УДК 004.413.2

ПРИМЕНЕНИЕ МОНИТОРИНГА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Черненко С.С., Барабошин А.С., Лысенко Е.И., Духнина Л.С.

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

В обзоре рассмотрен вопрос автоматизации рутинных действий при обеспечении безопасности компьютерных сетей с точки зрения мониторинга процессов с целью оптимизации анализа системных событий, что должно приводить к более оперативному принятию решений по поводу потенциальных или фактических угроз безопасности сети. Мониторинг сети, определяемый как постоянное наблюдение за объектами и факторами, влияющими на функционирование сети, а также анализ результатов наблюдения, включая хранение и обобщение соответствующей информации, должен обеспечивать обнаружение недопустимых событий в работе сети, которые могут быть следствиями как технических сбоев, так и несанкционированных воздействий на сеть. Предлагаются способы, облегчающие принятие решений оператором: консолидированные оценки функционирования системы, применение нейронных сетей для анализа информационных процессов.

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

APPLICATION FOR MONITORING SAFETY INFORMATION SYSTEMS

Chernenko S.S., Baraboshin A.C., Lysenko E.I., Duhnina L.S.

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

The article discusses the automation of routine activities, while ensuring the security of computer networks from the perspective of monitoring processes in order to optimize the analysis of system events that should lead to a more rapid decision-making about potential or actual threats to network security. Network monitoring, defined as the constant observation of objects and factors affecting the operation of the network, as well as analysis of the results of observation, including storage and collating relevant information, should ensure detection of harmful events in the network, which may be due to technical glitches as well as unauthorized effects on the network. Suggests ways to facilitate decision-making by the operator: consolidated assessment of the functioning of the system, the use of neural networks for analysis of information processes.

Keywords: computer networks, information security, security policy.

Комплексная защита компьютерной сети современного уровня требует использования различных средств безопасности, таких как системы обнаружения сетевых атак, системы защиты от спама, антивирусы, межсетевые экраны (firewall), сканеры безопасности и т.д. При этом возрастание количества аппаратных и программных средств защиты сети значительно увеличивает объём анализируемой информации, необходимый для контроля безопасности. Как следствие – администраторы сети должны уделять значительное время анализу рутинной информации, что снижает продуктивность работы и, соответственно, влияет на оперативное принятие решений по поддержке функционирования компьютерной сети. Таким образом, возникает противоречие между увеличением объёма информации, которую целесообразно анализировать для предотвращения угроз, и оперативностью управления сетью.

Под угрозой с точки зрения безопасности следует понимать совокупность условий и факторов, потенциально приводящих к нарушению функционирования компьютерной сети в

целом, в том числе – контролируемым сетью активам (данным), а также отдельным пользователям [49]. Угрозы обычно разделяются на: умышленные (осознанное причинение вреда) и естественные. К первым относятся несанкционированные подключения, утечки информации, нарушение функционирования сети и т.д., ко вторым – форс-мажорные обстоятельства и несчастные случаи, а также ошибки вследствие сбоев аппаратуры [41]. При этом значительная часть угроз безопасности является следствием человеческого фактора — отсутствия у пользователей необходимых компетенций, а также игнорирования служебных инструкций (например, небрежное обращение с паролями). Анализ безопасности компьютерной сети требует учитывать все виды угроз, однако если естественные угрозы достаточно легко формализируются в плане рисков и защита от них достаточно линейна, то угрозы, имеющие причиной человеческий фактор, требуют особого внимания вследствие непредсказуемости действий даже при отсутствии намерения причинения вреда. С другой стороны, человеческий фактор имеет значение в тех случаях, когда дисфункция системы каким-либо образом угрожает человеку, что особенно важно с футуристической точки зрения – время, когда робототехника станет привычной в быту, относится к обозримому будущему [46].

В любой компьютерной сети даже за сутки происходят десятки и сотни тысяч событий, имеющих отношение к информационной безопасности, при этом подавляющее большинство – это нормальное функционирование сети, и лишь некоторые из них являются сигналами о потенциальных или же фактических нарушениях безопасности. Таким образом, крайне актуальной задачей является мониторинг состояния сети, который позволяет отслеживать не только текущее состояние сети, но и изменения в ней как в динамической системе. В целом, мониторинг компьютерной сети можно определить как постоянное наблюдение за объектами и факторами, влияющими на функционирование сети, а также как анализ результатов наблюдения, включая хранение и обобщение соответствующей информации [1].

Для обнаружения угроз на практике используется большой ассортимент специализированных систем: анализаторы сетевых протоколов, системы сетевого мониторинга, в качестве активного компонента — системы нагрузочного тестирования. Также широко используются антивирусы, межсетевые экраны, криптографические средства защиты информации, систем обнаружения атак (IDS) и др. Однако все эти средства защиты применяются периодически, исходя из субъективных решений администраторов сети, в качестве инструмента для решения уже возникшей проблемы и лишь изредка – для профилактики. Методы анализа направлены на выявление заранее известных и описанных в литературе угроз, следовательно — далеко не всегда имеют возможность обнаружить новые виды угроз или модификации уже известных, что значительно снижает безопасность сети.

Таким образом, в настоящее время актуальной задачей является разработка новых эффективных методов обнаружения недопустимых событий в работе компьютерной сети, которые могут быть следствиями как технических сбоев, так и несанкционированных воздействий. При этом требуется наличие возможности выявления произвольных типов нарушений работы сети и угроз безопасности, включая новые (по косвенным признакам нарушения работы сети), а также обнаружение вредоносных воздействий, пролонгированных во времени [38]. Важность этого научного направления стала понятна лишь с 90-х годов, когда компьютерные сети достигли достаточно высокого уровня сложности [5].

Для осуществления мониторинга требуется наличие в компьютерной сети единой системы управления всеми узлами и сегментами сети, которая будет служить базой для развёртывания системы мониторинга, что позволит осуществлять динамический контроль состояния всех важных узлов и элементов сети в реальном времени, а также накапливать соответствующую статистику для дальнейшего использования в прогнозировании ситуаций нарушения функциональности сети. Наличие подсистемы мониторинга должно учитываться ещё на этапе проектирования сети, поскольку требует выделенных ресурсов. Так, во время выполнениия дипломного проекта А.С. Барабошин, анализируя сеть филиала МГТУ МИРЭА в г. Дубне, обнаружил отсутствие централизованной системы мониторинга, и предложил обновление части технического парка оборудования, предусматривающее установку сетевых интерфейсов на серверах административной и студенческой сети, а также на управляемом сетевом оборудовании. Для решения подобных задач целесообразно использовать технологию VLAN (Virtual Local Area Network), которая позволяет взаимодействовать устройствам компьютерной сети виртуально напрямую, даже если они физически разнесены и подключены к различным коммутаторам, т.е. использование VLAN позволяет разнести логическую и физическую топологию сети, в том числе, задействуя устройства, подключённые через интернет. Следует отметить, что реализация такого подхода оптимально решается посредством нескольких виртуальных машин на одном физическом компьютере, что требует дополнительных мер безопасности, таких как использование супервизоров для изоляции виртуальных машин друг от друга [40].

В общем виде система мониторинга должна состоять из следующих компонентов:

- подсистема сбора информации, поступающей от всех имеющихся средств защиты;
- сервер событий, предназначенный для централизованной обработки поступающей информации о событиях, имеющих отношение к безопасности сети, в соответствии с правилами, заданными администратором сети;
- сервер хранения данных – как первичной информации (событий), как и результатов анализа;

- пользовательский интерфейс управления системой мониторинга, позволяющий осуществлять контроль и управление в реальном масштабе времени.

Сбор информации, необходимой для контроля состояния сети, может быть представлен как следующие взаимосвязанные направления:

- анализ сетевых пакетов (включая декодирование в случае необходимости);
- мониторинг функционирования активного сетевого оборудования;
- мониторинг рабочего состояния кабельной системы, а также беспроводных соединений;
- мониторинг функционирования серверов и рабочих станций (последние могут подразделяться по степени важности с точки зрения безопасности);
- мониторинг работы операционных систем и программных приложений.

Итак, помимо непосредственных данных от средств мониторинга, необходимо хранить и другие данные, имеющие отношение к безопасности сети: сведения о выполнении политик информационной безопасности, об уязвимости конечных систем, об имевших место сбоях и применявшихся методах восстановления работоспособности системы и т.д. Вся совокупность информации может быть в дальнейшем использована для принятия решений по обеспечению безопасности сети, поэтому хранение этих данных необходимо. Однако объем данных, а также разнородный характер таковых, делают задачу учёта параметров сети весьма сложной – требуется разработка методик, позволяющих классифицировать и анализировать соответствующий массив данных, причём во многих случаях — в режиме реального времени.

Одним из методов решения проблемы является оперативная обработка имеющейся базы данных системы мониторинга и вычисление консолидированной оценки результатов мониторинга по заранее определённым параметрам. Такой подход позволяет свести множество разноплановых данных, отслеживаемых системой мониторинга, к значимым и понятным для пользователей показателям, которые могут в дальнейшем использоваться при принятии оперативных решений специалистами по безопасности. Было показано [11], что применение консолидированной оценки в системе мониторинга компьютерной сети позволяет заблокировать в среднем больше на 25.35 % атак, чем при использовании обычных систем мониторинга.

В настоящее время уже недопустимо рассматривать обеспечение безопасности компьютерной сети как сохранение некоего оптимального заранее определённого состояния. Требуется подход к обеспечению безопасности, определяющий задачу адаптивного динамического управления процессами изменения состояний компьютерной сети как сложной системы, обеспечивающую предотвращение выхода системы не из одного

фиксированного состояния, а из диапазона таковых, в достаточной степени удовлетворяющих современным требованиям [9].

Однако даже наличие консолидированных оценок определённых параметров может быть недостаточным для обеспечения безопасности достаточно большой и сложной компьютерной сети. Принятие управленческих решений в таком случае зависит от множества факторов и должно определяться значительным количеством критериев, а также учитывать большое количество ограничений. В конечном итоге сотрудники, принимающие решения, нередко используют упрощённые методики анализа, опирающиеся на скорость в ущерб качеству, применяют привычные, но уже малоэффективные методы, и т.д. Из этого следует вывод о необходимости наличия системы поддержки принятия решений [12], которая должна взять на себя большую часть рутинной работы.

В общем виде наиболее оптимальным для управления является полуавтоматический режим: если имеется единственное известное решение проблемы, то оно применяется автоматически (дополнительно целесообразно оповещать специалиста по безопасности), а в случае имеющегося выбора вариантов действия, а также при отсутствии известных решений проблемы, решение должен принимать специалист [45].

Функционирование системы поддержки принятия решений требует ведения базы данных, в которой должны фиксироваться следующие параметры:

- описание инцидента, включая классификацию такового согласно разработанной системе;
- имеющиеся тенденции дальнейшего распространения сбоя системы (локализация события);
- список активов по категориям, затронутых инцидентом;
- список затронутых сбоем сети пользователей с учётом их уровней доступа и т.д.;
- влияние сбоя на функционирование и ресурсы сети в целом;
- наличие в базе алгоритмов противодействия угрозе.

Сложность задачи анализа данных системы мониторинга делает целесообразным применение нейронных сетей [33] для анализа данных и событий, что позволяет добиться оперативного результата без процесса аналитического программирования. При этом нейронные сети способны к самообучению, что даёт дополнительные преимущества: сбои системы, как и угрозы, могут проявляться в виде нелинейных зависимостей между параметрами, не всегда непосредственно связанными друг с другом, что крайне сложно обнаружить аналитически. Один из вариантов – это применение сети Хопфилда (полносвязная трёхслойная сеть с симметричной матрицей связей), которая стремится к

достижению равновесия, что может быть задано как оптимизация процессов в компьютерной сети [44].

Ещё одним перспективным направлением совершенствования систем мониторинга компьютерных сетей является оптимизация разграничения потоков данных, низкая эффективность которой даёт в настоящее время до четверти уязвимостей сети [13]. При этом необходимо интегрировать системы контроля безопасности и разграничения потоков данных.

В частности, типичные стандартные решения безопасности редко предусматривают механизм адаптации к различным конфигурациям сетей, вследствие чего исключается возможность оптимального использования свободных ресурсов сети. Более того, зачастую происходит конкуренция за вычислительные ресурсы с приложениями, работающими в сети в тот же момент времени. Для оптимизации работы требуется разделение информационных потоков в реальном времени, а также сокращение времени опроса рабочих станций, осуществляемого системой мониторинга; в целом – динамический многопоточный сбор информации системой мониторинга [42].

В наиболее общем виде система мониторинга должна осуществлять два стратегических видов контроля.

1. Контроль целостности системы, т.е. состояния сети, при котором компьютерная система функционирует как логически единая система аппаратных и программных средств (элементов системы), полноценно обеспечивающих работу защитных механизмов, включая логическую корректность работы и нормальное функционирование в плане нейтрализации угроз безопасности. Также современные системы контроля целостности обязаны отслеживать распределенные конфигурации сети и иметь защиту от несанкционированной модификации потоков данных между узлами сети.
2. Контроль защищенности системы, т.е. попытки санкционированного «взлома» информационной системы, которая осуществляется организацией-владельцем с целью обнаружения имеющихся уязвимостей в защите сети, которые целесообразно выявлять ранее злоумышленников. Особенно актуален этот метод при введении нового программного обеспечения (обновления существенно отличающихся версий), а также в случае изменения кадрового состава сотрудников, работающих с соответствующим узлом сети.

Системы мониторинга компьютерных сетей являются необходимой составляющей общего обеспечения информационной безопасности организации. Эффективность обеспечения информационной безопасности зависит от того, насколько однозначно сформулированы требования к оперативным (текущим), тактическим и стратегическим задачам, и насколько целостно при этом обеспечена их взаимосвязь [48]. Системы

мониторинга как часть системы информационной безопасности предназначены для обеспечения решения оперативных и частично тактических задач, содействуя достижению стратегических целей безопасности.

Необходимо учитывать, что построение сетей может отвечать разным системам стандартов, включая международные [47], а современные стандарты образования далеко не всегда соответствуют по набору компетенций [22] требованиям для специалистов по безопасности [27], особенно если учитывать специфику конкретных информационных систем. Как следствие, целесообразно заранее привлекать студентов высших учебных заведений [15] в соответствующие организации региона [39] в рамках социального партнёрства [6], с дальнейшим трудоустройством [37], что повысит уверенность студентов [17] и даст мотивацию к качественному обучению [4], при этом молодые специалисты уже будут в состоянии выполнять задачи по обеспечению безопасности информационных систем организации [14] без дополнительного периода обучения [21]. Таким образом, для привлечения квалифицированных молодых специалистов имеет смысл осуществлять мониторинг [8] высших учебных заведений регионов [28], отслеживая их соответствие современному уровню образования, наличию организационной культуры [30]. В целом целесообразно интегрировать высшее учебное заведение [20] с социокультурным пространством [23] региона [18] – эффективность такого подхода подтверждается зарубежным опытом [19].

Следует отметить, что описанный ранее динамический системный контроль процессов, имеющих место в компьютерной сети, требует постоянного двустороннего контакта специалистов по компьютерной безопасности со стороны заказчика (организации) с исполнителем работ по разработке и внедрению систем мониторинга для своевременного внесения исправлений и корректировок согласно принципам менеджмента качества [25], что, в свою очередь, подразумевает постоянную адаптацию систем контроля и управления к изменяющимся задачам [2] – все это должно являться обязательной целью организации в плане обеспечения информационной безопасности [16].

Обобщая вышесказанное, следует сделать вывод, что ещё несколько лет назад стандартным методом обеспечения защиты компьютерных сетей являлось применение традиционных услуг безопасности: систем разграничения прав доступа, межсетевых экранов, антивирусного программного обеспечения и т.д. В настоящее время уже можно назвать общепринятым среди специалистов подход, предусматривающий постоянный круглосуточный мониторинг информационных процессов в компьютерной сети, включая внутренний и внешний трафик, а также периодическую проверку на наличие уязвимостей (аудит сети).

Следует понимать, что одним из факторов обеспечения эффективной безопасности сети является постоянное повышение квалификации специалистов по сетевой безопасности, освоение ими новых профессиональных навыков [43] на уровне, соответствующем современным задачам [33]; таким образом, необходимо увеличивать кадровый потенциал [3] организации [26], отслеживая освоение современных технологий сотрудниками – без этого невозможно повышать качество работы [34], необходимое для экономической эффективности организации. Управления развитием персонала [31] является актуальным вопросом современности [24].

При разработке систем мониторинга сети целесообразно учитывать, что пользователи таковой являются специалистами в своей области, и ориентироваться необходимо на них [33], а не на малоквалифицированных пользователей [32], которые зачастую рассматриваются как основная целевая группа [29] из-за гуманистических соображений [10].

Всё большее количество организаций, заботящихся об информационной безопасности, начинают использовать системы мониторинга, что позволяет им повысить эффективность процесса обнаружения угроз и дисфункций сети, а также уменьшить время реагирования на инциденты, имеющие отношение к информационной безопасности, при одновременном увеличении качества принимаемых решений. Такой результат обеспечивается посредством автоматизации сбора и анализа данных о всех процессах сети, автоматически регистрируемых в системе мониторинга сети. Следует отметить, что применение систем мониторинга одновременно в значительной степени повышает эффективность ранее установленных в компьютерной сети средств защиты за счёт синергетического эффекта при обработке данных, имеющих отношение к информационной безопасности.

Настоящая работа выполнена в рамках научно-методической школы под руководством М.А. Назаренко в филиале МГТУ МИРЭА в г. Дубне [36].

Список литературы

1. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления безопасностью. – М.: Стандартинформ, 2006. – С. 62.

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 – С. 126–128.

3. 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.

4. Дзюба С.Ф., Нескоромный В.Н., Назаренко М.А. Сравнительный анализ мотивационного потенциала студентов вузов // Бизнес в законе. – 2013. – № 1. – С. 233-237.

5. Дружинин Е.Л. Разработка методов и программных средств выявления аномальных состояний компьютерной сети : дис. канд. техн. наук. – М., 2005. – С. 202.

6. 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.

7. Задувалова Е.В., Назаренко М.А. Инертность и глобализация в современном научном сообществе // Успехи современного естествознания. – 2014. – № 7. – С. 168-169.

8. 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.

9. Калинин М.О. Адаптивное управление безопасностью информационных систем на основе логического моделирования : дис. д-ра техн. наук. – СПб., 2010. – С. 310.

10. Калугина А.Е., Назаренко М.А. Стрессогенность и социально-ориентированное проектирование современной техники // Успехи современного естествознания. – 2014. – № 7. – С. 169-170.

11. Ковалев Д.О. Выявление нарушений информационной безопасности по данным мониторинга информационно-телекоммуникационных сетей: дис. канд. техн. наук. – М., 2011. – С. 170.

12. Ковалев Д.О. Милославская Н.Г. Особенности построения современных систем управления информационной безопасностью // Доклады Томского государственного университета систем управления и радиоэлектроники. 2008. – Т. 2. – № 1. – С. 112-113.

13. Козачок А.В. Контроль сетевой политики безопасности и разграничение потоков данных в компьютерных сетях научных организаций: дис. канд. техн. наук. – Орёл, 2010.

14. Лысенко Е.И., Черненко С.С. Организация сети образовательного учреждения // Международный журнал прикладных и фундаментальных исследований. – 2014. – № 3-1. – С. 128-129.

15. 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.

16. Назаренко М.А. Межпредметные связи теории организаций, организационной культуры и кадрового аудита // Международный журнал прикладных и фундаментальных исследований. – 2013. – №10-3. – С. 518-519.

17. Назаренко М.А. Мотивационные факторы при получении образования в регионе // Международный журнал экспериментального образования. – 2013. – № 11-1. – С. 159-160.
18. 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.
19. Назаренко М.А. Особенности европейской интеграции в сфере профессионального образования // Мир науки, культуры, образования. – 2013. – № 5. – С. 50-53.
20. 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.
21. Назаренко М.А. Повышение квалификации специалистов по промышленной электронике в области современных информационных технологий // Современные проблемы науки и образования 23.03.2014 URL: http://www.science-education.ru/116-12419 (дата обращения: 15.07.14).
22. Назаренко М.А. Программа развития образования в Московской области и особенности вступившего в действие законодательства // Современные проблемы науки и образования. – 2014. – № 1. – С. 64.
23. 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.
24. Назаренко М.А. Технологии управления развитием персонала в диссертационных исследованиях // Успехи современного естествознания. – 2013. – № 6. – С. 160-162.
25. 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.177–178.
26. 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. 151-152.
27. 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.
28. 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.

29. 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.

30. Назаренко М.А., Котенцов А.Ю. Анализ организационных структур современных предприятий // Международный журнал прикладных и фундаментальных исследований. — 2014. – № 5-2. – С. 143-146.

31. 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.

32. 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.

33. 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.

34. Назаренко М.А., Петров В.А., Сидорин В.В. Управление организационной культурой и этический кодекс вуза // Успехи современного естествознания. – 2013. – № 4. – С. 171–172.

35. Нестерук Ф.Г. Разработка модели адаптивной системы защиты информации на базе нейро-нечетких сетей: дис. канд. техн. наук. – СПб., 2005. – С. 164.

36. 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.

37. 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.

38. Репин Д.С. Анализ и моделирование трафика в корпоративных компьютерных сетях: дис. канд. техн. наук. – М., 2008. – С. 143.

39. 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.

40. Семенов Ю.А. Виртуальные локальные сети VLAN, Интранет [Электронный ресурс] // Телекоммуникационные технологии: сайт. – URL: http://book.itep.ru/6/vlan_62.htm (дата обращения: 14.07.2014).

41. Степашкин М.В. Модели и методика анализа защищенности компьютерных сетей на основе построения деревьев атак: дис. канд. техн. наук. – СПб., 2007. – С. 196.
42. Сторожук Д.О. Методы и алгоритмы для систем мониторинга локальных сетей: дис. канд. техн. наук. – М., 2008. – С. 121.
43. 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.
44. Хайкин С. Нейронные сети: полный курс. – М.: Вильямс, 2006. – 2-е изд. – С. 1104.
45. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: Юниор, 2003. – С. 504.
46. Черненко С.С., Назаренко М.А. Робототехника и ее перспективы в социо-культурном аспекте // Успехи современного естествознания. – 2014. – № 5-2. – С. 194-195.
47. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Книжный мир, 2009. – С. 352.
48. Carter E., Hogue J. Intrusion Prevention Fundamentals. – Indianapolis, IN: Cisco Press, 2006. – P. 312.
49. Chirillo J. Hack Attack Testing: How to Conduct Your Own Security Audit. – Wiley Publishing, 2003. – P. 576.

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.