УДК 004.056(045)

Философия безопасности — безопасность информации и энергии

ТРУСОВ НИКОЛАЙ АЛЕКСЕЕВИЧ, *кандидат философских наук, директор университетского колледжа информатики и программирования Финансового университета. E-mail: ntrusov@fa.ru*

БАШЕЛХАНОВ ИГОРЬ ВИКТОРОВИЧ*, кандидат физико-математических наук, заведующий лабораторией, преподаватель университетского колледжа информатики и программирования Финансового университета. E-mail: ivbashelhanov@fa.ru*

КОЛМЫКОВА ЕЛЕНА АЛЕКСЕЕВНА*, кандидат экономических наук, заместитель директора по УМР университетского колледжа информатики и программирования Финансового университета. E-mail: ekolmykova@fa.ru*

Аннотация*. Актуальность исследования соотношения понятий энергии (в форме кванта) и информации была выделена в фундаментальной работе Джона А. Уилера.*

В нашей работе изучаются последствия семантической эквивалентности энергии и информации для информационной безопасности как кросс-науки.

Мы приходим к выводу, что любая система защиты требует обязательной надсистемной интеграции (в отличие от системной интеграции), более того — участия кросс-методологического оператора, владеющего конвергентной философией информационной безопасности, поскольку все вышеуказанные меры предотвращают стандартные, формализованные, схоластические угрозы, сколь бы «свежими» и инновационными ни были методы защиты. При динамическом древовидно-фрактальном подходе надсистемный интегратор в любой момент может расширить рассматриваемое им множество угроз и принять адекватные меры. Нами впервые рассмотрено появление дополнительных угроз, появляющихся при сегментации (разделении) методов защиты. Также впервые рассмотрены перспективы фрактально-математического и динамического подхода для анализа и предотвращения угроз, а также методологические последствия семантической эквивалентности энергии и информации. Впервые информационная безопасность (философия безопасности, философия информационной безопасности) рассматривается как единая кросс-наука — уходящая от междисциплинарности к единой конвергентной науке. Впервые предложено введение этих новых кросс-научных курсов в учебных заведениях всех уровней; вводится новый термин «метофилософер информационной безопасности» для субъекта, принимающего наиболее адекватные кросс-методологические, кросс-научные решения по актуальным, насущным задачам информационной безопасности. Наконец, мы обнаруживаем с помощью семантической эквивалентности энергии и информации (эффекта, феномена Итигэлова) обоснованность фундаментальной философской гипотезы Джона А. Уилера в отношении информации.

Ключевые слова*: гипотеза Джона Уилера; защита информации; информационная безопасность; информационное отравление; информационные войны; киберпреступность; науки Hi-Hume; сегментирование; семантическая эквивалентность энергии и информации; токсичность информации; феномен Итигэлова; философия безопасности; фракталы.*

Security Philosophy — Security Information and Energy

NIKOLAI A. TRUSOV, *PhD, Director of the CCSP Financial University. E-mail: ntrusov@fa.ru*

BASHELHANOV IGOR V. *PhD., head of the laboratory, the teacher CCSP Financial University. E-mail: ivbashelhanov@fa.ru*

KOLMYKOVA ELENA A. *Ph.D., Deputy Director of CCSP Financial University E-mail: ekolmykova@fa.ru*

Abstract. *The research of the relationship between the concepts of energy (in the form of quantum) and information was highlighted in the fundamental work of John A. Wheeler.*

In our work we study the consequences of semantic equivalence of energy and information for information security — as cross-science.

We come to the conclusion that any protection system requires mandatory super integration (as opposed to system integration), moreover the participation of cross-methodological operator, owning convergent philosophy of information security, since all these measures prevent standard, formalized, scholastic threats, no matter how fresh and innovative methods were not protection. When the dynamic tree-fractal approach super integrator may at any time extend considered by many threats and to take adequate measures. We first considered the appearance of additional threats emerging in the segmentation (division) methods of protection. Also for the first time discussed the prospects of fractal mathematics and dynamic approach for the analysis and prevention of threats and methodological implications of semantic equivalence of energy and information. First information security (security philosophy, philosophy of information security) are treated as a single cross-science — science, disappearing from interdisciplinarity to a single convergent science. First proposed the introduction of these new cross-academic courses in educational institutions of all levels. For the first time introduces a new term «metaphilosopher information security» for the subject, taking the most adequate cross-methodological, cross-scientific solutions for current, pressing problems of information security. Finally, we find with the help of semantic equivalence of energy and information (the phenomenon Itigelov) the validity of the fundamental philosophical hypotheses John A. Wheeler, in respect of information.

Keywords: *Security philosophy, information security, semantic equivalence of energy and information, the hypothesis John Wheeler, the phenomenon Itigelov, fractals, segmentation, data protection, information poisoning, toxicity information, information warfare, cyber crime, science Hi-Hume.*

Изучение соотношения энергии и информации, а также отдельно — понятия «информация» было, безусловно, одной из первоочередных задач современной науки. В своей недавней философской работе Е. А. Мамчур [1, с. 57] упоминает гипотезу выдающегося американского физика Джона А. Уилера [2], которая говорит о том, что в основе мироздания лежат «кусочки» информации («Все от бита» — «*It from bit*»). В результате исследований эффекта, феномена Итигэлова было установлено семантическое единство энергии и информации, а другими словами, установлена эквивалентность энергии и информации, но в более сложной форме, чем эквивалентность массы и энергии [3, с. 50]. При данных обстоятельствах гипотеза Уилера оправдана и обоснована. Далее мы рассмотрим научные и учебно-методические последствия нашего заключения и фундаментальной идеи Уилера. При семантическом объединении этих основополагающих понятий, как оказалось, кардинально упрощается мировидение и описание универсума. Человек является одной из замечательных вершин современного развития природы, Вселенной. Для его развития требуется гармонично сбалансированная информация, представленная в виде генетической (химической) энергии ДНК, в виде химической энергии разнообразных продуктов питания и поступающая при передаче энергии от внешних источников в форме физико-химических полей, воздействующих на человека по оптическим, акустическим, обонятельным, осязательным, вкусовым каналам. При избытке, отсутствии или недостатке какого-либо вида информации (энергии) человек сначала чувствует дискомфорт (дисгармонию), при долговременном избытке или дефиците он заболевает (появляются депрессия, неадекватное поведение и т.д.), а затем гибнет. Информация в данном контексте выступает как гуманитарная энергия. Эта гуманитарная энергия в связи с вышесказанным может быть «токсичной», «отравляющей» при превышении порогов (пределов).

Так, при обсуждении своего доклада на Инфофоруме-2014 [4] профессор, главный научный сотрудник ФГБУ НИИ медицины труда РАМН, лауреат премии Правительства РФ в области науки и техники и премии Ф. Ф. Эрисмана по гигиене, кандидат технических наук и доктор биологических наук Э. И. Денисов использовал термин «отравление информацией». Мы подтверждаем научную обоснованность этого термина. Очевидна при таких условиях насущная необходимость защиты информации, обеспечения

информационной безопасности личности. Эксперты Инфофорума-2014 отметили, что в мире не хватает специалистов по информационной безопасности [4]. Этот кадровый дефицит составляет в настоящее время около 1 млн человек. Угрозы информационной безопасности представляют уже не отдельные хакеры, а их преступные группировки. Криминальный оборот, связанный со взломами официального программного обеспечения, совсем немного не дотягивает до мирового оборота наркотиков. Таким образом, угрозы, порождаемые киберпреступностью, могут определять в скором времени состояние экономики, экономическую, финансовую, военную безопасность целых стран.

Информационные ресурсы, сайты российских банков и их филиалов уже регулярно подвергаются атакам, угрожая значительной части их ликвидности. Сращивание противоправных структур со СМИ (в том числе и интернет-СМИ) может привести к потере устойчивости банковского учреждения (независимо от его размера), государства и любой другой социотехнической системы. Остра проблема отставания российских законов и нормативных актов от цифровых реалий современных угроз. Законодатели не успевают и «бьют по хвостам» злоумышленников, вместо того чтобы принимать предупредительные меры. При запоздалой борьбе используются старые подходы — подходы индустриального общества. Специалист одной из *IT*-компаний пояснил, что в день к ним поступает на анализ до 250 тыс. «зловредных» программ, в то время как год назад ежедневно поступало 100 тыс. Эксперты установили, что 80% инцидентов в сфере информационной безопасности связаны с человеческим фактором, поэтому гуманитарным проблемам информационной безопасности должно уделяться гораздо большее внимание, чем это делается сейчас. «Токсичность» информации, «отравление» информацией все больше дает о себе знать в связи с аномальным поведением подростков-школьников и вообще молодых людей до 40 лет. По сведениям прокуратуры г. Москвы, подростковая преступность только за 2013 г. выросла на 24%, а по особо опасным преступным проявлениям — на 30%. 70% этих преступлений совершают учащиеся школ и студенты [5].

Все это приобретает масштабы военных действий. Морально-этическому воспитанию молодежи в условиях информационных войн должно уделяться больше внимания со стороны образовательных и других учреждений России. Эта проблема становится еще актуальнее, поскольку в последних технических новациях рассматривается вопрос прямого и косвенного «мягкого» (с помощью так называемой «мягкой силы» — *software*) вживления, встраивания микропроцессоров и их процессов в высшую нервную деятельность человека. Информационная безопасность в современных реалиях становится из узкоспециализированной *Hi-Tech* науки наукой *Hi-Hume*. Встречая на улице человека, совсем скоро мы рискуем натолкнуться на гибридного индивидуума, чьи возможности (а вместе с тем и угрозы) будут многократно усилены посредством физических полей, генерируемых процессами в киберпространстве.

В связи с этим считаем насущно необходимым ввести в учебные планы всех учебных заведений курс «Философия информационной безопасности», а в учебный курс физики — раздел «Физические основы защиты информации: энергия, информация, физика, квант, квантовая криптография» (в первую очередь для студентов, проходящих подготовку по специальности «Информационная безопасность»). Здесь мы учитываем упомянутую в начале нашей статьи идею фундаментальной философской работы 1990 г. Джона А. Уилера «Information, physics, quantum: the search for links» [2].

По определению [6, с. 39], «философия безопасности» — это наука о сохранении (защищенности) динамики устойчивых состояний системы социальных, технических и природных объектов и ближайших к ним координационных сфер (ближней социотехно-природной системы). Принципиальную роль в этой науке играет способность специалистов по философии безопасности (философии информационной безопасности) распознавать «своих» или «чужих», а точнее, какие «дружеские» или «вражеские» элементы находятся в изучаемой системе либо вблизи нее и их пропорции (величина угроз).

Все это возвращает нас к извечной философской проблеме «добра» и «зла», а именно к вопросу, что считать «добром», а что «злом». Для большинства это далеко не всегда очевидно. И даже более того, специалисты зачастую не различают угрозы и понятия «добра» и «зла». Нередко они сливаются в одно. Чтобы избежать этого слияния и путаницы понятий, на практике должен применяться дуалистический подход, развитый еще в древних религиозно-философских учениях.

Междисциплинарный подход, конвергенция наук, отмеченные ранее М.В. Ковальчуком, О.С. Нарайкиным, Е.Б. Яцишиной [7, с. 3; 8, с. 4], проявляются ныне на примере рассматриваемой нами информационной безопасности (философии безопасности, философии информационной безопасности), как феномен появления кросс-дисциплинарной науки [9], а в нашей уточненной терминологии — появления кросс-науки (поскольку границы в конвергирующей науке исчезают, а следовательно, исчезают и дисциплины в обычном понимании). Упомянутые в последней ссылке кросс-дисциплинарные методологические семинары проведены в Российской академии народного хозяйства и государственной службы при Президенте РФ с помощью математиков ИПМ им. М.В. Келдыша РАН, но мы должны перейти на новый, следующий уровень обобщения, абстракции. При этом философия безопасности и информационная безопасность очевидно конвергируют, сливаются в одну научную сущность.

В старом, но еще действующем определении Доктрины информационной безопасности РФ говорится: «информационная безопасность» — это состояние защищенности национальных интересов страны (а именно жизненно важных, сбалансированных между собой интересов личности, общества и государства) в информационной сфере от внутренних и внешних угроз [10, с. 31]. При нашем подходе узкая информационная сфера автоматически расширяется и становится семантически тождественной энергетической сфере. Под энергетической сферой, очевидно, понимается совокупность всех видов энергии, входящих и исходящих за пределы национально-государственных, суперэтнических границ. Среди видов энергии мы можем выделить также и «финансовую» энергию, проявляющуюся в финансовых отношениях. Национальная безопасность, например, Российской Федерации и США как развитых социотехнических систем, в настоящее время напрямую определяется состоянием их информационной безопасности. Все это позволяет рассматривать обеспечение национальной безопасности как способ защиты нации (и соответствующих ей суперэтносов, этносов и субэтносов) от внешнего и внутреннего вмешательства в уровень ее энергии. Несанкционированное и резкое изменение ее энергии, энергобаланса приводит к гибели социотехнической системы независимо от знака изменения (будь-то положительного или отрицательного).

Фрактальная геометрия реального пространства, природы, материальной и духовной культуры, обнаруженная в последние десятилетия [11, с. 7], и бурно развивающиеся ее физико-математические подходы уже дают замечательные плоды познания окружающего мира [12, с. 5].

Фрактальное подобие можно распространить как с объектов неживой природы на объекты живой, так и наоборот. Исходя из принципа фрактального подобия, мы можем расширить эти подходы и на такие объекты, как знания и способы получения нового знания [13, с. 38].

В работе Г.Г. Малинецкого и др. [14, с. 6] подчеркивается идея, что парадигма динамического хаоса, которая может быть применена в нано-науке, приводит к выводу, что сложные структуры могут создаваться по весьма простым правилам. Как говорил советский нобелевский лауреат П.Л. Капица, «открытие — это необычное соединение уже известных элементов».

Рассмотрим вышесказанное применительно к такой конвергентной науке, как информационная безопасность.

М.А. Борисов и др. [15, с. 8] среди основных направлений защиты информации выделяют три: нормативно-правовую, организационно-техническую и экономическую. Так, И.Р. Бегишев [16, с. 433] выделяет три группы мер защиты информации: правовые, технические и организационные. При этом последний справедливо отмечает, что технические меры включают в себя, в том числе, криптографические и стеганографические.

Мы думаем, что выделение всех вышеуказанных мер является оправданным, и предлагаем дополнить и системно интегрировать все возможные варианты защиты в три группы. Последнее число целесообразно использовать в связи с тем, что человеческий мозг с трудом оперирует одновременно с большим числом параметров, степеней и степеней свободы. Вспомним, например, про математические уравнения второй и третьей степени, для которых возможны относительно простые аналитические решения. Большее число степеней и неизвестных резко увеличивает объем и время вычислений (время принятия решения). Поскольку время в информационной безопасности имеет критическое значение, то, следовательно, по аналогии имеет смысл сократить число рассматриваемых объектов до трех в первом приближении.

Таким образом, мы можем выделить, расширить и интегрировать три группы мер защиты информации, обеспечения информационной безопасности:

1) физико-технико-математические меры (ФТМ);

2) организационно-экономико-маркетинговые меры (ОЭМ);

3) нормативно-право-конституционные меры (НПК).

В свою очередь, во втором приближении каждую составляющую нужно разделить на три меры (оптимальное число). Например, физическую защиту (физические меры) разделим на три метода.

1. Методы по физико-географической защите. Выбор физико-географического расположения объекта защиты информации очень важен. Например, место расположения атомной электростанции Фукусима в Японии было выбрано крайне неудачно как место атомного объекта, так и объекта информатизации, что привело к многочисленным его уязвимостям.

2. Меры по созданию физических препятствий (ограждение, стены, рвы, валы и т.п.) при приближении злоумышленника к объекту защиты.

3. Непосредственная капитальная защита объекта (здание, стены и т.п.).

Технические меры можно разделить, в свою очередь, на следующие три метода.

1. Непосредственная техническая защита информационных ресурсов, в том числе и физических лиц (как носителей информации): защищенные, бронированные двери, окна, бронежилеты, шлемы, оружие, система контроля управления доступом (СКУД, СКД) и т.п.

2. Непосредственная программная защита информационных ресурсов на физико-технических носителях (защита компьютеров, сетей, памяти от вирусов, атак и т.п.).

3. Аппаратная защита (защита от утечек ПЭМИН, заземление, экранирование, маскирование, скремблирование, «белый шум» и т.п.).

Таким же образом «разворачиваем» три математические меры.

1. Криптография.

2. Электронно-цифровая подпись (ЭЦП),

3. Стеганография.

Ветвление мер в последующих приближениях производится по такому же фрактальному (древовидному) принципу.

Как и всякое дробление, сегментирование, разделение приводит к потере информации и появлению новых уязвимостей, поскольку человеческий мозг при анализе ошибается в большей или меньшей степени. Это можно продемонстрировать на уязвимостях, появившихся в РФ, США и других развитых странах в результате разделения властей. В целом управленческая парадигма разделения властей — мера вынужденная и предназначена в основном для соблюдения прав и свобод граждан. Однако при отсутствии надсистемного интегратора, который нейтрализует угрозы, внедряющиеся через границы раздела компетенций отдельных, сегментированных государственных органов, эта парадигма становится ущербной и угрожающей безопасности государств и наций. Угрозы, не входившие в сферы компетенций ни одного государственного органа США, привели, например, к успешным атакам злоумышленников на Всемирный торговый центр в Нью-Йорке в 2001 г.

Сегментирование рынка [17] (маркетинговое понятие), сегментирование рынка угроз и рынка мер противодействия им является удовлетворительным приближением в большом количестве случаев, но при появлении новой категории товаров (или по аналогии — новых угроз) такой подход равносилен защите от дождя под дырявым зонтом. В информатике, как и в других науках, сегментирование является неотъемлемой частью научного процесса. Например, в китайской информатике, становящейся лидирующей в результате развития таких *IT*-компаний, как *HUAWEY* и др., выделяют четыре ее основных направления, сегмента: конкурентная разведка, библиометрия, управление знаниями и автоматизированный информационный поиск. В свою очередь, в конкурентной разведке проводится сегментация контента, его анализ.

Видение антропологической, гуманитарной цели, конвергентный [18, с. 222], междисциплинарный подходы прослеживаются и во многих частных работах [19, с. 209; 20, с. 236; 21, с. 170].

Последствия конвергенции наук, установления семантической эквивалентности энергии и информации дают возможность лавинообразного развития науки *Hi-Hume*, а также насущную необходимость введения нового субъекта обеспечения информационной безопасности — метофилософера информационной безопасности (от терминов «методология» и «философия информационной безопасности»).

Литература

1. *Мамчур Е.А.* Информационно-теоретический поворот в интерпретации квантовой механики // Вопросы философии. 2014. № 1. С. 57–71.
2. *Уилер Джон Арчибальд.* [Электронный ресурс] URL: http://www.ru.wikipedia.org/wiki/Уилер (дата обращения: 28.02.2014).
3. *Башелханов И.В.* Кристалл Итигэлова // Байкальские перспективы: Материалы IV научно-практической конференции, посвященной памяти М.П. Маликова. Российский государственный гуманитарный университет, ф-л в г. Улан-Удэ. Улан-Удэ: Из-во БГСХА. 2010. С. 48–50.
4. Инфофорум-2014. [Электронный ресурс] URL: http://www.2014.infoforum.ru (дата обращения: 06.03.2014).
5. Детская преступность в Москве выросла за год на 24% // Информационное агентство Моссовет. [Электронный ресурс] URL: http://www.mossovetinfo.ru/news/index.php?article=9444 (дата обращения: 06.03.2014).
6. *Башелханов И.В.* Философия безопасности и философия Заратуштры // Байкальские перспективы: Материалы III научно-практической конференции, посвященной памяти М.П. Маликова (5 мая 2008 г.). Российский государственный гуманитарный университет, ф-л в г. Улан-Удэ. Улан-Удэ: Из-во ВСГТУ. 2008. С. 39–40.
7. *Ковальчук М.В., Нарайкин О.С., Яцишина Е.Б.* Конвергенция науки и технологий — новый этап научно-технического развития // Вопросы философии. 2013. № 3. С. 3–11.
8. *Ковальчук М.В.* Наука и жизнь: моя конвергенция. М.: Академкнига, 2011. 304 с.
9. Методологический семинар «Кросс-дисциплинарный синтез знаний как источник власти и лидерства для глобальных и локальных «точек сборки»: вызовы науке и образованию». [Электронный ресурс] URL: http://www.igsup.ane.ru/index.php/meropriyatiya/613-metodologicheskij-seminar-kross-distsiplinarnyj-sintez-znanij-kak-istochnika-vlasti-i-liderstva-dlya-globalnykh-i-lokalnykh-tochek-sborki (дата обращения: 06.03.2014).
10. *Партыка Т.Л., Попов И.И.* Информационная безопасность. М.: ФОРУМ, 2011.— 432 с.
11. *Басса Мария Изабель Бинимелис.* Мир математики: в 40 т. Т. 10. Новый взгляд на мир. Фрактальная геометрия. М.: Де Агостини, 2014. 144 с.
12. *Капица С.П., Курдюмов С.П., Малинецкий Г.Н.* Синергетика и прогнозы будущего. М.: Едиториал УРСС, 2003. 288 с.
13. *Башелханов И.В., Башелханов С.И.* Концепция защиты информации. Новые аспекты обеспечения информационной безопасности // VI Международная научно-практическая конференция студентов, аспирантов и молодых ученых «Информационные технологии в науке, бизнесе и образовании (Технологии безопасности)». М.: Изд-во Финуниверситета, 2013. 272 с.
14. *Малинецкий Г.Г., Митин Н.А., Науменко С.А.* Нанобиология и синергетика. Проблемы и идеи. // Препринт Института прикладной математики им. М.В. Келдыша РАН. 2005. № 29.
15. *Борисов М.А., Романов О.А.* Основы организационно-правовой защиты информации. М.: Книжный дом «ЛИБРОКОМ». 2013. 208 с.
16. *Бегишев И.Р.* Меры предупреждения преступлений в сфере обращения цифровой информации // Информация и безопасность. 2011. № 3. С. 433–438.
17. Сегментация рынка. [Электронный ресурс] URL: http://www.slovari.yandex.ru/сегментация/Лопатников/Сегментация%20рынка/ (дата обращения: 06.03.2014).
18. *Де Шарден Пьер Тейяр.* Феномен человека (Преджизнь, жизнь, мысль, сверхжизнь). М.: Наука,1987. 240 с.
19. *Белая Е.Н.* Междисциплинарность, антропоцентричность, комплексность как основы интегративного метода исследования языковых репрезентаций эмоций // Вестник Омского государственного университета. 2012. № 2. С. 209–212.
20. *Полещенко К.Н., Разумов В.И., Рыженко Л.И., Семенюк Н.А.* Конвергенция социальных и технологических инноваций как основа перехода современного общества в когнитивную фазу развития // Вестник Омского государственного университета. 2012. № 2. С. 236–240.
21. *Гидлевский А.В., Здриковская Т.А.* Уровневая модель понимания текста // Вестник Омского государственного университета. 2012. № 2. С. 170–173.