УДК 004.413.2

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ

Лысенко Е.И., Барабошин А.С., Черненко С.С., Нескоромный В.Н.

ФГБОУ ВПО «Московский государственный технический университет радиотехники, электроники и автоматики», Вавилова 4а, Дубна, Россия 141980, mirea.dubna@mail.ru

В обзоре рассмотрен вопрос общих принципов обеспечения безопасности корпоративной сети как единой системы, которая рассматривается как состояние защищенности интересов (целей) организации (владельца сети) в условиях наличия угроз в информационной сфере. Показано, что для разработки системы защиты компьютерной корпоративной сети необходимым является осуществление анализа сети как системы узлов (элементов), соединённых связями (информационными потоками). При этом предлагается концепция моделирования графа сети, предполагающая типологизацию элементов по двум взаимодополняющим друг друга классификационным подходам, а именно: аппаратно-программного деления на элементы, соответствующие физическим устройствам и работе программного обеспечения; функционального выделения сегментов сети, соответствующих выполнению определённых целей. Обосновано применение междисциплинарного подхода к вопросам безопасности корпоративных компьютерных сетей, которому соответствует анализ рисков и угроз, связанных как с аппаратной частью сети и программным обеспечением, так и с человеческим фактором. В главном система безопасности должна быть организована как совокупность мер по своевременному обнаружению и реагированию на возможные угрозы компьютерной сети в виде цельной системы. В качестве практического примера в обзоре использован дипломный проект Барабошина А.С., в котором разработана схема оптимизации структуры сети филиала МГТУ МИРЭА в г. Дубне.

Ключевые слова: компьютерные сети, защита информации, политика безопасности.

PRINCIPLES OF CORPORATE NETWORK SECURITY

Lysenko E.I., Baraboshin A.S., Chernenko S.S., Neskoromnyj V.N.

Dubna branch of Moscow State Technical University of Radioengineering, Electronics and Automation, Vavilova 4a, Dubna, Russia 141980, mirea.dubna@mail.ru

The paper discusses the general principles of corporate network security as a single system, which is regarded as a condition of security interests (goals) of the organization (the owner of the network) in the presence of threats in the information sphere. Shown that the development of the system of protection of computer corporate network is to implement the necessary network analysis as a system of nodes (elements) connected by links (information flow). It is proposed the concept of modeling the network graph, which involves two elements typology classification approaches complement each other, namely hardware and software division into elements corresponding to physical devices and software work as well as the functional separation of network segments corresponding to the implementation of certain objectives of the organization goals. The application of a multidisciplinary approach to the security of corporate computer networks, which corresponds to the analysis of the risks and threats associated with both network hardware and software, as well as taking into account the human factor. In general, the security system should be organized as a set of measures for the early detection and response to potential threats to computer networks as a whole system. As a practical example, the article used Baraboshin AS thesis project, which developed a scheme for optimizing the structure of the branch network MIREA in Dubna.

Keywords: computer networks, information security, security policy.

Информационная среда современного мира является фактором, оказывающим влияние на все сферы деятельности человека. В настоящее время практически невозможно оказывать воздействия на объекты без информационной составляющей, будь эти объекты материальными или идеальными (данные, парадигмы, теории и т.д.). Распространённость обработки, хранения и обмена информацией закономерно приводит к важности вопроса обеспечения безопасности как самой информации (данных), так и осуществляемых

соответствующей деятельностью процессов. Вопрос защиты компьютерных сетей усложняется тем, что факторы уязвимости таковых относятся к различным областям: аппаратному и программному обеспечению, человеческому фактору, организации сети и др. Стоит отметить и фактор непонимания важности проблемы со стороны руководства многих организаций, недооценивающих важность безопасного функционирования компьютерных сетей и приводящий не только к прямым потерям из-за утечки информации или дисфункциям работы сетей, но и к дополнительным расходам ресурсов на перестройку сетей, в которых изначально не были заложены концепции безопасности и развития.

Информационную безопасность можно определить как «состояние защищенности интересов (целей) организации в условиях угроз в информационной сфере» [3].

Под информационной сферой здесь понимается вся система информационной инфраструктуры сети, а также субъектов, осуществляющих работу с информацией, начиная со сбора таковой и завершая использованием, с промежуточными задачами хранения и анализа, а также регулирование соответствующих отношений в организации.

Анализ компьютерных сетей с точки зрения безопасности необходимо проводить по двум классификациям, взаимно дополняющих друг друга.

Во-первых, это анализ аспектов уязвимости сети, а именно [48]:

- аппаратурный уровень безопасности;
- надёжность хранения информации;
- отказоустойчивость;
- защищённость протоколов обмена информацией;
- контроль внутреннего и внешнего доступа;

и другие.

Во-вторых, это анализ функциональных аспектов сети и разделение таковой на сегменты в соответствии с выполняемыми задачами. В качестве примера используем дипломный проект Барабошина А.С., в котором он предложил схему оптимизации структуры сети филиала МГТУ МИРЭА в г. Дубне. Архитектура сети должна подчиняться логике функционирования компьютерной сети как системы, т.е. сеть должна быть построена таким образом, чтобы оптимизировать достижение функциональных задач, определяемых для конкретной сети целями организации.

Таким образом, следует формализовать и разделить информационные потоки, соответствующие системно разным задачам компьютерной сети и имеющие различную функциональность и требования к безопасности. В сети филиала МГТУ МИРЭА в г. Дубне

были выявлены следующие функциональные информационные сегменты, типичные для высшего учебного заведения [18]:

1. Бухгалтерия, финансовые операции. Особенностью сегмента являются повышенные требования к безопасности, вследствие чего возникает необходимость выделения бухгалтерской подсети в отдельный изолированный кластер, к которому не должно быть доступа из основной сети. Специфика работы также подразумевает особые требования к внешним подключениям с использованием особо защищённых сетевых протоколов, специального программного обеспечения, систем резервного копирования информации и т.д.
2. Административное управление. Этот сегмент сети является крайне важным для учебного заведения, так как имеет отношение к организации всего учебного процесса в целом. Спецификой является наличие информации, важной как для преподавателей, так и для учащихся, а также обработка информации, содержащей персональные данные, в связи с чем согласно законодательству РФ требуется использование сертифицированных средств защиты информации. В этом сегменте особенно актуальным вопросом безопасности является строгое разграничение доступа, предотвращающее несанкционированное изменение персональных данных учебного процесса, а также обеспечение сохранения всей информации.
3. Приёмная комиссия. Этот сегмент сети также должен быть отделён от основной сети, что повысит устойчивость к взлому всей компьютерной сети как единой системы, но основным вопросом функционирования является оптимизация работы с внешними пользователями, обладающими различным уровнем навыков работы с компьютерами. Требования удобства пользования, особенно для неквалифицированного пользователя, и требования безопасности сети часто антагонистичны, и необходимо соблюдать баланс требований, оптимальный с точки зрения приёмной комиссии. Дополнительным требованием является наличие вариантов пользовательского интерфейса для различных типов устройств, включая мобильные.
4. Учебный процесс. В этот сегмент сети входит обеспечение проведения лабораторных работ, семинаров, научных конференций и т.д. Особых требований этот сегмент с точки зрения обеспечения безопасности сети не имеет.
5. Специфическое оборудование: IP-телефония, системы видеонаблюдения и проч. Выделяются как отдельные подсети с соответствующими функциональным задачам требованиями к аппаратному и программному обеспечению.

Таким образом, компьютерная сеть должна быть типологизирована как с аппаратно-программной, так и с функциональной точки зрения. Принято считать, что для обеспечения

безопасности сети таковая должна быть смоделирована в виде узлов, соединённых потоками информации (материальными линями связи либо виртуальной передачей данных согласно функциональным алгоритмам), при этом узлы могут состоять из нескольких объектов аппаратного или программного характера [7]. Следует учитывать, что нарушение безопасности на любом узле означает нарушение целостности безопасности всей компьютерной сети. Особую важность этот вопрос приобретёт в ближайшем будущем по мере развития робототехники [49].

Оценка безопасности компьютерной в целом, необходимая для минимизации рисков, требует оценку локальных рисков, соотносимых с каждым узлом компьютерной сети как системы, из которых выводится обобщённая оценка риска сбоя системы [43].

Исходя из вышесказанного, начальная стадия разработки системы безопасности для каждой компьютерной сети заключается в детальной разбивке сети в целом на отдельные элементы и связи между ними, исходя как из аппаратно-программного, так и из функционального факторов. Конечным результатом должно стать построение графа ресурсов сети, а также определение важности таковых относительно информационных процессов с точки зрения безопасности системы.

В качестве примера можно провести анализ уязвимости сети филиала МГТУ МИРЭА в г. Дубне, проведённый Барабошиным А.С. Наиболее типичными для корпоративных сетей являются следующие выявленные уязвимости:

- отсутствие единой схемы антивирусной защиты, наличие разнообразных средств, не связанных между собой, в различных сегментах сети;
- использование разными лицами одной и той же учётной записи для входа в сеть;
- отсутствие однозначных политик разграничения прав доступа, соответствующих служебным обязанностям;
- использование заводских паролей для сетевых устройств.

Системный подход к обеспечению безопасности компьютерной сети позволяет сделать вывод о необходимости контроля не только внешнего периметра сети: компьютерная сеть как система должна иметь сопротивляемость любым действиям, как целенаправленным, так и случайным, которые может совершить пользователь [13]. При этом необходимо учитывать как возможные действия злоумышленников, так и возможные угрозы безопасности сети вследствие невнимательности или даже умышленного нарушения установленного регламента безопасности. В частности, особо следует отметить отношение пользователей к хранению паролей: с теоретической точки зрения увеличение количества паролей доступа к различным ресурсам и действиям повышает защищённость системы, на практике же

усложнение процедуры доступа приводит к тому, что пользователи хранят пароли на рабочих местах (зачастую открыто), используют одну учётную запись коллективно и т.д.

Обеспечение безопасности по отношению к информации в компьютерной сети может быть классифицировано по следующим категориям:

- конфиденциальность;
- доступность;
- целостность.

Любое практическое обеспечение безопасности компьютерной сети имеет свои особенности реализации, зависящие от конкретики функционирования сети (так, в уже используемом примере филиала МГТУ МИРЭА в г. Дубне сеть имеет функциональный сектор «приёмная комиссия», имеющий смысл лишь для учебных заведений и т.п.). В общем виде можно выделить три «слоя» функционирования защиты, каждый из которых должен быть проанализирован и осуществлён на практике [5]:

1. Полное перекрытие механизмом защиты возникшей угрозы;
2. Прочность механизмов защиты по отношению к возможностям обхода или преодоления каким-либо способом;
3. Минимизация ущерба, причиненного в случае успешного преодоления механизма защиты.

Исходя из предыдущего, важно понимать, что при обеспечении безопасности компьютерных сетей важна не только непосредственная защита активов, являющаяся лишь одним из элементов системы безопасности. С современной научной точки зрения парадигма «защищённой крепости», ранее бывшая базовой для модели обеспечения безопасности компьютерных сетей, рассматривается лишь как один из уровней защиты [17]. Так, минимизация ущерба в случае преодоления защиты достигается за счёт обеспечения качественной системы резервного копирования информации, что также учитывается с точки зрения безопасности сети.

Как следствие, системное моделирование сети как функционально-аппаратных узлов и связей между ними должно осуществляться не произвольным образом, а с помощью междисциплинарного подхода, учитывающего не только аппаратные и программные особенности, но и человеческий фактор [6]. При этом целесообразно использовать моделирование графа системы сети как последовательно-параллельных соединений отдельных узлов, для каждого из которых представляется возможным определить количественные характеристики надежности [4], что позволит количественно оценивать [39] оптимизацию компьютерной сети с точки зрения безопасности.

Методы защиты компьютерных сетей могут быть типологизированы следующим образом:

1) регламентирование работы персонала с компьютерной сетью – определение политик доступа и т.д.;
2) разграничение физического доступа в помещения с соответствующей аппаратурой;
3) физические методы безопасности, устанавливаемые на компьютерах – аппаратные ключи, устройства распознавания по биологическим параметрам и пр.;
4) программные методы, включающие как идентификацию пользователей, так и мониторинг их работы;
5) криптографическое шифрование важной информации;
6) резервное копирование данных, в том числе «горячее».

Если относительно недавно основным методом защиты информации было резервное копирование, позволяющее осуществить восстановление данных, относящихся к предыдущему осуществлению процесса бэкапа, то современный объём информации в корпоративных компьютерных сетях требует постоянного функционирования всех процессов обеспечения безопасности [47]. При этом значительное количество решений должно применяться автоматически в случае наличия конкретного решения проблемы, а в случае наличия вариантов либо отсутствия стандартной процедуры должен информироваться оператор, который и должен осуществить выбор решения.

Отдельным аспектом разработки безопасности сетей является соответствие применяемых методов соответствующим нормативным документам, включая стандарты качества. При этом важно учитывать, что в сети могут применяться продукты, спроектированные согласно разным стандартам, включая международные [50]. Также необходимо учитывать введение новых стандартов образования, поскольку выпускники высших учебных заведений должны обладать набором компетенций, соответствующих таковым [26], что может расходиться с требованиями для пользователей конкретной корпоративной сети [31]. В рамках социального партнёрства [41] следует изыскивать возможности совместной обучающей практики студентов высших учебных заведений [19] и предприятий и институтов региона [42], являющихся потенциальными работодателями, что, в свою очередь, повысит уверенность студентов [20] в возможностях трудоустройства [11] и даст мотивацию к дальнейшей учёбе [10], одновременно повысив безопасность корпоративных сетей соответствующих предприятий, так как принятые на работу молодые специалисты уже будут обладать навыками работы с конкретной сетью [25]. Для уже работающих на предприятии пользователей целесообразно создавать возможность

получения дополнительного тематического образования [9], включая не только научные кадры, но и инженерный состав предприятия [14]. Соответственно, целесообразно заранее осуществлять мониторинг [15] эффективности вузов регионов [32], выводя их на современный уровень [12] организационной культуры [34] вуза [24], интегрированный с социокультурным пространством [27] города [23] и региона [21], для чего целесообразно изучать соответствующий зарубежный опыт [22].

Уровень сложности компьютерных сетей продолжает увеличиваться. В настоящее время основными тенденциями развития являются:

1) интеграция технологий, а именно – взаимодействие различных сетевых протоколов, а также совместное использование ресурсов и средств передачи данных со стороны провайдеров и т.д.;
2) внедрение новых сетевых протоколов и технологий, которые должны обеспечивать более качественную и помехозащищённую связь (могут включать системы шифрования и т.д.);
3) глобализация информационных ресурсов, вызванная необходимостью использования данных с разных мест доступа одним и тем же пользователем (в т.ч. коллективным использованием).

Таким образом, одним из факторов обеспечения качества безопасности корпоративной сети является постоянное повышение квалификации сотрудников отдела IT-безопасности, их ключевых компетенций [44], уровень владения которыми должен постоянно соответствовать мировому уровню развития отрасли [36], повышая кадровый потенциал [8] организации [30]. В целом управленческая структура организации должна быть направлена на своевременное освоение современных технологий [2], в том числе и в области защиты информации, что подразумевает соответствующую подготовку сотрудников [29], позволяющую постоянно повышать [1] качество работы [38], а, следовательно, и экономическую эффективность организации [45]. Вопрос управления развитием персонала [37] всё больше интересует научное общество [28], однако при этом следует учитывать современную тенденцию подстройки систем управления под пользователя, зачастую не обладающего соответствующими компетенциями [46], между тем как управление безопасностью должно учитывать таких пользователей [33], что понижает стрессогенность пользования компьютерными сетями для этой категории [16], но в области управления необходима направленность на более конкурентоспособный персонал [35], в частности – на специалистов по компьютерной безопасности.

Обобщая вышесказанное, можно определить систему безопасности как совокупность мер по своевременному обнаружению и реагированию на возможные угрозы сети как системы. При разработке систем безопасности требуется предварительное построение модели структуры сети в виде узлов, выделяемых как аппаратно-программно, так и с функционально-пользовательской точки зрения, соединяемых потоками информации виртуального характера или линиями связи (включая беспроводную). Определение угроз безопасности узлам корпоративной сети является мультидисциплинарной задачей, для решения которой необходимо учитывать аппаратную и программную составляющую сети, а также человеческий фактор, включая как преднамеренные вредоносные действия, так и непреднамеренные, исходящие из незнания и других факторов.

Работа выполнена в рамках подхода научно-методической школы под руководством М.А. Назаренко в филиале МГТУ МИРЭА В г. Дубне [40].

Список литературы

1. Абакумова Н.В., Бобров В.Н., Иткис М.Г. и др. Эффективность филиальной сети технического университета // Международный журнал экспериментального образования. — 2013. — № 11-1. — С. 203-204.
2. Акимова Т.И., Мельников Д.Г., Назаренко М.А. Применение принципа постоянного улучшения систем менеджмента качества в учебном процессе // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 3-1. — С. 126-128.
3. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса — М.: Альпина Паблишерз, 2011. — С. 338 (eBook).
4. Баранова А.В., Ямпурин Н.П. Основы надежности электронных средств. — М.: Академия, 2010. — С. 234.
5. Биячуев Т.А. Безопасность корпоративных сетей: Учебное пособие. — СПб.: СПб ГУ ИТМО, 2004. — С. 161.
6. Булгаков О.М., Удалов В.П., Кучмасов Е.А. Принципы построения модели надежности системы защиты информации // Вестник ВИ МВД России. — 2012. — № 3. — С. 167–176.
7. Волков, О. А. Разработка и анализ модели политики безопасности компьютерной сети // Известия высших учебных заведений. Поволжский регион. Технические науки. — 2011. — № 2 (18). — С. 38–45.

8. Горшкова Е.С., Назаренко М.А., Алябьева Т.А. и др. Роль кадрового аудита в организации // Международный журнал прикладных и фундаментальных исследований. — 2013. — № 10-2. — С. 330-331.
9. Дзюба С.Ф., Назаренко М.А. Применение учебных планов филиала МГТУ МИРЭА в г. Дубне в системе дополнительного образования // Современные проблемы науки и образования. — 2013. — № 5. — С. 242.
10. Дзюба С.Ф., Нескоромный В.Н., Назаренко М.А. Сравнительный анализ мотивационного потенциала студентов вузов // Бизнес в законе. — 2013. — № 1. — С. 233-237.
11. Духнина Л.С., Лысенко Е.И., Назаренко М.А. Основные принципы социального партнерства в сфере труда и доверие к ним со стороны работающей молодежи // Международный журнал экспериментального образования. — 2013. — № 4-2. — С. 174-175.
12. Задувалова Е.В., Назаренко М.А. Инертность и глобализация в современном научном сообществе // Успехи современного естествознания. — 2014. — № 7. — С. 168-169.
13. Интриери Р. Безопасность корпоративной сети // Журнал сетевых решений/LAN. — 2012. — № 10. URL: http://www.osp.ru/lan/2012/10/13018069/ (дата обращения: 14.07.2014).
14. Иткис М.Г., Назаренко М.А. Повышение квалификации инженерных кадров ОИЯИ на базе филиала МГТУ МИРЭА в г. Дубне // Современные проблемы науки и образования. — 2013. — № 5. — С. 254.
15. Иткис М.Г., Назаренко М.А. Результаты мониторинга деятельности вузов и эффективность базовых филиалов // Международный журнал прикладных и фундаментальных исследований. — 2013. — № 1. — С. 146–147.
16. Калугина А.Е., Назаренко М.А. Стрессогенность и социально-ориентированное проектирование современной техники // Успехи современного естествознания. — 2014. — № 7. — С. 169-170.
17. Королева Н.А. Экспертная система поддержки принятия решений по обеспечению информационной безопасности организации : дис. … канд. техн. наук. — Тамбов, 2006. — С. 198.
18. Лысенко Е.И., Черненко С.С. Организация сети образовательного учреждения // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 3-1. — С. 128-129.
19. Назаренко М.А. Взаимодействие школ, вузов и предприятий в подготовке инженерных кадров для экономики Дубны и Подмосковья // Фундаментальные исследования. — 2014. — № 5-1. — С. 192-198.

20. Назаренко М.А. Мотивационные факторы при получении образования в регионе // Международный журнал экспериментального образования. — 2013. — № 11-1. — С. 159-160.
21. Назаренко М.А. Основные направления процесса регионализации системы высшего образования как составляющей части социального партнерства в обществе // Сборник научных трудов Sworld. — 2013. — Т. 19. — № 3. — С. 88-93.
22. Назаренко М.А. Особенности европейской интеграции в сфере профессионального образования // Мир науки, культуры, образования. — 2013. — № 5. — С. 50-53.
23. Назаренко М.А. Особенности интеграции вуза в социокультурное пространство малого города // Наука и школа. — 2013. — № 4. — С. 8-10.
24. Назаренко М.А. Особенности интеграции вуза в социокультурное пространство малого города (на примере г. Дубна Московской области) // Мир науки, культуры, образования. — 2013. — № 5. — С. 45-47.
25. Назаренко М.А. Повышение квалификации специалистов по промышленной электронике в области современных информационных технологий // Современные проблемы науки и образования — 2014. — № 2. URL: http://www.science-education.ru/116-12419 (дата обращения: 15.07.14).
26. Назаренко М.А. Программа развития образования в московской области и особенности вступившего в действие законодательства // Современные проблемы науки и образования. — 2014. — № 1. — С. 64.
27. Назаренко М.А. Социальное партнерство — неотъемлемое условие эффективной управленческой деятельности вуза в малом городе (на примере г. Дубна Московской области) // Мир науки, культуры, образования. — 2013. — № 5. — С. 55-58.
28. Назаренко М.А. Технологии управления развитием персонала в диссертационных исследованиях // Успехи современного естествознания — 2013. — № 6. — С. 160.
29. Назаренко М.А., Адаменко А.О., Киреева Н.В. Принципы менеджмента качества и системы доработки или внесения изменений во внедренное программное обеспечение // Успехи современного естествознания. — 2013. — № 7. — С. 177.
30. Назаренко М.А., Алябьева Т.А., Напеденина А.Ю. и др. Использование кадрового аудита для развития компании в современных условиях // Международный журнал прикладных и фундаментальных исследований. — 2013. — № 6. — С. 151.
31. Назаренко М.А., Белолаптикова А.И., Лысенко Е.И. Вычислительные комплексы и системы — терминальные системы в рамках ФГОС ВПО // Успехи современного естествознания. — 2013. — № 6. — С. 158-159.

32. Назаренко М.А., Горькова И.А., Алябьева Т.А. и др. Оценка кадрового потенциала организации // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 4. — С. 178-179.
33. Назаренко М.А., Дзюба С.Ф., Котенцов А.Ю. и др. Организационная культура в системе управления персоналом // Международный журнал прикладных и фундаментальных исследований. — 2013. — № 7. — С. 191–192.
34. Назаренко М.А., Котенцов А.Ю. Анализ организационных структур современных предприятий // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 5-2. — С. 143-146.
35. Назаренко М.А., Котенцов А.Ю., Аверьянов Е.А., Сергеев Г.С. Разработка и внедрение политики отбора конкурентно-способного персонала // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 7. — С. 139-140.
36. Назаренко М.А., Котенцов А.Ю., Аверьянов Е.А., Сергеев Г.С. Разработка учебно-методических материалов для обучения персонала в соответствии со стратегией развития организации // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 7. — С. 140.
37. Назаренко М.А., Котенцов А.Ю., Аверьянов Е.А., Сергеев Г.С. Кадровый аудит в системе управления персоналом // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 7. — С. 138-139.
38. Назаренко М.А., Петров В.А., Сидорин В.В. Управление организационной культурой и этический кодекс вуза // Успехи современного естествознания. — 2013. — № 4. — С. 171–172.
39. Назаренко М.А., Топилин Д.Н., Калугина А.Е. Квалиметрические методы оценки качества объектов в современных научных исследованиях // Успехи современного естествознания. — 2013. — № 7. — С. 175-176.
40. Никонов Э.Г., Дзюба С.Ф., Напеденина А.Ю., Напеденина Е.Ю., Омельяненко М.Н. Научно-методическая школа в филиале МГТУ МИРЭА В г. Дубне под руководством М.А. Назаренко // Международный журнал прикладных и фундаментальных исследований. — 2013. — № 7. — С. 189-190.
41. Охорзин И.В., Акимова Т.И., Назаренко М.А. Применение принципов менеджмента качества для обеспечения социальной мотивации и улучшения качества трудовой жизни // Международный журнал экспериментального образования. — 2013. — № 4-2. — С. 176.

42. Самохвалова А.Р., Дзюба С.Ф., Ковалева Е.В., Назаренко М.А. Проектирование кадровой политики и критерии ее эффективности // Успехи современного естествознания. — 2014. — № 1. — С. 85-86.

43. Симонов, С.В. Анализ рисков в информационных системах. Практические аспекты // Защита информации. Конфидент. 2001. — № 2. — С.48–53.

44. Тукачёва А.Б., Дзюба С.Ф., Назаренко М.А., Алябьева Т.А. Развитие ключевой компетенции как основа повышения эффективности управления персоналом организации // Проблемы региональной экономики. — 2013. — № 21. — С. 42-47.

45. Тукачёва А.Б., Дзюба С.Ф., Назаренко М.А. и др. Связь степени развития организационной культуры и экономической эффективности организации // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 3-1. — С. 102-103.

46. Уаттс Р. ЭВМ и непрофессиональные пользователи: Организация взаимодействия. — М.: Радио и связь, 1989. — С. 94.

47. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. — К.: Юниор, 2003. — С. 504.

48. Черненко С.С., Назаренко М.А. Разработка научных методов защиты компьютерных сетей // Современные проблемы науки и образования. — 2014. — №3. URL: http://www.science-education.ru/pdf/2014/3/173.pdf (дата доступа: 15.07.2014).

49. Черненко С.С., Назаренко М.А. Робототехника и ее перспективы в социо-культурном аспекте // Успехи современного естествознания. — 2014. — № 5-2. — С. 194-195.

50. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. — С. 352.

Рецензенты:

Никонов Э.Г., д.ф.-м.н., старший научный сотрудник, заведующий кафедрой информационных технологий МГТУ МИРЭА (Министерство образования и науки Российской Федерации), г. Дубна.

Омельяненко М.Н., д.т.н., профессор, заведующий кафедрой промышленной электроники МГТУ МИРЭА (Министерство образования и науки Российской Федерации), г. Дубна.