (ИО) – это не подвид материального оружия, очередной этап его развития, а это – самостоятельный вид вооружений, основанный на своих принципах;
- по мощности воздействие ИО может быть сопоставимо как с пулей (воздействие на отдельного человека), так и с атомной бомбой (воздействие на целый народ);
- для защиты от ИО требуются средства индивидуальной защиты (типа информационных противогазов), информационные бомбоубежища (коллективные средства) и так

далее, вплоть до Государственного Комитета Информационной Обороны (по типу ГКО во время войны);

- требуется качественно новое изучение информационного оружия на основе качественно новых подходов и философских принципов.

Об информационной безопасности, кибербезопасности, их соотношении и взаимосвязи

Анализируя национальную безопасность (НБ) государства, ее составные части (в соответствии с Законом Украины «Про национальную безопасность»), мы разбиваем НБ на 9 составляющих так, как показано на рис. 6.

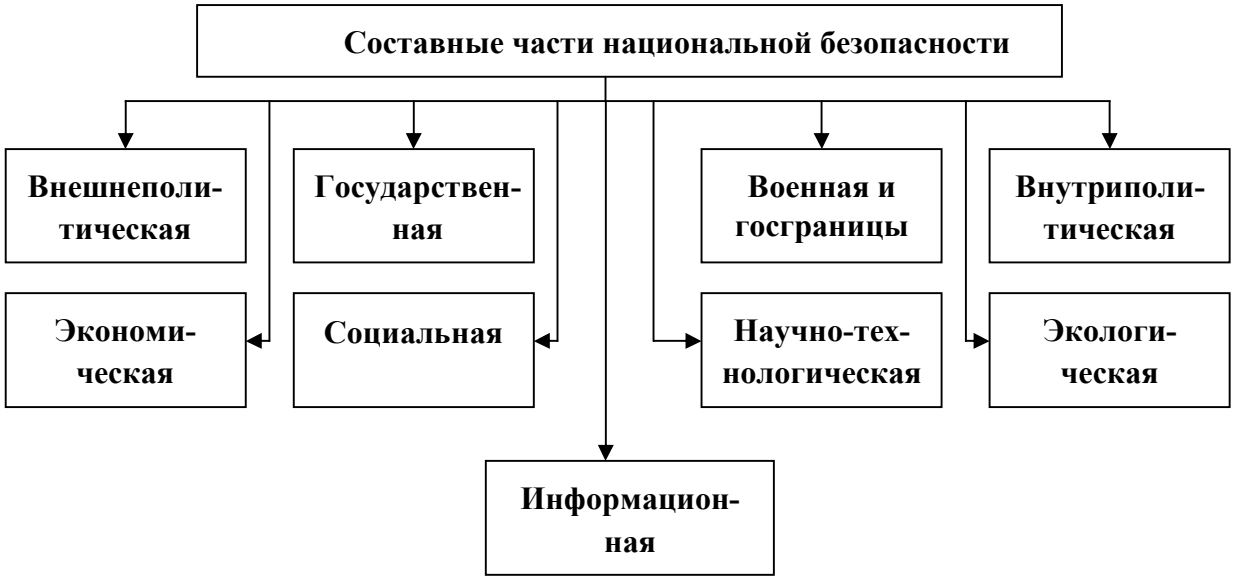

Рис. 6 Составные части национальной безопасности Украины

Вместе с тем, в соответствии с Доктриной информационной безопасности Украины [6] отмечаем, что «Информационная безопасность является неотъемлемой составной частью каждой из сфер национальной безопасности», то есть она пронизывает все остальные сферы национальной безопасности. Отсюда вытекает, что информационная безопасность сочетается с другими составляющими национальной безопасности в несколько ином виде, а именно так, как это представлено на рис. 7.

Таким образом, рис. 7 отражает роль и место информационной безопасности в составе национальной безопасности государства.

Аналогичным образом можно проанализировать понятие «информация». Согласно Закону Украины «Об информации» по содержанию различают следующие ее виды: информация, касающаяся физического лица (персональные данные), справочно-энциклопедическая информация, экологическая информация, информация о товарах и услугах, научно-техническая информация, налоговая, правовая, статистическая, социологическая и другая информация.

С одной стороны, информация относится к какой-то определенной области знаний о явлениях природы и общества. С другой стороны, в ее структуре имеются как описательные блоки, так и блоки, относящиеся к управлению в данной области. Например, едет человек на верблюде, что видит – о том поет. Что он видит – это просто описательная информация. Но, подъехав к перекрестку, человек должен решить, куда ехать дальше. А

здесь уже ему потребуется информация для принятия решения, т.е. «киберинформация». Итак, киберинформация – это информация для принятия решения (выбора, различения). Это управленческая часть информации вообще.

Рис. 7 Место информационной безопасности в системе национальной безопасности

Если принять, что применительно к некоторой сущности есть обычные элементы и связи, а также элементы и связи критические, при воздействии на которые можно управлять этой сущностью вплоть до ее уничтожения (физического или еще какого-либо, например, имиджевого), то и информацию об этой сущности можно разделить на части: общеописательную и управленческую. Последняя и будет киберинформацией для данной сущности. Воздействие на нее будет называться кибератакой, а защита этой жизненно важной части информации – киберзащитой. Условно такую модель можно изобразить на рис. 8.

Таким образом, киберинформация в предлагаемой модели является составной частью информации вообще. Ее объектами являются критические элементы инфраструктуры явления природы (живой и неживой) и общества, а также связи между ними. В случае общества, например, носителем киберинформации является лицо, принимающее решения.

Рассмотрим несколько примеров кибервоздействий на элементы природы (неживой, живой) и общества.

А. Неживая природа. Рассмотрим устройство автоматического освещения какого-нибудь двора. Имеется лампа, которая включается через автомат, состоящий из фотоэлемента, реле включения/выключения лампы и порогового устройства с регулятором, который определяет, при каких значениях тока через фотоэлемент (а этот ток зависит от степени освещенности фотоэлемента) лампа должна включаться и выключаться. В регуляторе имеется подстроечный резистор, который, в общем-то, и определяет режим работы всего устройства.

Рис. 8 Место киберинформации в структуре информации

В данном объекте элементом кибервойздействия является подстроечный резистор, а само кибервоздействие (управляющее воздействие – кибератака) может быть осуществлено методом изменения сопротивления резистора с помощью обычной отвертки. В итоге, в одном крайнем положении резистора света во дворе не будет вообще, а в другом – свет будет гореть постоянно. Выбирай требуемый режим и атакуй! А отвертка в данном случае – это элемент кибероружия.

Б. Живая природа. В качестве примера из живой природы можно рассмотреть тело человека как биологический организм. Существует процедура – акупунктура (от лат. *acus* – игла и лат. *punctura* – колоть, жалить) – при которой воздействие на организм осуществляется специальными иглами через особые точки на теле человека посредством введения их в эти точки и манипуляций ими. Киберпространство в данном случае представляет собой множество особых (критических) точек на теле человека, кибероружием являются специальные иглы, а кибервоздействие осуществляет доктор. Результатом его является изменение процессов функционирования организма, приводящее, например, к ослаблению боли в каком-нибудь органе.

В. Общество. Выше уже разбирался пример с бизнесменом, который в критической ситуации должен решать – давить котенка колесами своего автомобиля, или не давить? Вместо этого бизнесмена можно представить лицо, принимающее решения. Тогда в результате кибервоздействия решение «давить» или «не давить» (реально – вести подчиненный ему коллектив в ту или иную сторону) принимает не это лицо (хотя оно и думает, что именно оно решает), а некто, сформировавший порог (воздействием на нравственность) в системе принятия решений этим лицом такой, какой необходим для принятия им нужного решения. В этом случае кибервоздействием является сам процесс «обработки» нравственности ЛПР в нужном направлении до достижения заданных величин порогов принятия решений.

Образно рассуждая, можно заключить, что в крупном плане задача кибероружия – это заставить ЛПР задавить (или не задавить) котенка в нужный момент, не обращая внимания на то, хочется ему этого или нет.

Терминология

Известно, что о терминах не спорят, а договариваются.

В рассматриваемом контексте предполагается, что термины могут быть такими, которые описывают явление или в узком смысле, как среду общения и принятия решений в виртуальном мире (по типу Интернета), или же в широком смысле, когда задача кибервоздействия заключается в достижении такого состояния, когда объект воздействия функционирует и принимает решения так, как навязывает ему субъект воздействия. Мы рассмотрим второе определение. В тезисном представлении это будет выглядеть следующим образом.

1. Существуют критические элементы (точки) какого-нибудь явления. Это элементы, воздействуя на которые, можно влиять на протекание процессов внутри явления.
2. Критические элементы и связи между ними образуют специфическое пространство – киберпространство.
3. Кибервоздействие заключается в осуществлении влияния субъекта воздействия на объект воздействия через его критические элементы и связи.
4. Разновидности кибервоздействия различаются в зависимости от длительности и масштаба – кибератака, операция, война.
5. Существуют киберуязвимости объекта и система его киберзащиты, предназначенной для недопущения реализации киберугроз через киберуязвимости.
6. Возможные пути реализации киберугроз в отношении ЛПР – шантаж, подкуп, обман и др.

Таким образом, в киберпространстве субъект кибервоздействия осуществляет влияние на критические элементы и связи объекта кибервоздействия с целью перевода объекта в нужный ему режим функционирования. Влияние при этом может быть как явным, так и не явным. Примеры явного влияния – рейдерство (критическими элементами являются погрешности уставных документов компаний, другой компромат). Пример неявного влияния – финансовый «трюк» государства в 2008 году, когда населению Украины сначала опосредованно длительное время внушалось, что курс доллара будет падать с курса 5:1 до 3:1, а потом (после того, как население в это поверило и начало избавляться от валюты) произошло обратное явление – увеличение курса доллара более чем в два раза, до 12:1 с последующей стабилизацией на отметке 8:1.

Но в целом вопрос терминологии в рассматриваемой области еще далек от общепризнанных решений и требует дальнейшего обсуждения специалистами.

Моделирование кибервоздействия

Наконец, необходимо затронуть вопросы математического моделирования явления кибервоздействия и защиты от него. Остановимся на двух моделях – модели процесса воздействия и модели киберпространства.

Для построения модели воздействия воспользуемся математическим аппаратом теории исследования операций [7]. Основные положения этой теории следующие.

Операцией называется всякое мероприятие (система действий), объединенное единым замыслом и направленное к достижению какой-то цели. Операция есть всегда

управляемое мероприятие, то есть от нас зависит, каким способом выбрать некоторые параметры, характеризующие ее организацию. «Организация» здесь понимается в широком смысле слова, включая набор технических средств, применяемых в операции. Всякий определенный выбор зависящих от нас параметров называется **решением**. Решения могут быть удачными и неудачными, разумными и неразумными. **Оптимальными** называются решения, по тем или иным признакам предпочтительные перед другими. Цель исследования операций – предварительное количественное обоснование оптимальных решений.

Математическая запись основной идеи выглядит следующим образом:

$$W = W(a, h, x) \Rightarrow \max$$

Словами это соотношение раскрывается так:

при заданных условиях a, с учетом неизвестных факторов h, найти такое решение x из множества возможных решений X, которое, по возможности, обеспечивает максимальное значение показателя эффективности W. Из-за наличия в условии задачи неопределенных факторов h она из чисто математической задачи нахождения экстремума превращается в задачу о выборе решения в условиях неопределенности, и поэтому в ее формулировке появляется оговорка «по возможности».

Вторая модель – модель киберпространства. В последние годы появились работы [8, 9], в которых исследуется предложение легендарного создателя *World Wide Web* (*WWW*) Тима Бернерса-Ли переходить к сетецентрическим моделям развития информационного общества в виде многоуровневого графа ***GGG*** (*Giant Global Graph* – Гигантский Глобальный Граф). Граф является развитием цепочки построения виртуальных сетей *NET–WEB–GRAPH*. Суть модели, приведенной в [9], показана на
рис. 9.

Рис. 9 *NET, WEB, GRAPH,…*

Данную идею можно применить в отношении моделирования киберпространства. В этом случае киберпространство можно представить в виде графа – слоеного пирога. Вершины графа представляют собой критические элементы системы, ребра – связи между ними, причем связями пронизан весь «слоеный пирог». На нижнем уровне пирога (синтаксическом) находится виртуальная среда общения компьютерных систем. Это может быть Интернет и все, что мы назвали киберпространством в узком смысле (позиции *NET* и *WEB*). Синтаксический уровень имеет свои критические элементы и связи между ними.

Высшие уровни (позиция *GRAPH*) – семантические. Второй уровень – семантический 1-го рода. Это смысловой уровень, выделяющий из единичек и ноликов синтаксического уровня информацию в виде конкретных фактов. Здесь существуют уже свои критические элементы и связи.

Третий уровень – семантический 2-го рода. Из фактов составляются знания для обеспечения жизни общества. Правила, по которым факты объединяются в знания, могут быть гласными и негласными. Они и являются критическими элементами данного уровня.

Четвертый уровень – концептуальный 1-го рода. Людьми, образующими знания для жизни общества, руководят «кукловоды», реализующие определенную концепцию жизнеустройства данного государства или группы государств. Это – концептуальный уровень, со своими критическими элементами и связями.

Пятый уровень – концептуальный 2-го рода. «Кукловодами» тоже управляют с более высокого и глубокого уровня другие «кукловоды». Это так называемое «управление управляющими» или **киберменеджмент**. Видно, что данный термин не является тавтологией, а отражает вполне определенное явление.

Сколько еще уровней может быть сверху? Пока что нам не дано этого осознать в силу объективной ограниченности исходных данных и мыслительных способностей человека. Но предложенная методология построения модели киберпространства может позволить ответить на этот вопрос в дальнейшем.

Заключение

Приведенные аспекты анализа понятия «кибербезопасность» далеко не в полной мере отражают всю широту и глубину данного явления. По мере его изучения будут вскрываться новые, подчас неожиданные моменты. Пока что сделаем некоторые выводы, актуальные на сегодняшний день.

1. Боевое применение кибероружия в виде вирусных программ типа Stuxnet, Duqu, Flame, Gauss и им подобных определило необходимость и начало этапа резкого повышения требований к глубине и качеству изучения кибервоздействия с целью выработки эффективных мер защиты от него.

2. Киберпространство необходимо рассматривать не только в узком, общепринятом на сегодняшний день смысле виртуальной среды общения людей с помощью компьютерной техники, но и в широких аспектах взаимодействия критических элементов систем и их связей в режимах принятия ими управленческих решений.

3. При воздействиях на лиц, принимающих решения, необходимо учитывать специфику обработки информации в психике человека, таблицу нравственности конкретного руководителя.

4. Термины «информационная безопасность» и «кибербезопасность» не конкурируют между собой. Киберинформация является частью информации вообще и отражает ту

ее часть, которая используется для принятия управленческих решений. Поэтому кибербезопасность можно считать частью информационной безопасности.

5. При моделировании кибербезопасности можно использовать современную модель сетецентрического развития информационного общества в виде *GGG*-графа как этапа эволюционного развития по цепочке *NET-WEB-GRAPH*.

Литература:

1. Поваров Г.Н. Ампер и кибернетика / Поваров Г.Н. – М. : Сов. радио, 1977. – 96 с.
2. Винер Н. Кибернетика и общество / Винер Н. ; [пер. с англ. Е.Г. Панфилова]. – М.: Издательство иностранной литературы, 1958. – 199 с.
3. Ожегов С.И. Толковый словарь русского языка / С.И. Ожегов, Н.Ю. Шведова – М.: Изд-во «Азъ», 1992. – 680 с.
4. Достаточно общая теория управления / В кн. Мертвая вода (от «социологии» к жизнеречению). – Харьков: обществ. орг-ция «Живая вода», 2009. – 862 с.
5. Богданов А.М. Современная трактовка понятия «оружие массового поражения» / А. Богданов, В. Мохор // Бизнес и безопасность. – 2013. – № 1. – С. 7–11.
6. Про Доктрину інформаційної безпеки України: Указ Президента України від 8.07.2009 р. № 514/2009 // Офіційний вісник Президента України. – 2009 № 20. – С. 18. – ст. 677.
7. Вентцель Е.С. Исследование операций: задачи, принципы, методология / Е.С. Вентцель. – М.: Наука, Гл. ред. физ.-мат. лит., 1988. – 208 с.
8. Бородакий Ю.В. К проблеме обеспечения интероперабельности / Ю.В. Бородакий, Ю.Г. Лободинский // Информационные технологии и вычислительные системы. – 2009. – № 5. – С. 16–24.
9. Хохлова М.Н. Основы ПОСТвинеровской кібернетики [Электронный ресурс] / М.Н. Хохлова. – Режим доступа. : http://viphmn.ru/index.php