Скрипкин С.К.

ГИПЕРБЕЗОПАСНОСТЬ

Анотація:

Вводиться поняття гіпербезпека як нелінійна цільова сутність сучасних засобів захисту складних соціо-технічних систем, більш адекватна в умовах розвитку засобів ведення інформаційних війн нових поколінь. Основою реалізації гіпербезпеки на сучасному етапі являються нелінійні активно-адаптивні інфраструктури корпоративних інтрамереж з інтелектуальним управлінням. Надалі очікується поява та активне застосування складних захисних та шкідливих гіперкомплексів, складених із найрізноманітніших елементів ведення конкурентної боротьби.

Аннотация:

Вводится понятие гипербезопасность как нелинейная целевая сущность современных средств защиты сложных социо-технических систем, более адекватная в условиях развития средств ведения информационных войн новых поколений. Базой реализации гипербезопасности на современном этапе являются нелинейные активно-адаптивные инфраструктуры корпоративных интрасетей с интеллектуальным управлением. В дальнейшем ожидается, появление и активное применение сложных защитных и вредоносных гиперкомплексов, составленных из самых разнообразных элементов ведения конкурентной борьбы.

Abstract:

The concept hypersecurity as nonlinear target essence of modern means of protection of difficult sotsio-technical systems more adequate in the conditions of development of means of conducting information wars of new generations is entered. Base of realization of hypersecurity at the present stage are nonlinear active and adaptive infrastructures of corporate intranets with intellectual management. Further it is expected, emergence and active application of the difficult protective and harmful hypercomplexes made of the most various elements of conducting competitive fight.

Введение

В результате экономических достижений в ряде стран уже идет очередная технологическая революция, позволяющая формировать новую материально-техническую базу ведения информационных войн в XXI веке, основу которой составляют высокие наукоемкие технологии и информационные системы. При этом важнейшую роль играют сенсорная и квантовая техника, а также новые технологии производства (3d-принтеры) и применение новых информационных технологий с новыми свойствами (Веб вещей, «умные» вещи, персональные «облака», «облака» в «облаках» и др.). При этом создаются не имеющие аналогов виды кибероружия, способные не только заменить старое вооружение, но и полностью изменить характер войн в целом. Передовые технологии позволяют создать принципиально новые возможности для эффективного ведения конкурентной борьбы.

В ИСЭМ СО РАН за многие годы исследований накоплен значительный интеллектуальный опыт исследования энергетической безопасности, прогнозирования развития

сложных энергетических систем. В настоящее время для решения задач разработки новой технологической платформы ЕЭС России – интеллектуальной энергосистемы с активно-адаптивной сетью (ИЭС ААС) – проблема обеспечения безопасности энергосистем смещается в область обеспечения информационной и кибербезопасности [1,2].

В статье рассматриваются проблемы обеспечения более высокого уровня безопасности в современных условиях, основные виды опасностей, а также проблема выявления и устранения уязвимостей информационных систем в условиях современных информационных войн.

Гипербезопасность (сверхбезопасность) рассматривается как состояние, характеризующее степень комплексной защиты, обеспечивающей не только информационную составляющую безопасности, но и значительную часть всей пирамиды безопасности [3] современного общества.

Генезис развития антропных систем, то есть филогенетически, проблемы обеспечения безопасности возникли не мгновенно, а появлялись исторически последовательно и имеют явную иерархическую структуру. Имеющиеся на современном этапе филогенеза проблемы безопасности объекта задаются онтогенетически все сразу, но каждая – с разной степенью интенсивности. Каждая антропная система решает одновременно свои задачи защиты от всех видов реальных опасностей. В [3] предложен один из возможных вариантов классификации феномена комплексной безопасности, объектом которой является антропная система любого структурного уровня сложности: от отдельного индивида, предприятия, организации, учреждения, государства или союза государств, до всего человечества.

Главные достоинства предложенной классификации – четкое указание на активные объекты, безопасность которых исследуется, т.е. антропные системы, и единое основание классификации – степень влияния опасностей на жизнь и жизненно важные функции каждой антропной системы. Основные уровни опасностей в пирамиде безопасности: (7) консциентальная; (6) психическая; (5) политическая; (4) экономическая; (3) энергетическая; (2) продовольственная; (1) экологическая.

Консциентальная опасность наиболее актуальна и связана с разрушением мудрости общества и государства на основе искажения и подмены целей в сознании людей (разрушения этноконфессиональной и цивилизационной идентичности). Проблема имеет несколько измерений: 1) сохранение национальной идентичности в условиях превращения либерализма в тотальную идеологию; 2) удержание органического этнографического поля взаимоотношений людей; 3) выработка более глубоких форм идентичности для участия в межцивилизационных диалогах; 4) формирование здоровых форм сознания и состязательности при решении глобальных задач и эффективного взаимодействия с другими нациями с целью устойчивого развития и др.

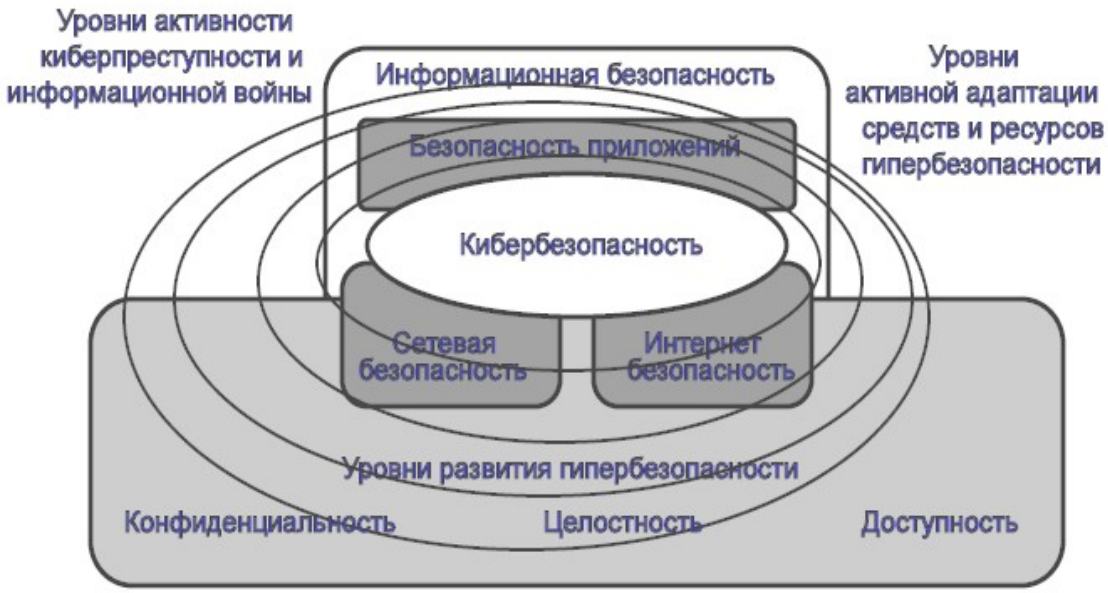

Рис. 1 Связь основных понятий гипербезопасности

Кибербезопасность рассматривается как один из основных компонентов гипербезопасности и характеризует степень защищенности киберсреды, ресурсов организаций и пользователей. Понятие кибербезопасности тесно связано с разными факторами и элементами более общего понятия безопасности (рис. 1) и является ядром эволюционирующей гипербезопасности от вредоносных гиперкомплексов.

Исходными задачами систем обеспечения безопасности считаются: доступность, целостность и конфиденциальность информационных ресурсов. Кибербезопасность является необходимым условием современного этапа развития информационного общества и включает более широкий спектр задач.

Недостатки современного подхода к кибербезопасности

Следует в первую очередь признать устаревшим традиционное деление на активные и пассивные сущности (субъекты и объекты в привычной терминологии). В кибербезопасности пассивных объектов нет. Все объекты активны одновременно и при необходимости каждым используются функции и ресурсы других активных объектов. Причем используются не только от имени пользователя, но и от имени среды.

Так как реализации объектов кибербезопасности более интегрированы, то их нельзя рассматривать как инструменты выполнения задач пользователей. Пользователь прямо или косвенно «просит» некоторый объект об определенной услуге. Объект действует скорее от имени (во всяком случае, по воле) своего создателя, чем от имени вызвавшего его пользователя. Можно считать, что объекты обладают достаточной «свободой воли», чтобы выполнять действия, о которых пользователь не только не просил, но даже не догадывается об их возможности. Особенно это справедливо в сетевой среде и для программного обеспечения (ПО), организованного как фраймвоки, имеющие свое поведение.

Современное состояние в области кибербезопасности и информационной безопасности характеризуется как состояние дискретного (поколения) и непрерывного (градиентного) развития информационных войн различного вида и уровня. Под этим подразумевается комплексное информационное воздействие на систему государственного и военно-

го управления, изменяющее в нужном направлении функционирование структуры управления, либо вообще парализующее это управление при необходимости. Наряду с этим наступательным фактором государства стремятся к обеспечению защиты национальной информационной инфраструктуры.

В результате развития информационных, телекоммуникационных и интеллектуальных технологий в настоящее время изменилась стратегия и тактика ведения современных информационных войн, появились концепции, учитывающие факторы информационной и интеллектуальной уязвимости сторон. Ускоряющаяся динамика развития, предоставление широких возможностей возникновения уязвимостей информационной инфраструктуры постиндустриального общества создают множество проблем в различных сферах, прежде всего в области международной, национальной и энергетической безопасности. Возрастает зависимость процессов, происходящих в различных областях человеческой деятельности, от качества функционирования информационно-коммуникационных сетей и циркулирующих в них знаний.

Появление информационного оружия, в официальной трактовке, принципиально меняет механизм эскалации вооруженных конфликтов, так как даже выборочное применение информационного оружия по объектам военной и гражданской информационной инфраструктуры противника может завершить конфликт на его ранней стадии, еще до начала активных боевых действий. Обладание информационным оружием обеспечивает военно-стратегическое преимущество над обществами, у которых его нет.

Кибернетическая борьба (warfare) охватывает полный комплекс проблем и аспектов (организационные, доктринальные, стратегические, тактические, технические) ведения информационных операций и в настоящее время становится все более актуальной именно в глобальной сфере. При этом понятие кибернетической борьбы относится скорее к организационной форме информационного противоборства, чем собственно к борьбе с информационной инфраструктурой противника. Более того, кибервойна подразумевает использование ИТ-инфраструктуры противника в своих целях.

Основные генетические архетипы методов и средств информационной борьбы:

- 0GW – нулевое поколение (естественный отбор в животном мире)
- 1GW – первое поколение (информационная борьба на бытовом уровне)
- 2GW – второе поколение (ситуационная борьба регулярных сил)
- 3GW – третье поколение («холодная” войн»)
- 4GW – четвертое поколение (война цивилизаций)
- 5GW – пятое поколение (глобальная конкуренция)
- xGW – градиентные уровни современной кибервойны (0MGW – 5MGW), соответствующие генетическим архетипам (рис. 2).

Особенности современной кибервойны:

- охватывает в качестве самостоятельных объектов (мишеней) все виды информации и информационных систем;
- ведется как при объявлении войны, так и в кризисных ситуациях в самых различных сферах жизнедеятельности;
- ведется как специализированными военными, так и гражданскими структурами;
- киберобъекты могут выступать и как объект защиты, и как оружие, если защита не сработала, тем самым расширяя пространство ведения кибервойны.

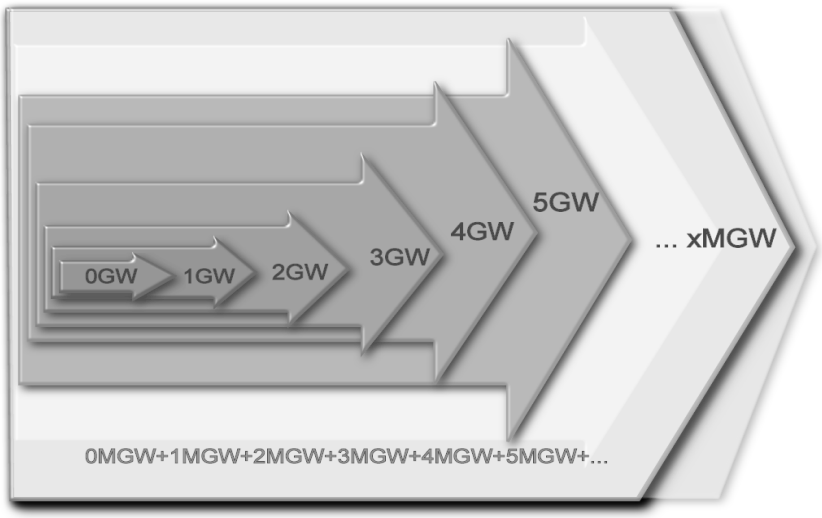

Рис. 2 Интенсивность информационных войн разных поколений

Уязвимости в кибервойне

Понятие уязвимость (англ. vulnerability) применяется для обозначения недостатка в системе. Используя его, можно нарушить её целостность и провести атаку на защищенные ресурсы. Уязвимость может быть результатом ошибок, недостатков, допущенных при проектировании системы, ненадежных паролей, действий множества типов вредоносных программ. Некоторые уязвимости известны только теоретически, другие активно используются и имеют известные эксплойты (эксплуатируемые уязвимости).

В общем случае, уязвимость ассоциируется с нарушением политики безопасности, вызванным неправильно заданным набором ее правил или ошибкой при указании целей. Теоретически все компьютерные системы имеют уязвимости самой различной природы. Но то, насколько велик потенциальный ущерб от атаки, использующей уязвимость, позволяет подразделять уязвимости на активно используемые (высокие уровни риска) и не используемые вовсе (безопасные). Оценка риска может быть определена как **риск = угрозы * уязвимости*ценность ресурса** (объемная модель риска).

Обычно уязвимости позволяют атакующему «обмануть» приложения – заставить их совершить действия, на которые у них нет ни целей, ни прав. Это делается путем внедрения каким-либо образом в программы данных или кодов в такие места, что программа воспринимает их как «свои». Некоторые уязвимости появляются из-за недостаточной проверки данных и позволяют вставить в интерпретируемый код произвольные команды и осуществлять вторжения в высоко защищенные информационные системы.

Определение состава угроз

Подход в определении безопасности через угрозы и их источники достаточно распространен, но при этом отсутствует единая методология в определении киберугроз, их отношения между собой, что указывает на необходимость разработки целостной теории угроз [4]. Если раньше угрозы носили внешний и военный характер, когда невоенные и военные средства практически невозможно было применять комплексно, то сейчас в условиях взаимозависимого мира и общемировых технологий угрозы кибербезопасности носят комплексный характер.

Технология проведения кибератак в информационно-коммуникационные сетях различных типов достаточно хорошо изучена и состоит из приемов и методов организа-

ции вторжений на ключевые узлы для нанесения наиболее значительного ущерба объектам соответствующей инфраструктуры. Кроме традиционных угроз информационной безопасности возникают принципиально новые, например, угроза использования пораженной информационной инфраструктуры для достижения целей противника и выполнения его задач.

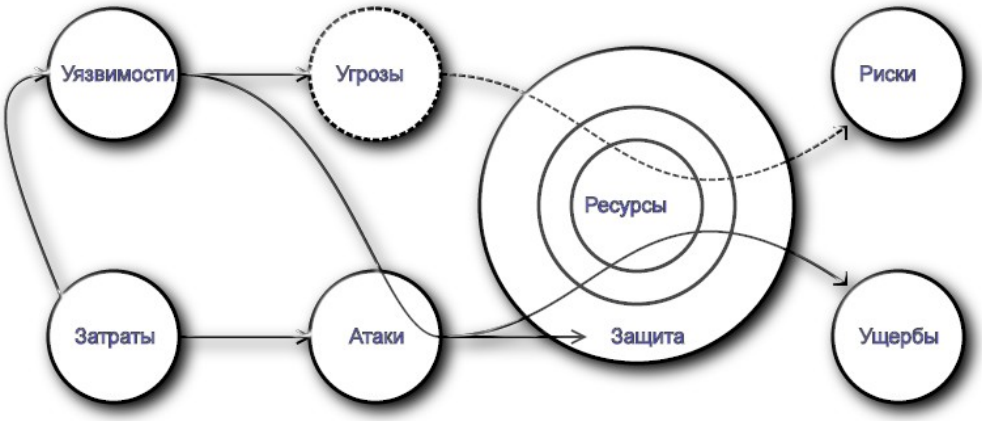

Рис. 3 Связи основных категорий гипербезопасности

Проблема обеспечения гипербезопасности – комплексная, защищать приходится сложные инфраструктуры, и сами защитные средства не менее сложны. Если три грани кибербезопасности – это доступность, целостность и конфиденциальность, то гипербезопасность значительно многогранней. Каждую грань на начальном этапе можно рассматривать относительно независимо, и считается, что если все они обеспечены, то обеспечена и гипербезопасность в целом. Вместе с тем, необходимо учитывать нелинейные системные эффекты (эмерджентность), особенно в процессе изменения среды, характерные для активной адаптации.

Как и средства достижения информационной безопасности, средства кибербезопасности и гипербезопасности могут использовать:

1. Международные договоры, стандарты информационного обмена;
2. Законодательные меры обеспечения кибербезопасности;
3. Административные политики руководства организаций;
4. Процедурные меры, ориентированные на людей;
5. Программно-технические меры с применением онтологического пространства безопасности и языка энергетических систем [4,5].

Меры и средства можно рассматривать и как результат варьирования уровня детализации («международный уровень», «законодательный уровень», «процедурный уровень» и т.п.) [6]. Законы и нормативные акты ориентированы на всех субъектов отношений независимо от их организационной принадлежности (это могут быть как юридические, так и физические лица) в пределах страны (международные конвенции имеют даже более широкую область действия), административные меры – на всех субъектов в пределах организации, процедурные – на отдельных людей или небольшие категории субъектов, программно-технические – на оборудование и программное обеспечение. При такой трактовке в переходе с уровня на уровень можно усмотреть применение наследования (каждый следующий уровень не отменяет, а дополняет предыдущий), а также полимор-

физма (субъекты выступают сразу в нескольких ролях – например, как инициаторы административных мер и как обычные пользователи, так и как нарушители (злоумышленники).

Для всех выделенных граней действует принцип инкапсуляции – грани «относительно независимы» и две совокупности граней можно назвать ортогональными, поскольку для фиксированной грани в одной совокупности грани в другой совокупности должны пробегать все множество возможных значений (нужно рассмотреть соответствующие международные, законодательные, административные, процедурные и программно-технические меры).

Обычно интересы субъектов отношений гипербезопасности концентрируются вокруг отдельных организаций, располагающих территориально разнесенными производственными узлами, на каждом из которых есть серверы, обслуживающие своих (интранет) и внешних пользователей (экстранет), а также пользователи, нуждающиеся во внутренних и внешних сервисах. Одна из площадок оборудована внешним подключением (то есть имеет выход в Internet).

Наиболее слабыми элементами с точки зрения безопасности являются все ресурсы, использующие файлы (файловые системы), возникшие задолго до появления современных вредоносных средств и не обеспечивающие требования кибербезопасности. Как универсальный элемент организация данных с операциями READ, WRITE, RUN (читать, писать, запускать) имеет фундаментальный дефект, упрощающий задачу записи и запуска любых вредоносных средств. Значительно более безопасными зарекомендовали себя структуры данных с операциями READ/WRITE для объектов типа документ и операцией RUN для программ.

Использование MIME-типов для явного указания форматов кодирования данных в сопровождении электронных писем и сетевых объектов мультимедиа раскрывают формат кодирования информации для вредоносных средств, облегчая манипулирование скрытым вредоносным кодом и распространяют дефекты файловых систем на распределенные и сетевые структуры данных.

Злонамеренные гиперкомплексы

Современная кибербезопасность предоставляет множество примеров распространения в сетях симбиозов вредоносных средств разных классов. Одни из них используются для более широкого распространения (телевидение, кинематограф, интернет), другие – для менее затратной организации и проведения атак, третьи – для нанесения либо максимального по стоимости ущерба, либо ущерба заданного типа. Наиболее широкое распространение получили симбиозы компьютерных вредоносных средств и вирусов сознания [7]. Начинают прослеживаться первые интеграционные связи информационных и биологических агентов (например, «птичий», «свиной» грипп), разработка генетического оружия против отдельных народов. Конечно, еще рано ожидать широкой интеграции биологических и компьютерных вредоносных агентов с распространением эпидемий человека через Internet, но пример психологической зависимости от Internet говорит о том, что мост переброшен и рано или поздно, по мере дальнейшей компьютеризации это неминуемо должно произойти.

Защитные гиперкомплексы

Существуют разнообразные инструментальные средства, которые могут обнаруживать уязвимости в системе. Примером таких средств являются системы IDPS – Intrusion Detection Prevention System. Типовая среда обнаружения и предотвращения вторжений для сетей офисных зданий представлена на рис. 4.

Хотя некоторые инструменты могут обеспечить хороший обзор возможных уязвимостей, существующих в системе, они не могут заменить участие человека в их оценке. Уязвимости обнаруживались во всех широко используемых операционных системах, включая Microsoft Windows, Mac OS, различные клоны UNIX (в том числе GNU/Linux). Все новые уязвимости обнаруживаются непрерывно и основной путь уменьшить риски их использования против любой системы – активно-адаптивное обнаружение и предотвращение вторжений.

Рис. 4 Среда обнаружения и предотвращения вторжений IDPS

Обнаружение вторжений (IDS) включает мониторинг событий, происходящих в активно-адаптивной сети, их анализ на наличие признаков, указывающих на попытки вторжения – нарушения конфиденциальности, целостности, доступности. Предотвращение вторжений (IPS) включает как процессы активной блокировки выявленных вторжений, так и накопление знаний об особенностях атак и злоумышленниках для ускорения предотвращения и минимизации последствий. Средства обнаружения и предотвращения вторжений (IDPS) автоматизируют данные процессы и необходимы в защищенной сети любого уровня, чтобы минимизировать риск ущерба и потерь, к которым могут привести вторжения.

Активно-адаптивные гиперкомплексы в электроэнергетике

В соответствии с программами развития энергетики рассматриваются различные концепции построения интеллектуальных систем передачи и распределения электроэнергии, известные в Европе и США под названием Smart Grid, основная цель которых – оптимизировать энергопотребление при сохранении надежности и устойчивости работы электрических сетей.

В нашей стране предполагается развитие такой технологии на магистральных сетях, модернизации которых с использованием новых инновационных технологий также

уделяется особое внимание. При этом разрабатываются решения, позволяющие преобразовать пассивную в настоящее время магистральную сетевую инфраструктуру в главный интеллектуальный компонент электроэнергетической системы с активно-адаптивными сетями. Для этого необходимо развитие и внедрение не только технических средств и приборов автоматизации, измерения, учета параметров электроэнергии, но и формирование многоуровневой и гибкой системы кибербезопасности. Активно-адаптивные свойства такого защитного гиперкомплекса должны соответствовать решаемым задачам.

Сервисные модели пока являются главными средствами для достижения поставленных целей. Облака пока стоит рассматривать как перспективы поворота всей индустрии к защищенным сетевым сервисам.

Заключение

Вводится понятие гипербезопасность как нелинейная целевая сущность современных средств защиты сложных социо-технических систем, более адекватная в условиях развития средств ведения информационных войн новых поколений. Базой реализации гипербезопасности на современном этапе являются инфраструктуры корпоративных защищенных интрасетей. В дальнейшем ожидается, появление и активное применение сложных распределенных защитных и вредоносных гиперкомплексов, составленных из самых разнообразных элементов ведения конкурентной борьбы.

Исследования проводятся при поддержке гранта РФФИ № 13-07-00140а «Методология создания и интеграции интеллектуальных, агентных и облачных вычислений в Smart Grid (умных энергетических системах)».

Литература:

1. Воропай Н.И. Интеллектуальные электроэнергетические системы: концепция, состояние, перспективы / Н.И. Воропай // Автоматизация и IT в энергетике. – 2011. – №3. – С. 11–16.

2. Массель Л.В. Интеллектуализация поддержки принятия решений при моделировании и управлении режимами в Smart Grid / Л.В. Массель // Интеллектуализация обработки информации: Труды 9-й Международной конференции. – Черногория, Будва, 2012. – С. 692–695.

3. Атаманов, Г.А. Основные виды безопасности антропных систем и их иерархия / Геннадий Альбертович Атаманов // Материалы и публикации о безопасности [Электронный ресурс]. – Режим доступа: http://www.naukaxxi.ru/materials/author/52.

4. Скрипкин С.К. Кибербезопасность в условиях информационных войн новых поколений / С.К. Скрипкин // Информационные и математические технологии в науке и управлении. Труды XVII Байкальской Всероссийской конференции «Информационные и математические технологии в науке и управлении». Ч.III. – Иркутск: ИСЭМ СО РАН, 2013. – С. 127–134.

5. Скрипкин С.К. Онтологическое пространство безопасности / С.К. Скрипкин // Информационные и математические технологии в науке и управлении. Труды XVI Бай-

кальской Всероссийской конференции «Информационные и математические технологии в науке и управлении». Ч.III. – Иркутск: ИСЭМ СО РАН, 2012. – С. 127–134.

6. Кузнецов Н. Информационная безопасность систем организационного управления / Н. Кузнецов // Теоретические основы. Т. 1. – Москва: Наука, 2006. – 495 с.

7. Лайт С. Вирусы сознания. Принципы и методы исцеления души и тела / Сан Лайт. – М.: Мир Детства, 2010. – 176 с.