ПРОБЛЕМЫ И ПАРАДОКСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ МЕНЕДЖМЕНТЕ

УДК 004.056.5

Елена Петровна Гусева,
к.э.н., доцент, доцент кафедры Общего менеджмента и предпринимательства, Московский государственный университет экономики, статистки и информатики
Эл. почта: epguseva@mesi.ru

Целью данной статьи является исследование проблем и парадоксов информационной безопасности (ИБ) в современном, прежде всего, российском менеджменте, а так же проблем и парадоксов сохранения информации, её защиты от угроз, гарантии полноты и точности выдаваемой информации, минимизации её потерь и искажений. Рекомендация применения SMART-менеджмента в службах обеспечения ИБ.

Ключевые слова: SMART-менеджмент, информация, безопасность, проблемы, парадоксы, защита, Интернет, концепция, организация.

Elena P. Guseva,
PhD in Economics, Associate Professor, the Department of General Management and Entrepreneurship, Moscow State University of Economics,Statistics and Informatics
E-mail: epguseva@mesi.ru

PROBLEMS AND PARADOXES OF INFORMATION SECURITY IN MODERN MANAGEMENT

The aim of this article is to study the problems and paradoxes of information security (IS) in a modern, first of all, the Russian management, and preservation of information and its protection from threats, guarantee of completeness and accuracy of the output data, minimize its losses and distortion. The recommendation of application of SMART management in services of providing IB.

Keywords: SMART management, information, security, problems, paradoxes, protection, Internet, conception, organization.

1. Введение

Менеджмент, как любая другая наука и практическая деятельность в современных условиях, не может обходиться без информации. [Подробности о взаимосвязи менеджмента и информационной безопасности были изложены в статье: «Менеджмент: аспекты информационной безопасности, прозрачности и доверия к информации», опубликованной в журнале «Экономика, Статистика и Информатика. Вестник УМО №5, 2012 г. – С. 174».] Информация – важнейший экономический ресурс каждой организации. Без неё уже не возможно социальное, экономическое, техническое, технологическое, интеллектуальное и др. виды развития любой системы. Поэтому исследование *проблем и парадоксов* ИБ в условиях информационного общества весьма актуально. ИБ информационно-технологических сетей и систем (ИТС) в современном российском менеджменте для экономики, основанной на знаниях, входит в число первоочередных стимуляторов повышения эффективности производства продукции и услуг. Но в практической деятельности это теоретическое положение сталкивается с определёнными проблемами, обусловленными фактическими условиями и конкретными возможностями функционирующих в нашей стране организаций и частных предпринимателей.

Не везде развиты информационно-коммуникационные технологии (ИКТ), нет опыта ИКТ-менеджмента у предпринимателей и у руководства многих организаций, прежде всего, средних и малых, трудно прогнозируемая динамика деятельности делового и особенно фонового окружения, недостаточная надёжность ИБ, т.к. не построена комплексная система управления ИБ.

По мере совершенствования ИТС проблемы их безопасного использования стремительно возрастают и становятся всё актуальнее с каждым годом.

В настоящее время в условиях информационного бума мировой опыт показывает, что проблемы и парадоксы ИБ в современном менеджменте тормозят ускорение экономического роста.

В современном российском менеджменте на всех его уровнях с ИБ связано очень много проблем и парадоксов, но дефицит времени позволяет рассмотреть только некоторые из них [1, 2, 3, 4, 5, 6].

2. Проблемы и парадоксы информационной безопасности после интеграции России в глобальные процессы

В настоящее время с его сверхбыстрыми, сверхточными и сверхсложными переменами во всех сферах менеджмента при все более обостряющейся конкуренции, глобальной полиинформации, как никогда ранее, возрастает значение информационной безопасности, связанное также с информационно-технологическими сетями и системами (ИТС). Парадоксальность позитива Интернета заключается в том, что он одновременно вызывает опасность и в связи с ней угрозы личности, организации, Родине.

Менеджмент невозможен без действий с информацией: сбора, перемещения, обработки, хранения, накопления, организации доступа для поиска новой информации, использование информации – её формирования, для ограниченного круга пользователей. Владелец конфиденциальной информации стремится обезопасить её от несанкционированного доступа. Но появляются люди, которых обстоятельства могут толкнуть к поиску информации, доступ к которой ограничен определённым кругом сотрудников. Человеческий фактор при работе с информацией обусловливает необходимость дополнения стандартного набора функций для открытых систем ещё одной функцией – обеспечение ИБ. Именно противоправная деятельность людей стала источником угроз ИБ. Чаще всего нельзя предвидеть действия и поступки потенциального нарушителя. А иногда нарушителем является

специалист, от которого никогда не ожидали злостных правонарушений. Сами угрозы ИБ весьма разнообразны. Они «совершенствуются», изменяются, становятся более изощрёнными, непредсказуемыми, так как за ними стоит человеческий фактор. Специализирующиеся на проблемах ИБ, выделили 4 вида основных последствий угроз: вскрытие, обман, разрушение, узурпация (захват). Результатом воздействия угроз становится нарушение ИБ ИТС. Следовательно, обратная сторона «медали» под названием Интернет, беспрепятственное и бесконтрольное проникновение в сетевые и информационные ресурсы и даже их разрушение посредством услуг ИТС.

Информационные связи между пользователями позволяют группам пользователей решать задачи моделирования сложных систем, выполнять проектные и др. работы, опирающиеся на распределенные между многими компьютерами программное обеспечение и базы данных. Таким образом, сетевая обработка и хранение данных – качественно новая организация обработки, при которой в значительной мере увеличиваются проблемы, связанные со сложностью и скоростью решения задач, требующих участия большого числа пользователей.

ИТС способствует повышению уровня загрузки компьютеров, программного обеспечения и баз данных, что обеспечивается следующим:

1. ИТС обслуживает значительное число специалистов, поэтому нагрузка, создаваемая всеми ими, в меньшей степени подвержена колебаниям, чем нагрузка, создаваемая одним человеком или небольшой группой людей. Данный эффект можно статистически измерить, рассчитав дисперсию среднего значения нагрузки, создаваемой работающими с компьютерами. Например, среднее квадратическое отклонение нагрузки, создаваемое одним человеком, равно «*a*», то «*n*» людей создадут суммарную нагрузку, среднее квадратическое отклонение которой равно $a\sqrt{n}$, т.е. колебания нагрузки, создаваемой, например, 10000 людьми, в 100 раз меньше, чем у создаваемой одним человеком. Таким образом, растет вероятность того, что в каждый момент времени есть работа для каждого компонента сети, т.е. загрузка сети увеличивается;

2. Загрузка сети становится стабильной, когда сеть охватывает территорию, расположенную в нескольких часовых поясах. Эффект стабилизации особенно существенен для эксплуатации специализированных и проблемно-ориентированных компьютеров, аналого-цифровых вычислительных комплексов, информационно-справочных систем и т.д.

Опыт показывает, что за счет расширения возможностей обработки информации и лучшей загрузки ресурсов себестоимость обработки информации средствами сети снижается в полтора раза и более в сравнении с обработкой данных на несвязанных компьютерах.

При маршрутизации в IP-сетях возникает проблема нехватки IPv4-адресов.

Блок-схема алгоритма маршрутизации пакетов в узле IP показана на рис. 1. Центральным элементом этой схемы является маршрутизационный вычислитель. На его вход поступают пакеты от вышележащих уровней (протоколы TCP, UDP), от системы разрешения конфликтных ситуаций – Internet Control Message Protocol, например, контрольное сообщение о потере пакета, от нижестоящих уровней через канальный интерфейс.

Маршрутизационный вычислитель работает с маршрутной таблицей (routing table), указывающая маршрут передачи пакета с заданным адресом, т.е. направляет либо в некоторый IP-узел (прямая маршрутизация), либо некоторому маршрутизатору (непрямая маршрутизация), либо в некоторую подсеть. При этом в маршрутной таблице определяется канальный интерфейс, через который должен быть передан пакет (у IP-узла, осуществляющего маршрутизацию, таких канальных (физических) интерфейсов может быть много).

Классическая Internet-архитектура вполне универсальна. Она предоставляет оптимальный способ доставки данных, посредством которого возможно создание весьма разнообразных прикладных и технологических сетевых систем. Практика позволяет разработчикам создавать стандарты с максимально целостной структурой. Решением проблемы нехватки IP-адресов является система IPv6-адресации, которая сохраняет принцип «сквозного соединения». [Подробности о протоколе IPv6 изложены в книге:

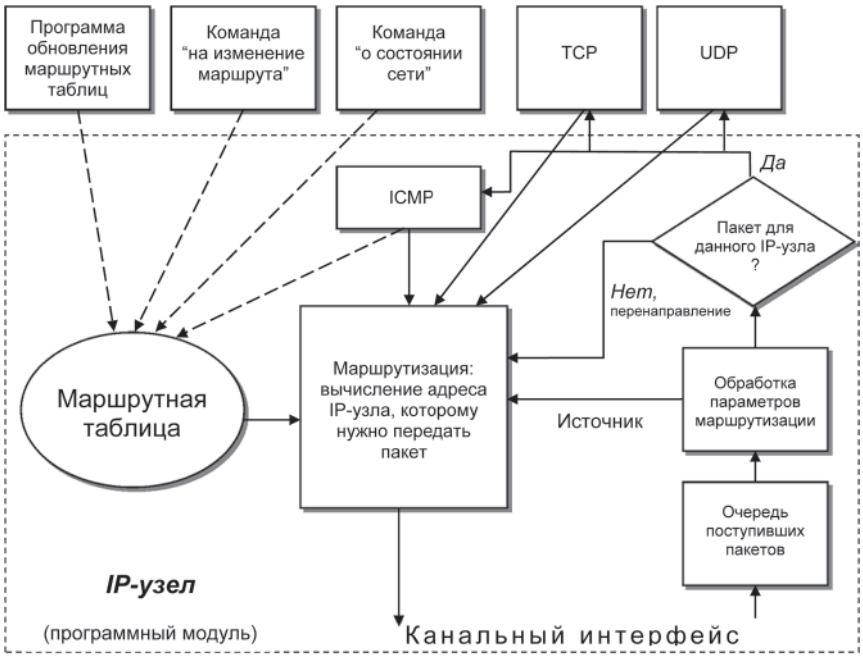

Рис. 1. *Блок-схема алгоритма маршрутизации пакетов в IP-узле.*

«Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем». – М.: Университетская книга, 2012. С.144–190]

3. Целесообразность SMART-менеджмента в службах обеспечения информационной безопасности

В буквальном смысле «SMART» в переводе с английского означает «умный», «сообразительный». Однако, в данном контексте это аббревиатура.

SMART (Specific – конкретность, специфичность, Measurable – измеримость, ощутимость, Achievable – достижимость, выполнимость, Realistic – реалистичность, Timely – своевременность, актуальность) – мнемоническая аббревиатура, используемая в менеджменте и проектном управлении для определения целей и постановки задач.

Следовательно, SMART-менеджмент можно рассматривать в том числе, в службах обеспечения ИБ, как эффективное управление, учитывающее конкретность ситуации, измеримость результатов, т.е. соотношение затрат с полученным эффектом; достижимость поставленных кратко- и долгосрочных целей обеспечения ИБ; актуальность решаемых проблем с учетом ограниченности во времени.

Организации и частные предприниматели в настоящее время выделяют огромные средства на содержание служб обеспечения ИБ, но эти средства далеко не всегда расходуются рационально. В связи с этим возникает целесообразность внедрения SMART-менеджмента в службы обеспечения ИБ (СОИБ).

Что же собой представляют СОИБ и чем они занимаются?

Но сначала несколько слов о документах, определяющих производственную деятельность СОИБ. Эти документы можно классифицировать на три группы:

1. Действующие законодательные акты и нормативные документы РФ по обеспечению ИБ;

2. Нормативные акты региональных (муниципальных) органов власти по обеспечению ИБ;

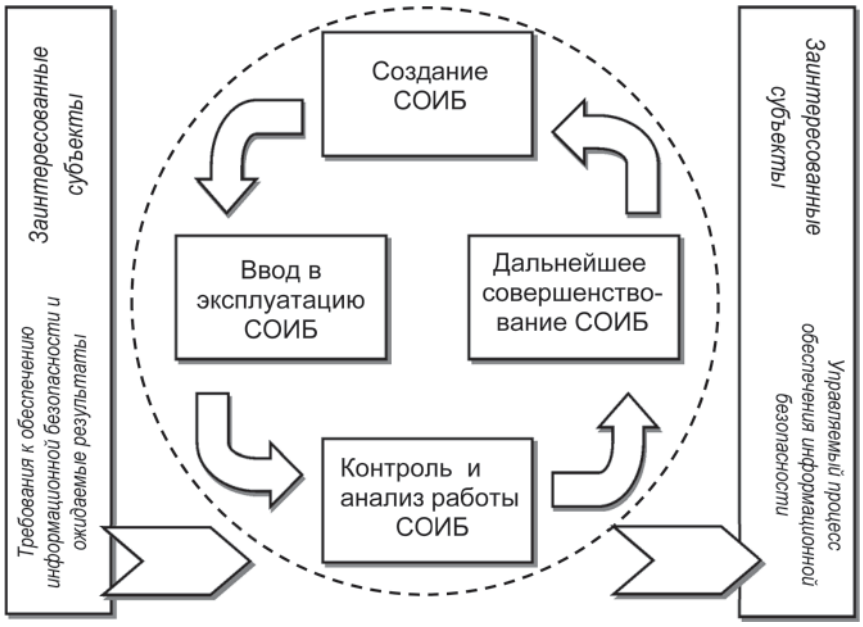

Рис. 2. *Рабочая модель служб обеспечения информационной безопасности организации.*

3. Внутренние документы организаций (предпринимательских структур) по обеспечению ИБ.

Теперь рассмотрим основные направления и принципы работы СОИБ ИТС в организациях.

В любой ИТС ведомства, концерна, фирмы, организации и др. (далее – организация) одним из направлений обеспечения надежного и достоверного информационного обмена и нормального функционирования самой организации является обеспечение ИБ. Иначе говоря, любая ИТС должна обеспечивать дополнительную функцию безопасности (помимо стандартного набора функций, определяемого архитектурой ИТС).

Обеспечение ИБ ИТС – это непрерывный процесс, направленный на достижение должного уровня ИБ. В целях организации обеспечения ИБ ИТС необходимо создать и в дальнейшем совершенствовать СОИБ, структура и функции которых будут напрямую зависеть от реализации основных направлений деятельности организации и наличия возможных угроз ИБ.

Основная цель и назначение СОИБ – реализация полнофункционального процесса обеспечения ИБ. Непрерывность процесса обеспечения ИБ достигается обеспечением его цикличности, что подразумевает реализацию представленной на рис. 2 модели функционирования СОИБ.

Рабочая модель СОИБ включает следующие процессы:

– Создание СОИБ начинается с разработки концепции СОИБ, целей их деятельности, процессов и процедур, относящихся к управлению рисками и совершенствованию самого процесса обеспечения ИБ.

– Ввод в эксплуатацию СОИБ и реализация стратегии обеспечения ИБ.

– Контроль и анализ работы СОИБ, измерение параметров процессов, непосредственно влияющих на обеспечение ИБ.

– Дальнейшее совершенствование деятельности СОИБ после внедрения SMART-менеджмента.

Руководство каждой организации несет ответственность за формирование, внедрение, обеспечение работы, текущий мониторинг, анализ обслуживания и совершенствования СОИБ посредством, главным образом, проведения внутренних аудиторских проверок СОИБ.

За обучение, осведомлённость и компетентность персонала несет ответственность руководство организации:

– Определяет необходимые компетенции на основе должностных

инструкций для менеджеров, обеспечивающих работу СОИБ.

– Организует обучение и другие мероприятия, связанные с необходимостью проведения в рамках организации или вне ее.

– Ведет учет компетентности, обучения, мастерства, опыта и квалификации SMART-менеджеров.

Руководство организации обязано гарантировать осведомленность соответствующего персонала относительно значимости и важности его деятельности по обеспечению ИБ и о его участии в достижении целей, поставленных перед СОИБ.

Парадоксальным является тот факт, что сами сотрудники СОИБ могут быть источниками возможных угроз ИБ. Например, системный программист нарушает защиту программного обеспечения (ПО), обеспечивая себе право входа в систему, обходя способы защиты, о которых он осведомлен в соответствии со своими служебными обязанностями. Оператор, призванный обеспечить защиту компьютера, может отключить (взломать) ее. Инженер по эксплуатации может воспользоваться доступными ему ключами и служебными программами для входа в систему и доступа к защищенным файлам. [Подробности о сетевых атаках, киберугрозах и защите от них изложены в статье Гусевой Е.П. «Менеджмент: аспекты информационной безопасности, прозрачности и доверия к информации», опубликованной в журнале «Экономика, Статистика и Информатика. Вестник УМО №5, 2012 г. – С.175–177»]

4. Заключение

Прежде всего, следует выделить следующие основные проблемы, решение которых может значительно повысить информационную безопасность:

– Недостаточная грамотность пользователей в вопросах ИБ

– Негарантированность криптостойкости аутентификации при доступе к информации

– Погрешности в обработке и хранении данных.

При решении проблем в сфере ИБ необходимо обеспечить должный уровень уверенности в том, что организация способна эффективно противостоять угрозам в информационной сфере. Это относится не только к ведомствам и к общественности, но и к владельцам и сотрудникам организаций, деловому и фоновому окружению.

В современных условиях наиболее актуальным становится решение проблемы процесса эффективного взаимодействия ИТС и SMART-менеджмента в обеспечении ИБ.

Следует отметить, что обеспечение ИБ очень разнопланово как на макро-, так и на микроуровне.

Мировой опыт показывает, что увеличение инвестиций в ИКТ и повсеместное внедрение ИКТ не гарантируют решение большинства проблем ИБ в SMART-менеджменте. В настоящее время в условиях информационного бума огромные средства вкладываются в развитие ИКТ. Это вызвано как стремлением компенсировать недостаток квалификации персонала, так и отсутствием эффективной рыночной стратегии информатизации.

Проблемы и парадоксы поддержания защищенной среды информационного обмена были, есть и будут. В настоящее время возрастает ущерб, наносимый владельцу информации посредством несанкционированного проникновения в информационную структуру и воздействия на ее компоненты. Информация становится важнейшим экономическим ресурсом со своими стоимостными показателями (прибылью или убытком), зависящими от деятельности СОИБ.

Непременное, неукоснительное соблюдение мер по защите процессов создания информации, её ввода, обработки и вывода – позволит пользователя заранее быть готовыми к новым угрозам, проблемам и парадоксам ИБ в современном менеджменте.

Проблемы и парадоксы ИБ в современном, особенно в российском менеджменте, касаются каждого.

Литература

1. Гусева Е.П. Менеджмент: аспекты информационной безопасности, прозрачности и доверия к информации // Экономика, Статистика и Информатика. Вестник УМО №5, 2012 г. – С.173–182.

2. Гусева Е. П. Парадоксы информационной безопасности в современном российском менеджменте. С.72–76. Сборник посвящен 80-летию МЭСИ. Модель менеджмента для экономики, основанной на знаниях. Материалы трудов участников IV Международной научно-практической конференции. – М.: МЭСИ, 2012 – 370 с.

3. Гусева Е. П. Генезис теории, практики отечественного менеджмента и информационной безопасности. С. 19–41 Модель менеджмента для экономики, основанной на знаниях. Международная научно-практическая конференция: сборник статей. – Москва: МЭСИ, 2013. –194 с.

4. Гусева Е.П. Менеджмент: Учебно-методический комплекс. – М.: изд. центр ЕАОИ. 2008.– 416 с.: ил.

5. Гусева Е.П. (Соавтор). Производственный менеджмент: Учебник / Под ред. С.Д. Ильенковой.– М.: ЮНИТИ – ДАНА. 2002. – 583с.: ил.

6. Гусева Е.П. Стратегическая роль E-learning world в модели менеджмента для экономики, основанной на знаниях. В кн. «Модель менеджмента для экономики, основанной на знаниях». Материалы трудов участников второй международной научно-практической конференции. Под ред.: д.э.н., проф. Орехова С.А. – М.: МЭСИ, 2010. – 496 с.

7. Гусева Е.П. Исследование приоритета творчества В.М. Глушкова в создании теоретических основ, практики менеджмента и среды e-learning. (281–296 с) В кн. «Модель менеджмента для экономики, основанной на знаниях. Материалы трудов участников III Международной научно-практической конференции. – М.: МЭСИ, 2011. – 314 с.

8. Мельников Д.А. Информационные процессы в компьютерных сетях. Протоколы, стандарты, интерфейсы, модели. – М.: КУДИЦ – ОБРАЗ, 2001. – 256с.: ил.

9. Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем: учебник. – М.: Университетская книга, 2012. – 598с.: табл., ил.

10. Садердинов А.А, Трайнёв В.А., Федулов А.А. Информационная безопасность предприятия: 3-е изд. – М.: Издательско-торговая корпорация «Дашков и Ко», 2006. – 336 с.: ил.

11. Тихомирова Н.В., Тихомиров В.П. Россия на пути к SMART-обществу / Коллективная Монография под редакцией проф. Н.В. Тихомировой, проф. В.П. Тихомирова. М.: МЭСИ. – 280 с.

12. Теория менеджмента: Учебник для вузов. / Под ред. А.М.Лялина. Стандарт 3-го поколения. – СПб.: Питер, 2009. – 464 с.: ил. – (Серия «Учебник для вузов»).

13. ITU-T, «Security Architecture for Open Systems Interconnection for CCITT Applications», Recommendation X.800, 1991.

14. ISO, "Information Processing Systems – Open Systems Interconnection Reference Model – Part 1: Basic Reference Model", ISO/IEC 7498-1.

15. ISO, «Information Processing Systems – Open Systems Interconnection Reference Model – Part 2: Security Architecture», ISO/IEC 7499-2.

16. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework X.816, 1995.

17. J. McNamara. Secrets of Computer Espionage: Tactics and Countermeasures, John Wiley & Sons, Inc., New York, 2003.

18. http://ru.wikipedia.org/wiki/SMART // определение термина SMART. Дата обращения 16.11.2013г.

19. http://www.gks.ru // Официальный сайт Федеральной службы государственной статистики. Дата обращения 16.11.2013г.

References

1. Guseva E.P. Management: aspects of information security, transparency and trust to information// Ekonomika, Statistika i Informatika. Vestneyk UMO №5, 2012 g. – S.173–182.

2. Guseva E. P. Paradoxes of information security in modern Russian management. The collection is devoted to the 80 anniversary of MESI. Management model for the economy based on knowledge. Materials of works of participants of the IV International scientific and practical conference. – M: MESI, 2012 – 370 p.

3. Guseva E. P. The Genesis of the theory, the practice of the domestic management and information security. P.19–41. Management model for the knowledge economy. Mezhdunarodnaya nauchno-prakticheskaya konferenciya: sbornik statej. – Moskva: MESI, 2013. – 194s.

4. Guseva E.P. Management: CMD. Moscow: Izd. EAOI Center, 2008. – 416 p.

5. Guseva E.P. (co-author). Production management: Textbook./ Edited by S.D. Il'enkova. – M: UNITY – DANA. 2002. – 583c.: Il.

6. Guseva E.P. Strategic role of e-learning world in management model for the economy based on knowledge. In book. "Management model for the economy based on knowledge". Materialy trudov uchastneykov vtoroj mezhdunarodnoj nauchno-prakticheskoj konferencii. Pod red.: d.e.n., prof. Orehova S.A. – M.: MESI, 2010. – 496 s.

7. Guseva E.P. Research of a priority of creativity of V. M. Glushkov in creation of theoretical bases, practice of management and the e-learning environment. (281–296 p.) In book. "Management model for the economy based on knowledge. Materialy trudov uchastneykov III Mezhdunarodnoj nauchno-prakticheskoj konferencii. – M.: MESI, 2011. – 314 s.

8. Melnikov D.A. Information processes in computer networks/ Protocols, standards, interfaces, model. – M.: KUDIC – OBRAZ, 2001. – 256 s.: il.

9. Melnikov D.A. Organization and safety of information and technological networks and systems: Textbook. – Universitetskaya kniga, 2012. – 598 s.: tabl., il.

10. Saretdinov A.A., Trajnev V.A., Fedulov A.A. Company's information security-3rd ed. – M.: Izdatelsko-torgovaya korporaciya «Dashkov i Ko», 2006. – 336 s.: il.

11. Tikhomirov N. V., Tikhomirov V.P. Russia on a way to SMART-society / Kollektivnaya Monografiya pod redakciej prof. N.V. Tihomirovoj, prof. V.P. Tihomirova. M.: MESI. – 280 s.

12. Theory of management: Textbook for universities. Ed. A.M. Ljalina. Standard 3-rd generation. – SPb.: Peter, 2009. – 464 s.: il. – (Seriya «Uchebnik dlya vuzov»).

13. ITU-T, «Security Architecture for Open Systems Interconnection for CCITT Applications», Recommendation X.800, 1991.

14. ISO, "Information Processing Systems – Open Systems Interconnection Reference Model – Part 1: Basic Reference Model", ISO/IEC 7498-1.

15. ISO, «Information Processing Systems – Open Systems Interconnection Reference Model – Part 2: Security Architecture», ISO/IEC 7499-2.

16. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework X.816, 1995.

17. J. McNamara. Secrets of Computer Espionage: Tactics and Countermeasures, John Wiley & Sons, Inc., New York, 2003.

18. http://ru.wikipedia.org/wiki/SMART // the definition of the term SMART. Reference date 16.11.2013.

19. http://www.gks.ru // Official site of the Federal service of state statistics. Reference date 16.11.2013.