РЕЦЕНЗИЯ НА КНИГУ «НАЦИОНАЛЬНАЯ СИСТЕМА РАННЕГО ПРЕДУПРЕЖДЕНИЯ О КОМПЬЮТЕРНОМ НАПАДЕНИИ»

Марков А.С.[1]

Монография «Национальная система раннего предупреждения о компьютерном нападении»

Издательский дом «Афина» выпустил первую книгу Университета #Иннополис из серии «Подготовка ИТ-специалистов международного уровня в области Computer Science». Монография «Национальная система раннего предупреждения о компьютерном нападении» рассказывает об успешном опыте проектирования и создания опытных образцов открытого сегмента национальной системы раннего обнаружения компьютерных атак на критическую инфраструктуру Российской Федерации.

Над книгой работали доктор технических наук, профессор, руководитель Центра информационной безопасности Университета Иннополис Сергей Петренко и кандидат технических наук, доцент, заместитель генерального конструктора ОАО «РТИ» Дмитрий Ступин.

DOI: 10.21681/2311-3456-2017-4-67-74

Введение

Взглянув на название книги [1], сразу пришло на память, что заявленная авторами тематика уже академически прорабатывалась в период изучения возможности массового подключения учреждений России к информационно-телекоммуникационным сетям международного информационного обмена (1993-1995 гг.) в ряде научных коллективов, имеющих опыт создания специальных глобальных сетей СССР (в том числе в ответ на ARPANET). Одним из активистов, инициировавших обсуждение данной тематики был специалист по надежности программ кандидат наук Борис Павлович Пальчун - в память о нем хотелось бы указать открытую (совместную с членкором РАН Р.М. Юсуповым) публикацию по смежной тематике 1993 г. [2].

Представленная же читателю монография Петренко С.А. и Ступина Д.Д. является совершенно иным, оригинальным и смелым взглядом на обозначенную проблематику с учетом абсолютно новых условий и реалий, в первую очередь связанных с реализацией в стране *государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак* (ГосСОПКА). Символично, что данная книга появилась как раз в момент подписания Президентом страны *Закона о безопасности критической информационной инфраструктуры* (КИИ), определившего принципиальные моменты устойчивого функционирования КИИ при проведении в отношении ее компьютерных атак.

Отмечая востребованность книги, следует безусловно согласиться с академиком РАН И.А. Каляевым, профессорами С.Ф. Боевым, А.И. Смирновым и А.Г. Тормасовым, которые в вступительной части отметили соответственно рост роли информационного противоборства во современных гибридных войнах, своевременность ознакомления читателей с опытом создания ситуационных центров по тематике, резкий рост в иерархии угроз *инфогенного нарратива*, а также острую потребность в совершенствовании национальной системы подготовки высококвалифицированных кадров в области кибербезопасности.

1 Марков Алексей Сергеевич, доктор технических наук, CISSP, президент НПО «Эшелон», Москва, Россия. mail@cnpo.ru

Основное содержание монографии

Книга, на наш взгляд, имеет мультидисциплинарный научный вид[2] информационно-публицистического, прикладного и теоретического характера и касается как освещения исторических событий, литературного описания эволюционных ИТ-процессов, форумов и конференций, так и аналитического разбора доктринных документов и парадигм, описания современных и перспективных архитектурных и технологических ИТ-решений, а также иллюстрирования результатов формального и полуформального моделирования, связанных при этом с заявленным авторами *интеллектуальным и когнитивным аспектом* решения проблемы раннего предупреждения о компьютерном нападении (КН) на критические информационные ресурсы страны.

Концептуально по главам книга вполне логична и включает в себя изложение:

1. Актуальности разрешения научной проблемы обнаружения и предупреждения компьютерного нападения на КИИ страны;
2. Предельных возможностей известных технологий контроля и мониторинга киберпространства;
3. Возможных решений научной проблемы раннего предупреждения о КН на КИИ страны;
4. Перспективных поисковых исследований в области ИБ и раннего предупреждения о КН на КИИ страны.

Авторы обосновывают постановку *научной проблемы*, заключающейся в создании научного аппарата (и далее – системы) раннего предупреждения о КН, и связанной с решением комплекса сложных научных задач, а именно [1, с.16]:

- классификации входных данных и признаков КН на основе больших данных TCP/IP-сетей и интернет-вещей;
- формирования шаблонов обнаружения КН;
- многофакторного прогнозирования на основе больших данных;
- порождения новых знаний о закономерностях информационного противоборства;
- обучения интеллектуальных подсистем.

Что касается реализационных моментов системы раннего предупреждения о КН, то авторы предлагают два этапа ее создания:

1. Развитие высокопроизводительных центров ведомственных сегментов ГосСОПКА;
2. Внедрение в работу ГосСОПКА авторских методов «вычислительного когнитивизма» [1, с.20].

В последнем утверждении авторы указывают на назревшую необходимость смещения текущей *парадигмы* современных систем глобального мониторинга ИБ, основанных на корреляции событий и реагировании на инциденты, в сторону внедрения когнитивных технологий (методов когнитивной лингвистики), позволяющих выявить скрытый замысел операционной деятельности источников КН и перейти к предупреждающим управленческим решениям в области информационного противоборства.

Глава 1. Актуальность тематики

Первая глава книги посвящена обоснованию собственно актуальности и своевременности поставленной ранее во введении научно-технической проблемы. Авторы предлагают оригинальное решение поставленной в главе задачи путем:

- обзора концептуальных документов;
- подведения итогов учебно-тренировочных мероприятий;
- демонстрации уязвимости отдельных технических решений и отдельных сегментов (в частности, релевантных [3]);
- описания примера решения смежной проблемы устойчивости вычислений в условиях киберпротивоборства.

Наибольший прикладной интерес, на наш взгляд, вызывают первые подразделы главы, а именно:

- определение важности обеспечения безопасности киберпространства с учетом российской законодательной базы (на основе детального разбора Концепции внешней политики РФ 2016 г., Доктрины ИБ РФ 2016 г. и Стратегии национальной безопасности РФ до 2020 г.);
- констатация политики доминирования Запада в вопросах киберпротивоборства (на основе концептуальных и программных документов НАТО и США, таких как: NATO Cyber Defence Concept, Tallinn Manual on the International Law Applicable to Cyber Operations, DARPA Research Program и других источников, в том числе литературных [4]);
- анализ зарубежных киберучений (на примере деятельности ENISA, а также краткого сравнения учений Cyber Europe, Locked Shields, Quantum Dawn и др.);
- обзор типовых документов командно-штабных киберучений и новостей по тематике[3], а также

2 Следует заметить, что вводные слова к монографии подготовили доктора различных научных отраслей – *исторических, технических, физико-математических* и экономических наук.

3 Например: http://rbc.ru/newspaper/2016/06/20/576157479a794763a3751e7b

детальных итогов межгосударственных антитеррористических киберучений СНГ «Кибер-Антитеррор-2016».

Что касается теоретического решения смежной проблемы - устойчивости вычислений, то здесь авторами монографии представлен полный исторический экскурс по научным школам абстрактных вычислений и смежным дисциплинам (перечислено более полсотни выдающихся научных светил) и комплекс теоретических результатов, что познавательно для молодых ученых, увлекающихся данным направлением науки.

Глава 2. Предельные возможности известных технологий контроля и мониторинга киберпространства

Вторая глава ставит своей целью исследование «потолка» современных механизмов безопасности путем определения задач:

- критического разбора опыта использования ситуационных центров (СЦ) органов госвласти;
- оценки ограниченных возможностей коммерческих услуг безопасности уровня провайдера (Managed Security Services);
- исследования ограничений вариантов предоставления услуг по ИБ (in/out sourcing), а также изучения причин недоверия к ним в России;
- описания ограниченных возможностей СЦ на примере решения Microsoft;
- описания границ функционирования команд критического реагирования (CERT, CSIRT);
- описания ограничений возможностей отдельного центра ГосСОПКА сегмента Минобрнауки России;
- предложения оригинального варианта так называемого «иммунного» ситуационного центра.

Определив указанные задачи, авторы в главе раскрывают весьма важную тему – это накопленный колоссальный опыт СЦ государственной власти, в частности ссылаясь на профильную *конференцию, посвященную 20-летию ситуационного центра Президента Российской Федерации*, где констатируется естественный переход от разрозненных центров мониторинга к единой системе распределенных ситуационных центров (СРСЦ) с учетом замысла на импортозамещение. Авторы отстаивают весьма интересную в теоретическом плане идею о возможности и необходимости создания СЦ принципиально нового типа, а именно, на основе технологий NBIC (нано-, био-, инфо- и когно-), включая концепцию «управления знаниями», что должно позволить перейти к так называемым **когнитивным ситуационным центрам**, ориентированным на предупреждающие управленческие решения.

Можно отметить важное познавательное значение приведенных в главе вариантов аутсорсинга, в том числе классификацию MSS, примеров команд реагирования CERT/CSIRT, иллюстрирование работы ситуационного центра Microsoft (Global SOC) и продуктов компании Fortinet. Теоретическое значение имеет описание модели **«иммунного» ситуационного центра** по ИБ, функционально эквивалентного (авторы здесь формулируют оригинальную рабочую гипотезу) иммунной системе живого существа.

В итоге авторы делают вывод о заявленных в названии главы ограничениях современных технологий в виде декларации предопределенных эволюций, как-то:

- переход от разрозненных центров к единой системе, функционирующей на базе единого регламента;
- отказ от автономных и локальных центров в пользу «облачных» вычислений;
- трансформацию концепции управления данными к управлению знаниями, в том числе, возможно, и на базе методов когнитивной лингвистики;
- повышение доверия к внешним услугам по ИБ.

В последнем случае следует заметить актуальность нового подвида лицензионной деятельности по технической защите информации – *мониторинга ИБ*[4].

Глава 3. Возможные научно-технические решения проблемы раннего предупреждения о компьютерном нападении

В третьей главе авторы обозначили несколько отдельных проблемных направлений:

- обоснование роли супервычислителя в системе обнаружения и предупреждения о КН;
- обоснование использования когнитивных методов (когнитивной лингвистики) при оценке замысла КН;
- констатацию актуальности извлечения знаний из неструктурированной информации (технологии BigData);
- обоснование возможности применения технологии управления мастер-данными (Master Data Management) для предварительного сбора данных о замысле КН;
- разработку концептуальной модели программного решателя с использованием принципов антиципации.

В рамках обсуждения суперкомпьтерной платформы в главе представлены:

- классификации вычислительных систем (от

4 https://www.osp.ru/resources/releases/?rid=36830

абакуса до супервычислителей, а позже – и до когнитивных компьютеров);
- планы, концепции и проблемы создания и развития отечественных суперкомпьютерных технологий сверхвысокой производительности, соответствующих задачам по ИБ.

Авторы подробно описывают успехи мегакластеров предприятий компьютерной промышленности (МСЦ РАН, НИЦ «Курчатовский институт», ВЦ РФЯЦ ВНИИЭФ-ИТМФ, НИИСИ РАН, МЦСТ, НИИ МВС ЮФУ и НИЦ СЭ и НК, НИЦЭВТ, ФГУП НИИ «Квант», ФГУ ФИЦ ИПМ им. М. В. Келдыша, ИПС им. А. К. Айламазяна РАН, НПО «Роста», МГУ им. М.В.Ломоносова, компании «Т-Платформы», РСК, «Ниагара», «Иммерс»), отмечая возможности создания отечественного суперкомпьютера в 1–3 EFLOPS к 2020-2025 гг., что, однако, может оказаться и недостаточным для решения задач именно в области ИБ, так как ожидаемые к 2025 г. потребности могут достичь 20 EFLOPS [1, табл.15].

Подводя итоги первой части данной главы, авторы констатируют, что «*назрела необходимость существенно расширить номенклатуру соответствующих аппаратных и программных компонентов. Для решения данной задачи необходимо программно-целевым способом реализовать комплекс мероприятий на период до 2025 г. по организации их разработки и серийного производства, главным образом, различных типов отечественных микропроцессоров, а также микросхем специального и общего применения*», а «*для достижения этой цели необходимо существенно развить отечественное производство высокопроизводительных и доверенных средств вычислительной техники*» [1, с.205-206]. Можно поддержать авторов указанием на отечественные технологические решения, к примеру, отечественная госсистема МИР не так давно перешла на отечественные высокопроизводительные системы МЦСТ и защищенные технологии Рубикон-К и др.[5]

В следующей части главы авторы приводят результаты составной части ОКР «Предупреждение-2016». Представленные авторами результаты ОКР демонстрируют инновационность и эффективность разработанного проекта программно-аппаратного комплекса так называемой когнитивной системы раннего предупреждения о компьютерном нападении.

5 http://expert.ru/2017/01/18/mir/

Глава 4. Перспективные поисковые исследования в области информационной безопасности и раннего предупреждения о компьютерном нападении

В четвертой главе при обсуждении базовых перспективных поисковых исследований в рамках предметной области авторы инициировали научную дискуссию о:
- важности глобальных научных проектов и развитии навыков и компетенции инженеров- исследователей и конструкторов;
- деятельности Агентства перспективных оборонных исследований США – DARPA, а также российском аналоге - ФПИ;
- о перспективах программно-конфигурируемых сетей – SDN-сетей (Software Defined Networking), в том числе отечественного сегмента проекта «Центра прикладных исследований компьютерных сетей»;
- о безопасных возможностях технологии мобильной связи LTE (Long-Term Evolution);
- о безопасных возможностях облачных вычислений;
- о внедрении технологий интеллектуального анализа данных (Business Intelligence) в работу современных аналитических информационных систем;
- о внедрении предложенного авторами подхода к контролю корректности работы стека протоколов на примере решения Oracle;
- о возможности построения центра мониторинга ИБ (SOC) на базе продукции SAP;
- об онтологии кибербезопасности SMART GRID;
- о ГОСТ Р МЭК 61508 и необходимости его развития.

На старте чтения данной главы невозможно не процитировать задорные авторские строки: «*История нашей страны наглядно демонстрирует, что наиболее значимые прорывы в области научно-технического развития были связаны с крупными государственными программами: планом ГОЭЛРО, индустриализацией 1930-х годов, ракетно-космической программой, атомным проектом, созданием систем ракетно-космической обороны, развитием гидроэнергетики и т.д. Таким образом, логично предположить, что для новых «рывков» необходимы серьезные проекты государственной важности*».

Далее, при демонстрации актуальности поисковых исследований, весьма интересным является описание подобного опыта работы и достижений Агентства DARPA.

К достоинству главы можно отнести дополнение современной нормативной базы информаци-

онных и кибероперациий [5], отраслевых и международных стандартов по кибербезопасности [6, 7], а также стандартов по оценке соответствия СЦ [8, с. 216] аналитическим обзором линейки стандарта ГОСТ Р МЭК 61508-2-2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью».

Наукометрические характеристики монографии

Изучив монографию по форме представления, можно отметить, что она удовлетворяет основным общепринятым в научной среде требованиям, как-то: наличие ISBN и УДК, заявлен тираж в 3 тыс. экз., объем работы более 35 п.л., присутствуют ученые рецензенты и редактор, авторы – признанные профессиональным сообществом ученые в соответствующей области, очевиден их личный вклад (например: [9-11] и др.) и принципиальная позиция на поставленную проблему, имеется представительный обзор актуальных индексируемых литературных источников.

Что касается содержания, то стоит лишь пролистать монографию, как бросается в глаза колоссальный объем (BigData) исходных тематических данных, а именно: упоминание ученых, конференций, документов, отдельного рода ИТ-проектов, что в совокупности достаточно любопытно и представляет безусловный научный интерес и «пищу» для будущих концептуальных выводов, в первую очередь *исторического, социального, военно-политического, нормативно-технического плана*. На наш взгляд, по литературному объему событий в области кибербезопасности книга не уступает известным летописям в области киберпротивоборства [4, 12]. К примеру, в работе обсуждаются десять федеральных законов и пятьдесят стандартов ГОСТ/ISO/IEC, приведено 295 иллюстрации. Это несомненно является характерным показателем работы и кругозора авторского коллектива.

Следует отдельно указать на следующие характеристики монографии:

- историческая ценность;
- учебно-методическая ценность;
- теоретическая и прикладная значимость.

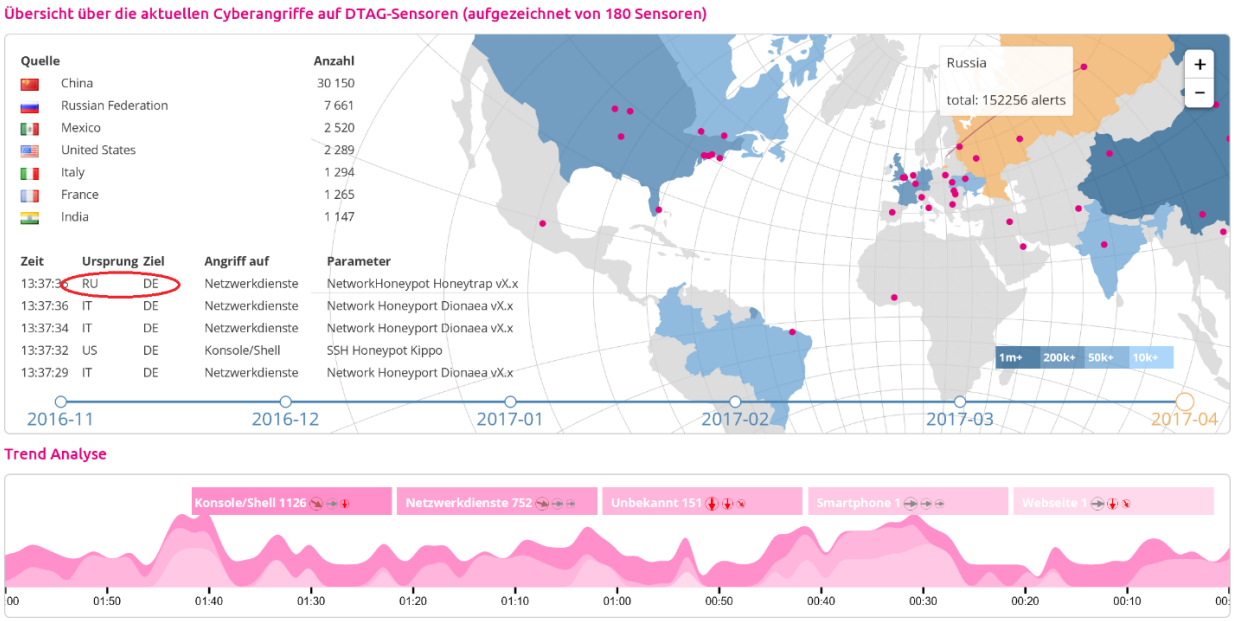
В *историческом* плане можно выделить следующие занимательные описания:

- исторические предпосылки разработки основ теории устойчивых вычислений, где перечисляются выдающиеся основатели программотехники как научной дисциплины (двадцать два ученых с мировым именем от А.П.Ершова до А.А.Маркова) и заслуги отечественных школ (с указанием еще около полусотни советских ученых от Я.М.Барздиня до Б.А.Трахтенброта), а именно: Сибирского отделения РАН, Института кибернетики Украины им. В.М.Глушкова, Института кибернетики Эстонии, Латвийского государственного университета, Московской и Санкт-Петербургской академических школ;
- история создания ЭВМ, начиная от архитектуры Яноша фон Неймана в 1945 г. и архитектурных принципов С.А.Лебедева в 1947 г. и переходя к декларированию отдельных успехов отечественных суперкомпьютеров линейки «Ломоносов»;
- исторические предпосылки когнитивного подхода, начиная от логики Аристотеля и переходя к аксиоматике А.Н.Колмогорова;
- эволюция развития средств вычислительной техники от электрической счетной машины до нейровычислителей и когнитивных компьютеров;
- история появления «когнитивных компьютерных систем», с указанием научных успехов ТюмГУ и ВКА им.А.Ф.Можайского;
- эволюционные элементы унивалентной математики в начале XXI века;
- история создания, эволюция и синергетические успехи DARPA;
- историческая эволюция спецификаций LTE;
- перечисление основателей онтологического моделирования и проектирования в нашей стране и за рубежом (Н.Гуарино, Л.В.Массель, Л.В.Найханова и др.) [1, с. 109, 195, 226, 254-256, 259, 266, 283, 308, 360, 246].

Что касается *учебно-методических* фрагментов книги, то их достаточно, чтобы подготовить отдельное учебное издание. Например, в книге изложены:

- сравнительный анализ моделей потоковой обработки данных;
- обзор способов построения онтологий;
- основные стадии формирования и реализации системного проекта;
- особенности и варианты реализации SDN-сетей;
- ключевые особенности, механизмы, варианты реализации LTE;
- проблемные вопросы обеспечения безопасности информации в облачной среде и другие [1, с. 236, 245, 279, 302, 309, 317].

Теоретическая и прикладная значимость монографии, на наш взгляд, обусловлена представлением уже достигнутых отдельных теоретических успехов, иллюстрацией огромного числа



Источник: http://sicherheitstacho.eu

***Рис. 1.** Отображение векторов компьютерных атак в реальном времени*

концептуальных (семантических) формальных и полуформальных моделей, а также анализом ряда ИТ-решений. В первом вопросе наиболее ярко выделяется развитие основ теорий устойчивых вычислений и интеллектуальных программных сред, дополнение теории подобия новыми прикладными областями, исследование гипотезы технических аналогов иммунной системы живого организма. Также можно отметить критические обзоры Global SOC (Microsoft), линейки UTM-устройств Fortinet, ряда программных решений SAP, Oracle, IBM, Концерна РТИ, ряда аппаратных решений отечественных предприятий промышленности и др.

Дискуссионные моменты

Как отметили авторы, книга представляет первый публичный труд по заявленной тематике, именно поэтому значительный объем работы имеет постановочный характер. Разумеется, подобные работы вызывают большое количество разного рода рабочей критики и научные дискуссии - к чему и призывают нас авторы в заключении книги [1, с.383]. Исходя из этого, отметим некоторые рекомендации, вопросы и замечания строго по главам работы.

1. Прочитав аннотацию и введение, первое, что хочется отметить в концептуальном плане, так это лаконичность в базовых определениях. Например, не сразу понятно, что понимают авторы под *ранним предупреждением* ***о*** *компьютерном нападении*, так как - как известно - глобальное противоборство в киберпространстве давно происходит и перманентно, угрозы технологического превосходства – налицо (некоторые – надолго), вирусные эпидемии[6] и низкоинтенсивные целевые компьютерные атаки не прекращаются с прошлого века (рис. 1), наконец, даже механизмы предотвращения вторжений (intrusion prevention system) уже стандартизированы за рубежом[7] и у нас[8]. На наш взгляд, было бы более прозрачно для читателя, если бы авторы определили стадии киберконфликта и таксономию компьютерных нападений (КН), ну и вообще - метрики, показатели и критерии оценки указанного в названии целенаправленного процесса.

2. При обосновании *актуальности* в 1-ой главе авторами совершенно правильно обозначены субъективные и объективные причины сложившихся противоречий проблемной области. В то же время авторы ограничились демонстрацией *актуальной* статистики и трендов базовых факторов ИБ лишь по отдельным сегментам информационных систем (например, [1, табл.4]).

3. При описании во 2-ой главе *предельных возможностей известных технологий контроля и мониторинга* можно было бы, на наш взгляд, уделить больше внимания консолидации указанных и других технологий в целях получения синерге-

6 https://www.anti-malware.ru/interviews/2017-07-19/23461
7 http://dx.doi.org/10.6028/NIST.SP.800-94
8 http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty/407-metodicheskie-dokumenty-utverzhdeny-fstek-rossii-6-marta-2012-g

Таблица 1.
Этапы развития госпрограммы EINSTEIN Program

Программа	Год	Технологии
Einstein 1	2004	Мониторинг трафика федеральных гражданских ведомств с целью выявления подозрительного трафика и расследования инцидентов
Einstein 2	2008	Система обнаружения вторжений на основе сигнатур
Einstein 3	2010	Изначальный план: реализация функционала предотвращения вторжений
	2012	Смена подхода: основные Интернет-провайдеры должны предоставлять федеральным агентствам сервисы предотвращения вторжений на основе коммерческих технологий

тического эффекта. Например, технической базой такой консолидации являются SIEM[9]-системы, а используемые ими методы корреляции событий и методы принятия антиципационных (пользуясь терминологией авторов) решений сейчас представляют значительное внимание в научно-практическом плане. Следует добавить, что SIEM-решение является и ядром центров ГосСОПКА и СПОКА[10], но, конечно, не единственным их компонентом - монография бы выиграла (в прокладном плане) в случае представления авторами результатов анализа всех процессов, компонент и сегментов указанных ситуационных центров именно *по информационной безопасности*.

4. При обосновании в главе 3 *возможных научно-технических решений проблемы раннего предупреждения* авторы делают упор на внедрение отечественной суперкомпьютерной платформы, что несомненно важно и очень отрадно. Однако роль и место суперЭВМ в предлагаемой системе раннего предупреждения о КН, а также собственно архитектура этой системы, представлены несколько размыто. Было бы интересно, если бы авторы как-то конкретизировали этот момент с научной точки зрения. Например, в США хорошо известен гражданский компонент глобальной системы мониторинга *по информационной безопасности* - Einstein 3.0[11], сервисно реализуемый в настоящее время на уровне провайдеров (табл.1). С другой стороны, в литературе [12] хорошо описаны госпрограммы США (например, PRISM[12]), основанные на датацентрах (типа, Utah Data Center), выполняющих несколько иные задачи[13].

5. При описании в главе 4 *перспективных поисковых исследований в области ИБ и раннего предупреждения о КН* авторы затронули вопросы построения доверенной облачной среды (в контексте предупреждения о КН), эквивалентной СВТ-1 («верифицированная защита»[14]) [1, с. 321]. Можно рекомендовать доведение указанного теоретического утверждения до практической реализации и внедрения, что может иметь важное «прорывное» значение для отрасли.

6. Что касается приложения к книге, основанное на теории подобия, то предлагаемая общая методика несомненно имеет весьма важное теоретическое значение и научный интерес, однако, остается открытым (вечный) вопрос обеспечения полноты факторов моделей (построения графа всех взаимодействующих баз, библиотек и протоколов в системе), так как при обеспечении полноты задача моделирования критически усложняется, при выборочном решении – конгруэнтные методики уже известны.

Несмотря на возникшие вопросы и рекомендации, в данном первом издании монографии авторами поднята несомненно важная проблема, заключающаяся в постановке *комплекса сложно связанных задач принципиального характера, отличающихся высокой степенью неопределенности*. Здесь можно напомнить определение проблемы, введенное академиками Новиковым А.М. и Новиковым Д.А., как «*знание о незнании*» [13, с.68].

Прочитав книгу, остается чувство, что ее отдельные подразделы хочется перечитать еще раз. Это связано с тем, что авторам реально хочется и есть что сказать и поделиться некоторым опытом, что важно в сложившейся ситуации динамичности противостояния в киберпространстве. И здесь снова следует согласиться с редактором книги, который призывает ее рассматривать в качестве «*информации к размышлению, введению в очень*

9 В то же время сокращение SIEM фрагментарно встречается в работе 23 раза.
10 https://lenta.ru/news/2016/10/24/cyberattack/
11 https://www.dhs.gov/einstein
12 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
13 https://ria.ru/world/20130707/948121011.html
14 http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2

важную, сложнейшую, но, безусловно, интереснейшую научно-техническую проблематику» [1, с.11].

Заключение

В представленной читателю монографии затронута крайне актуальная и важная проблема эффективного противостояния страны в киберпространстве угрозам и вызовам информационной сферы, решение которой связывается с выполнением ряда задач раннего выявления уязвимостей, угроз, рисков и инцидентов в области ИБ, а также принятия соответствующих управленческих решений, в первую очередь, опираясь на интеллектуальные методы анализа данных и эффективные вычислительные архитектуры.

Книга насыщена разного рода интересными событиями и фактами, описанием передовых практик в нормативном и технологическом плане, оригинальными примерами формальных и полуформальных моделей предметной области, а также примерами разрешения смежных научных задач, пограничных к проблематике.

Книга легко читается и местами весьма увлекательна. Полезна ученым, учащимся и увлекающимся тематикой глобального киберпротивоборства, независимо от научной отрасли. Руководителям высшего звена перспективных объектов информатизации федерального и регионального характера - ознакомиться обязательно.

Литература:

1. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении. / Под общей редакцией С.Ф.Боева; вводные слова А.И.Смирнова и А.Г.Тормасова; вводная статья И.А.Каляева. – Иннополис: Издательский Дом «Афина», 2017. 440 с.
2. Юсупов Р.М., Пальчун Б.П. Безопасность компьютерной инфосферы систем критических приложений // Вооружение. Политика. Конверсия. 1993. № 3. С. 23-31.
3. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. - СПб.: Питер, 2001. - 848 с.
4. Кларк Р, Нейк Р. Третья мировая война: какой она будет? Высокие технологии на службе милитаризма. СПб.: Питер, 2011. - 336 с.
5. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1 (1). С. 10-16.
6. Безкоровайный М.М., Татузов А.Л. Кибербезопасность и информационная безопасность: общие свойства и отличия // Информатизация и связь. 2016. № 4. С. 113-124.
7. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1 (2). С. 28-35.
8. Агапов А.М., Новиков Г.А., Снытников А.А., Смирнов С.Н. Ситуационно-кризисный центр: теоретические основы и практический опыт создания и эксплуатации / Предисловие Н.П. Лавёрова. - М.: Гелиос АРВ, 2014. - 304 с.
9. Боев С.Ф., Ступин Д.Д., Сухарева А.Н. Некоторые особенности инновационных процессов в оборонно-промышленном комплексе страны // Известия Московского государственного технического университета МАМИ. 2015. Т. 5. № 4 (26). С. 115-119.
10. Петренко С.А. Создание национальной системы раннего предупреждения о компьютерном нападении. В сборнике: Безопасные информационные технологии (БИТ-2016). Сборник трудов Седьмой Всероссийской научно-технической конференции. / Под редакцией В.А. Матвеева. 2016. С. 232-237.
11. Ступин Д.Д., Петренко С.А. Концепция создания когнитивной системы раннего предупреждения о компьютерном нападении. В сборнике: Суперкомпьютерные технологии (СКТ-2016) Материалы 4-й Всероссийской научно-технической конференции. В 2-х томах. 2016. С. 103-107.
12. Харрис Ш. Кибер войн@. Пятый театр военных действий/Пер. с англ. -М.: Альпина нон-фикшн, 2016. -390 с.
13. Новиков А.М., Новиков Д.А. Методология. Изд.2-е, испр. - М.: КРАСАНД, 2014. - 632 с.