На правах рукописи

КАЗАКОВА АРИНА ВАЛЕРЬЕВНА

РАЗВИТИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Специальность 08.00.05 - Экономика и управление народным хозяйством: экономика, организация и управление предприятиями, отраслями, комплексами промышленности

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата экономических наук

Самара 2011

Работа выполнена в Самарском государственном экономическом университете

Научный руководитель - доктор экономических наук, профессор
Татарских Борис Яковлевич

Официальные оппоненты: доктор экономических наук, профессор
Ашмарина Светлана Игоревна

доктор экономических наук, профессор
Афоничкин Александр Иванович

Ведущая организация - Ульяновский государственный
технический университет

Защита состоится 5 июля 2011 г. в 9 ч на заседании диссертационного совета Д 212.214.03 при Самарском государственном экономическом университете по адресу: ул. Советской Армии, д. 141, ауд. 325, г. Самара, 443090

С диссертацией можно ознакомиться в библиотеке
Самарского государственного экономического университета

Автореферат разослан 4 мая 2011 г.

Ученый секретарь
диссертационного совета Волкодавова Е.В.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В настоящее время интенсивно развиваются информационные технологии (ИТ), что так же, как глобализация и становление информационной экономики, относится к числу макротенденций современного мирового хозяйства.

За период своего существования, и особенно за последнее десятилетие, в сфере применения информационных технологий произошли коренные перемены. Они принесли бизнесу существенную выгоду, но при этом потребовали более серьезного внимания к сфере безопасности со стороны правительств, коммерческих предприятий, иных организаций и частных пользователей, которые разрабатывают информационные системы, владеют ими, предоставляют их в пользование, управляют ими, обслуживают или используют их.

Актуальность темы исследования определяется и обострением проблем информационной безопасности (ИБ) в условиях интенсивного совершенствования технологий и инструментов защиты данных. Об этом свидетельствуют рост нарушений информационной безопасности и усиливающаяся тяжесть их последствий. Так, общее число нарушений в мире ежегодно увеличивается более чем на 100%, а в России число выявленных преступлений в сфере компьютерной информации возрастает ежегодно в несколько наз. Статистика свидетельствует также, что если коммерческая организация допускает утечку важной внутренней информации, то она в 60% случаях становится банкротом.

Таким образом, существуют факторы, определяющие необходимость взвешенного подхода к указанной проблеме. К ним, в первую очередь, необходимо отнести постоянно возрастающее количество информационных угроз и рисков, а также недостаточный уровень обеспечения информационной безопасности существующих информационных систем.

Информационные риски реализуются через уязвимости современных информационных систем, поддерживающих различные виды деятельности социально-экономической системы. В данной ситуации возникает необходимость обеспечения информационной безопасности социально-экономической системы в целом.

Тенденции развития промышленных предприятий России показывают, что руководство уже принимает некоторые меры по защите важной информации, однако эти действия не носят системного характера, поскольку направлены на устранение отдельных угроз, оставляющих за собой множество уязвимых мест. Также одной из основных причин проблем промышленных предприятий в сфере обеспечения информационной безопасности является отсутствие в данной сфере продуманной и утвержденной политики, базирующейся на организационных, экономических и технических реше-

ниях с последующим контролем их реализации и оценкой эффективности. Это определяет необходимость разработки системы обеспечения информационной безопасности промышленных предприятий.

Таким образом, являются актуальными научные исследования, направленные на повышение эффективности управления промышленным предприятием на основе формирования системы информационной безопасности, способной обеспечить согласованность действий.

Область исследований. Исследование проведено в рамках п.п. 15.1 "Разработка новых и адаптация существующих методов, механизмов и инструментов функционирования экономики, организации и управления хозяйственными образованиями промышленности"; п.п. 15.15 "Теоретические и методологические основы эффективности развития предприятий, отраслей и комплексов народного хозяйства" по специальности 08.00.05 - Экономика и управление народным хозяйством: экономика, организация и управление предприятиями, отраслями, комплексами промышленности Паспорта специальностей ВАК (экономические науки).

Состояние изученности проблемы. Проблемам обеспечения информационной безопасности предприятий в России посвящены работы таких ученых, как А. Абросимов, В. Адрианов, А. Афоничкин, С. Ашмарина, А. Баутов, А. Голов, М. Давлетханов, А. Добрянин, Д. Дьяконов, А. Еляков, А. Курило, В. Лазарев, А. Макарова, Е. Мешайкина, Р. Насакин, Р. Нижегородцев, А. Павлов, А. Пастюшков, П. Покровский, В. Савельев, С. Симонов, Е. Смирнов, Н. Столяров, И. Стрелец, Б. Татарских, Е. Терехова, Ф. Удалов, И. Филиппова, Р. Хайретдинов, В. Ярочкин и др.

Среди исследователей, рассматривавших проблему информационной безопасности с точки зрения высшего руководства предприятий, наибольший вклад внесли Дж. Албаниз, С. Беринато, В. Галатенко, Дж. Джейсинг, Г. Лавджой, А. Лукацкий, Дж. Миллер, А. Мицци, М. Мишель, Д. Моррилл, Дж. Риз, В. Сонненрих, Б. Шнайер, Р. Уитти, А. Уилхайи и некоторые другие.

Вместе с тем подавляющее большинство работ носит сугубо технический характер и ориентировано, главным образом, на ИТ-персонал. Более того, несмотря на постоянно растущее количество исследований в области информационной безопасности, крайне редко затрагивается вопрос комплексного, системного обеспечения информационной безопасности промышленных предприятий на основе учета организационных, технологических, технических, правовых и экономических факторов. Проведенные исследования касаются лишь отдельных аспектов обеспечения информационной безопасности, в то время как комплексность этой проблемы предполагает разработку для ее решения более современных и адекватных методов.

Цель исследования заключается в обосновании теоретических и методических положений развития системы обеспечения информационной безопасности промышленных предприятий.

Для достижения поставленной цели потребовалось решение следующих **задач** диссертационной работы:

- исследовать роль информационной безопасности в процессе информационного обеспечения управленческой деятельности предприятий и проанализировать информационные ресурсы промышленных предприятий с позиции необходимости обеспечения их защиты;
- изучить информационную безопасность с позиции реализации системного подхода и выделить ее основные составляющие;
- выявить требования к информационной безопасности, позволяющие провести оценку защищенности информационных ресурсов, а также оценку достигнутого уровня информационной безопасности;
- разработать организационно-экономические мероприятия для развития системы обеспечения информационной безопасности промышленного предприятия.

Объектом исследования являются промышленные предприятия Российской Федерации.

Предметом исследования выступает совокупность организационно-экономических отношений, возникающих в процессе развития системы обеспечения информационной безопасности промышленных предприятий.

Методологической основой исследования явилась общенаучная методология, предусматривающая системный и процессный подходы к решению рассматриваемых проблем, экономические, социологические и прочие измерения, а также методы экономико-математического моделирования.

Теоретической базой исследования послужили научные труды зарубежных и отечественных ученых в области исследования проблемы обеспечения информационной безопасности, нормативные правовые акты Российской Федерации, а также материалы международных научно-практических конференций.

Информационной основой диссертации явились статистические данные Федеральной службы государственной статистики, российские социологические исследования, материалы исполнительных органов власти, статистические данные Института компьютерной безопасности и Федерального бюро расследований США, отчетность корпораций. Кроме того, использована электронная информация с серверов сети "Интернет".

Научная новизна диссертационного исследования заключается в разработке и обосновании теоретических и методических основ и практических рекомендаций по обеспечению информационной безопасности промышленных предприятий на основе развития сбалансированной системы, позволяющей с позиций комплексного подхода обеспечить согласованность и эффективность действий между организационными, технологическими, техническими, правовыми и экономическими решениями для достижения требуемого уровня информационной безопасности.

Научная новизна диссертационного исследования подтверждается следующими научными результатами, выносимыми на защиту.

1. Разработана иерархия комплексной системы информационного обеспечения управления на предприятии промышленности с учетом достижения требуемого уровня его информационной безопасности.

2. Определены задачи и уровни информационной безопасности в единой системе, реализуемой в рамках концепции информационной безопасности промышленных предприятий, устанавливающей системный подход к проблеме безопасности информационных ресурсов и представляющей собой систематизированное изложение целей, задач, принципов проектирования и комплекса мер по ее обеспечению на предприятии.

3. Выявлены требования, соответствие которым позволяет провести оценку защищенности информационных ресурсов и достигнутого уровня информационной безопасности деятельности промышленных предприятий с учетом проведенного автором ранжирования информационных ресурсов промышленного предприятия на классы по степени их важности и необходимости защиты.

4. Проведена оценка достигнутого уровня информационной безопасности промышленных предприятий Самарской области.

5. Разработана матрица организационно-экономических мероприятий развития системы обеспечения безопасности информационных ресурсов промышленного предприятия, исходя из особенностей их создания, обработки, хранения и перераспределения в рамках реализации системы обеспечения информационной безопасности.

Практическая значимость диссертационного исследования состоит в возможности использования методических положений и рекомендаций в качестве конкретного организационного и экономического инструментария, направленного на совершенствование методов управления промышленным предприятием на основе формирования эффективной системы обеспечения его информационной безопасности.

Полученные результаты диссертационного исследования могут быть использованы в учебном процессе при чтении таких дисциплин, как "Информационная безопасность", "Информационные технологии управления", Информационный менеджмент", а также в системе подготовки и переподготовки руководителей и специалистов промышленных предприятий.

Апробация и внедрение результатов диссертационного исследования. Основные положения и результаты диссертационного исследования прошли апробацию на ряде промышленных предприятий Самарской области, а также обсуждались и получили положительную оценку на международных и всероссийских научно-практических конференциях: V Всероссийской научно-практической конференции "Теоретические проблемы эконо-

мической безопасности России в XXI веке" (Томск, 2008), Всероссийской конференции студентов и молодых ученых "Новой экономике - новые подходы управления" (Самара, 2008), VII Международной научно-практической конференции "Стабилизация экономического развития Российской Федерации" (Пенза, 2008), 5-й Международной научно-практической конференции "Достижения ученых XXI века" (Тамбов, 20 июля 2010 г.), VIII Международной научно-практической конференции "Совершенствование управления научно-технологическим прогрессом в современных условиях" (Пенза, 2010), Международной научно-практической конференции "Инновационная экономика и промышленная политика региона (ЭКОПРОМ-2010)" (Санкт-Петербург, 29 сентября - 3 октября 2010 г.), 9-й Международной научно-практической конференции "Проблемы развития предприятий: теория и практика" (Самара, 18-19 ноября 2010 г.), II Международной научно-практической конференции "Власть, бизнес, бизнес-образование: интеграция на пути модернизации" (Ульяновск, 7 апреля 2011 г.), IX Международной научно-практической конференции "Совершенствование управления научно-технологическим прогрессом в современных условиях" (Пенза, 2011), II Всероссийской конференции студентов и молодых ученых "Новой экономике - новые подходы управления" (Самара, 2011).

Публикации. Основные результаты диссертационного исследования опубликованы в 20 научных работах общим объемом 12,44 печ. л.

Содержание работы. Во введении обоснована актуальность темы, сформулированы цель и задачи исследования, выбран его объект, охарактеризована примененная методика, определены научная новизна и практическая значимость диссертации.

В первой главе "Концептуальные основы обеспечения информационной безопасности" выявлена информационная составляющая управляющей деятельности, определены проблемы и концептуальные основы обеспечения информационной безопасности промышленных предприятий с позиции системного подхода.

Во второй главе "Предпосылки и необходимость развития системы обеспечения информационной безопасности промышленных предприятий" структурированы угрозы информационной безопасности и особенности обеспечения информационной безопасности в условиях информатизации деятельности промышленных предприятий Самарской области.

В третьей главе "Направления развития системы обеспечения информационной безопасности промышленных предприятий" исследована политика информационной безопасности как инструмент развития, а также разработана система организационно-экономических мероприятий, обеспечивающих развитие системы информационной безопасности промышленных предприятий.

В заключении приведены основные результаты исследования, обоснованы рекомендации по развитию системы обеспечения информационной безопасности промышленных предприятий.

ОСНОВНЫЕ ПОЛОЖЕНИЯ, ВЫНОСИМЫЕ НА ЗАЩИТУ

1. Разработана иерархия комплексной системы информационного обеспечения управления на предприятии промышленности с учетом достижения требуемого уровня его информационной безопасности.

Рыночная экономика в России выдвинула новые требования к организации современного управления производством. В этих условиях многими западными и отечественными учеными определяющая роль в развитии и целевом функционировании системы управления отводится информационному обеспечению управленческой деятельности. Это сложный, динамичный, комплексный процесс, позволяющий удовлетворять информационные потребности управленцев и выполняющий функции рационализации деятельности аппарата управлении, т.е. процесс предоставления информации отдельным лицам или их группам - пользователям информационных систем в соответствии с их информационными потребностями.

Смысл информационного обеспечения заключается в органическом соединении научных знаний, научной методологии и методики с новейшими техническими средствами во всех проявлениях информационной работы. Под информационным обеспечением управления промышленным предприятием понимается процесс удовлетворения потребностей пользователей в информации, необходимой для принятия решений. Иерархия уровней информационного обеспечения управления предприятием представлена на рис. 1.

В связи с возникновением правовых отношений в информационной сфере информационные ресурсы организации следует подразделять на открытые и с ограничением доступа. Под открытыми информационными ресурсами понимаются массивы информации, которые на основе законодательства или по добровольному решению собственника информации доступны для свободного ознакомления, копирования, тиражирования и т.д. Наряду с открытой информацией на предприятии объективно существует массив информации, к которой необходимо ограничить доступ из внешней среды, а также лимитировать его внутри организации. Причина появления данного вида информации в условиях рыночных отношений - наличие конкуренции между хозяйствующими субъектами. В экономической практике закрытая информация получила название конфиденциальной, т.е. информации ограниченного распространения.

Рис. 1. **Иерархия уровней информационного обеспечения управления предприятием**

Данная типология информации делает возможным моделирование иерархии внутрифирменной информации и проектирование информационных процессов, построение комплексной системы информационного обеспечения управления на предприятии промышленности с учетом обеспечения его информационной безопасности. С нашей точки зрения, при проектировании информационных систем управления ключевым признаком является классификация информации по различным уровням иерархии управления, раскрывающая специфику информационных потребностей руководителей различных уровней и в дальнейшем позволяющая разработать требования и критерии обеспечения необходимого уровня информационной безопасности предприятия (табл. 1).

Информация, обращающаяся в информационных каналах, представляет собой сведения о наиболее важных стратегических, оперативных и тактических управленческих решениях менеджеров предприятия, а также статистические и другие данные, которые служат основой для принятия этих решений. В результате информация, используемая в повседневной жизни предприятия, составляет его ресурс, содержащий сведения о стабильности финансово-экономической деятельности предприятия и факторах, влияющих на нее, а также о рыночном преимуществе перед конкурентами и причинах, предопределяющих его наличие или отсутствие. В настоящее время прослеживается тенденция возрастающей зависимости промышленных предприятий от значительного объема информационных потоков. С развитием информационных и коммуникационных технологий трансформировался обмен различного вида информацией между ее пользователями, что позволяет при помощи информационных технологий оперативно решать многие задачи современного общества. Тем не менее, постоянное усложнение вычислительных систем и сетей, на основе которых лежат внутриорганизационные, межорганизационные, национальные и мировое информационные пространства, ставит перед современным обществом задачи обеспечения его информационной безопасности. С каждым годом все больше и больше совершенствуются технологий защиты данных, но уязвимость защиты не только не уменьшается, а постоянно растет. Поэтому очевидна актуальность проблем, связанных с защитой потоков данных и информационной безопасностью их сбора, хранения, обработки и передачи.

В научной литературе авторы дают различные определения информационной безопасности, представляющей собой состояние информационной системы, в котором она может противостоять воздействию внутренних и внешних угроз, не инициируя их возникновение для элементов системы и внешней среды. Это состояние наиболее эффективного использования информационно-технологического ресурса предприятия в целях укрепления его финансово-экономической стабильности, защиты конфиденциальной информации и коммерческой тайны, сбора и анализа информации как о внутренней, так и о внешней среде.

Таблица 1

Особенности информации на различных уровнях иерархии предприятия

Признаки информации	Уровни иерархии управления		
	Оперативное управление	Средний уровень управления	Высшее руководство
Планирование	Минимальное	Умеренное	Значительное
Контроль	Значительный	Значительный	Умеренный
Временная перспектива	Изо дня в день	До года	От года до десяти лет
Тип используемой информации	Внутренняя, точная, ограниченная, запрограммированная, полученная из прошлого опыта	Внутренняя, более точная, незапрограммированная и запрограммированная	Внешняя и внутренняя, неограниченная, незапрограммированная, прогнозная
Область применения	Осуществление процессов, контроль за ходом процессов	Проектирование, текущая и оперативная деятельность	Стратегическое управление и планирование
Измерение работы	Сравнительно простое	Менее сложное	Затруднено
Уровень сложности	Простой	Менее сложный, с переменными, поддающийся определению	Очень сложный, с многими переменными
Сфера деятельности	Весьма ограниченная	Полная функциональная сфера, умеренно ограниченная	Крайне обширный
Степень доступа к информации	Ограниченный доступ	Высокая степень доступа	Полный доступ
Значимые информационные роли	Приемник	Распространитель	Космополит, разработчик
Степень агрегирования	Элементы данных	Блоки данных	Массивы данных
Периодичность	Ритмичная: квартальная, месячная, еженедельная, ежедневная	Последовательная - к сроку	Нерегулярная
Выходная информация	Сводки, отчеты, данные	Правила, процедуры, схемы процессов, аналитические обзоры	Цели, стратегии, внешние коммуникации, распоряжения
Тип деятельности	Работоспособность, эффективность	Ответственность, способность убеждать, управлять	Творческий подход
Число лиц, причастных к управленческой деятельности	Большое	Умеренное	Незначительное
Степени защиты и важность информации	Открытая информация, служебная конфиденциальная	Конфиденциальная и служебная и строго конфиденциальная	Абсолютно и строго конфиденциальная информация
Требуемый уровень обеспечения информационной безопасности	Произвольное управление информационной безопасностью	Принудительное управление информационной безопасностью	Верифицированная защита

2. Определены задачи и уровни информационной безопасности в единой системе, реализуемой в рамках концепции информационной безопасности промышленных предприятий, устанавливающей системный подход к проблеме безопасности информационных ресурсов и представляющей собой систематизированное изложение целей, задач, принципов проектирования и комплекса мер по ее обеспечению на предприятии.

Понятие "информационная безопасность" используется весьма широко. Наиболее часто оно подменяется родственным понятием "защита информации", в результате чего проблема сводится к частной задаче защиты информации от утечки по различным каналам при ее обработке средствами вычислительной техники.

По нашему мнению, наиболее важным и сложным для реализации на практике аспектом ИБ является обеспечение ее конфиденциальности. Существуют три основные причины, приводящие к потере конфиденциальности информации: разглашение, утечка и несанкционированный доступ. Условиями, способствующими неправомерному завладению конфиденциальной информацией, принято считать подкуп, болтливость сотрудников, отсутствие контроля и трудовой дисциплины, плохую работу кадровых служб при найме работников, психологическую несовместимость членов коллектива, низкую заработную плату и т.п. Информационная безопасность, представляющая собой сложную, многогранную проблему, должна обеспечиваться для всех экономических агентов и хозяйствующих субъектов. Определим уровни обеспечения ИБ, в которую включены заинтересованные в ней субъекты:

1) государственный:
- концептуально-политический;
- законодательный;
- нормативно-технический;

2) организационный:
- административный;
- процедурный;
- программно-технический;
- экономический;

3) гражданский.

Постоянный рост темпов развития и распространения информационных технологий, высокая конкуренция и существующая криминогенная обстановка ставят вопрос о создании на предприятии единой, соответствующей всем современным требованиям системы информационной безопасности. Система ИБ для предприятия должна включать в себя и увязывать правовые, организационные, физические, инженерно-технические и программные направления обеспечения защиты информационных ресурсов. Для полной оценки ситуации на предприятии по всем направлениям обеспечения ИБ необходима разработка концепции информационной безопасности (рис. 2), которая бы устанавливала системный подход к проблеме

безопасности информационных ресурсов и представляла собой систематизированное изложение целей, задач, принципов проектирования и комплекса мер по обеспечению ИБ на предприятии.

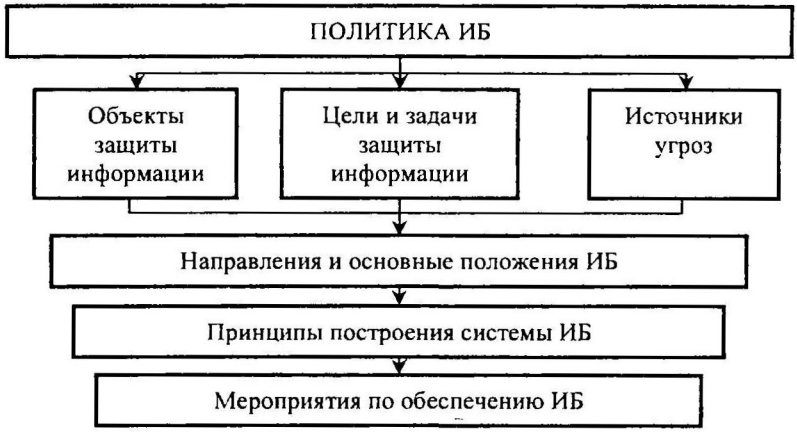

Рис. 2. **Концепция информационной безопасности предприятия**

При разработке данной концепции следует учитывать современные организационные, правовые методы и программно-технические средства противодействия внешним и внутренним угрозам ИБ, а также существующее состояние защищенности информации и перспективы развития информационных технологий.

Основной целью концепции ИБ является защита предприятий от возможного нанесения им материального, морального или иного ущерба из-за преднамеренных или случайных действий с информационными ресурсами, результатом которых выступает потеря их свойств, таких как доступность, целостность и конфиденциальность.

Задачи концепции ИБ состоят в обеспечении защиты существующей информационной инфраструктуры предприятия от вмешательства злоумышленников, в создании условий для локализации и минимизации возможного ущерба, в выявлении на начальной стадии причин возникновения источников угроз. Решение вышеназванных задач достигается путем: четкого категорирования информационных ресурсов компании; регламентации действий сотрудников; подготовки лиц, ответственных за обеспечение и соблюдение ИБ; строгого выполнения и знания сотрудниками предприятия свода правил и требований по обеспечению ИБ; использования программно-технических средств защиты информации; правовой и физической защиты информации; постоянного контроля и анализа эффективности и необходимости используемой системы защиты информации и принимаемых мер.

3. Выявлены требования, соответствие которым позволяет провести оценку защищенности информационных ресурсов и достигну-

того уровня информационной безопасности деятельности промышленных предприятий с учетом проведенного автором ранжирования информационных ресурсов промышленного предприятия на классы по степени их важности и необходимости защиты.

Информационная безопасность служит функциональным элементом системы обеспечения стратегического развития промышленного предприятия, поэтому ее основная задача - обеспечить стабильность существования предприятия в настоящем и перспективы его устойчивого развития в будущем. Основными предпосылками к созданию системы защиты информации являются ее значимость как инструмента и ресурса бизнеса, а также угроза для предприятия понести материальный ущерб от утечки информации.

Информационные ресурсы промышленного предприятия в зависимости от степени важности и необходимости обеспечения их защиты можно отнести к различным классам (табл. 2).

Таблица 2

Классы информационных ресурсов предприятия

Класс	Содержание
5-й: открытая информация	Общие сведения о предприятии и характере его деятельности, необходимые для составления публикуемых годовых отчетов, пресс-релизов, публикаций о предприятии в СМИ, рекламной и агитационной продукции
4-й: служебная информация	Применяемые в повседневной работе предприятия сведения, широкое опубликование или нарушение целостности которых причинило бы предприятию беспокойство, не нанеся при этом значимых материальных потерь или серьезного ущерба его имиджу. Примерами подобной информации могут быть служебные записки, расписание встреч, текущие данные, правила внутреннего распорядка и т.п.
3-й: конфиденциальная информация	Сведения о контрагентах предприятия и условиях работы с ними, о процедурах, разработанных или освоенных на предприятии методике и формах управления им, находящиеся на начальной стадии бизнес-проекты, а также документы, определяющие общие планы и перспективы развития предприятия, потенциально способные обеспечить конкурентное преимущество хозяйствующего субъекта в будущем
2-й: строго конфиденциальная информация	Сведения, содержащие аналитическую обработку результатов бухгалтерского учета, производственной, маркетинговой, управленческой деятельности предприятия, деловые планы и бизнес-проекты, предопределяющие конкретные направления развития предприятия и сферы приложения его усилий с целью укрепления и развития собственного конкурентного преимущества, собственные перспективные дизайнерские разработки, описание информационной политики предприятия, структура и методы работы системы его экономической безопасности, в том числе и по информационной составляющей, информация о конкурентах, собранная методами бизнес-разведки
1-й: абсолютно конфиденциальная информация	Важные внутренние документы, в том числе инвестиционные, маркетинговые, производственные и управленческие стратегии и стратегические приоритеты предприятия, программы поглощения и слияния компаний и другая информация, разглашение или разрушение которой способно нанести фатальный ущерб

Так, информационные ресурсы, относящиеся к категории открытой информации, не содержат сведений конфиденциального характера, но в то же время общедоступны, что делает наиболее уязвимой их целостность. Служебная информация обычно содержит элементы секретности, но считается, что оперативность ее использования полностью компенсирует потенциальный ущерб, который может возникнуть в результате нарушения ее конфиденциальности. Поэтому задача обеспечения безопасности данного класса информации - защита целостности и доступности сведений. Конфиденциальная информация чаще всего используется на тактическом и оперативном уровнях, что предъявляет авторизованным пользователям равные требования к обеспечению конфиденциальности, целостности и доступности сведений данного класса. При анализе массива строго конфиденциальной информации становится очевидным, что ключевыми свойствами ее являются конфиденциальность и целостность. Значение доступности снижается в связи с резким сокращением круга авторизованных пользователей. Контрагенты и конкуренты обычно проявляют максимальный интерес именно к конфиденциальности данной информации, поскольку затраты на приобретение таких сведений окупаются при их использовании. Абсолютно конфиденциальная информация предназначена только для высшего менеджмента предприятия, поскольку содержит в себе сведения, риск нарушения конфиденциальности которых неприемлемо высок при расширении круга пользователей. Основным свойством данной информации, способным обеспечить конкурентное преимущество предприятия, является конфиденциальность. В большинстве случаев именно нарушение конфиденциальности подобной информации приводит к возникновению значительного материального и морального ущерба.

Степень защиты информационных ресурсов и достигнутый уровень информационной безопасности можно оценить, анализируя политику безопасности предприятия - набор законов, правил и норм, определяющих, как оно обрабатывает, защищает и распространяет информацию. В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия. Также выделяют гарантированность функционирования системы, которая показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. Гарантированность можно считать пассивным компонентом защиты информации.

Основные элементы политики информационной безопасности следующие: 1) произвольное управление доступом к информационным ресурсам; 2) безопасность повторного использования информационных ресурсов; 3) метки безопасности информационных ресурсов; 4) принудительное управление доступом к информационным ресурсам. В зависимости от проработанности вышеперечисленных элементов политики безопасности можно ранжировать информационные системы по степени их надежности. Определяется

четыре уровня безопасности (надежности) - D, C, B и A. Уровень D вводится для систем, признанных неудовлетворительными. По мере перехода от уровня C к уровню A к надежности систем предъявляются все более жесткие требования. Таким образом, можно предложить следующие уровни информационной безопасности: D - неудовлетворительная безопасность; C - произвольное управление доступом; B - принудительное управление доступом; A - верифицированная защита. Чтобы система могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять огромному количеству требований, которые серьезно усложняются при переходе к последующему уровню.

Распределение требований по уровням вызывает ряд конкретных возражений. Неоправданно далеко отодвинуты такие очевидные требования, как извещение о нарушении защиты, конфигурационное управление, безопасный запуск и восстановление после сбоев. Возможно, это оправданно в физически защищенной военной среде, но никак не в коммерческой, когда постоянное слежение за перемещениями сотрудников может быть очень дорогим удовольствием. Требования полностью игнорируют коммуникационный аспект, присущий современным системам.

В разрабатываемой в нашей стране концепции информационной безопасности предусматривается подразделение информационных систем на классы их защищенности. Классы защищенности подразделяются на четыре группы, отличающиеся качественным уровнем защиты: первая группа содержит только один седьмой класс; вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы; третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы; четвертая группа характеризуется верифицированной защитой и содержит только первый класс. Приведем сводную таблицу распределения показателей защищенности по классам (табл. 3).

Соответствие системы информационной безопасности изложенным в таблице критериям позволяет определить ее класс защищенности. По существу, перед нами минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность защищаемой информации.

Таким образом, с практической точки зрения, под информационной безопасностью мы будем понимать защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям этой информации и поддерживающей инфраструктуры. Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности. На практике под этим понимается поддержание целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Таблица 3

Распределение показателей защищенности по классам

Показатель	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля	+	+	+	+	+	+
Идентификация и аутентификация	+	+	+	+	+	+
Тестирование	+	+	+	+	+	+
Руководство пользователя	+	+	+	+	+	+
Текстовая документация	+	+	+	+	+	+
Конструкторская (проектная документация)	+	+	+	+	+	+
Очистка памяти	-	+	+	+	+	+
Гарантия проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	+	+
Целостность	-	+	+	+	+	+
Мандатный принцип контроля	-	-	+	+	+	+
Изоляция модулей	-	-	+	+	+	+
Маркировка документов	-	-	+	+	+	+
Защита ввода и вывода на отчуждаемый носитель	-	-	+	+	+	+
Сопоставление пользователя с устройством	-	-	+	+	+	+
Взаимодействие пользователя с комплексом средств защиты (КСЗ)	-	-	-	+	+	+
Надежное восстановление	-	-	-	+	+	+
Контроль модификации	-	-	-	-	+	+
Контроль дистрибуции	-	-	-	-	+	+
Гарантия архитектуры	-	-	-	-	-	+

4. Проведена оценка достигнутого уровня информационной безопасности промышленных предприятий Самарской области.

Россия в период глобализации и информатизации мировой экономики находится в достаточно сложном положении. Она оказывается одновременно и включенной в глобализационные процессы, участвуя в мировом финансовом и информационном обмене, осуществляя различные виды внешнеэкономических связей, и, в значительной степени, исключенной из мирового информационного пространства. В целом уровень информатизации Самарской области несколько выше уровня информатизации в среднем по России.

Оценку организации информационных процессов на промышленных предприятиях Самарской области целесообразно проводить посредством анализа структуры и функций информационных систем управления. Анализ существующих систем обработки информации, в большей степени определяющих использование информационного ресурса, позволил выявить недостатки организационного характера, сдерживающие процессы максимального использования информационного потенциала производства, а также серьезные проблемы с обеспечением информационной безо-

пасности хозяйственной деятельности. К основным причинам неэффективности организационного построения информационных систем можно отнести следующие: отсутствие разработанных организационных принципов взаимодействия субъектов хозяйствования в регионе; отсутствие системного подхода к проблеме информатизации управленческой деятельности, информационной согласованности управленческих задач, решаемых внутри функциональных подразделений, с задачами других подсистем. В итоге происходит снижение оперативности, достоверности и качества результативной информации; отмечается статичная структура решаемых информационной системой задач с применением жесткого алгоритма и периодичности решения, следствием чего являются отсутствие способности реагирования на возмущающие воздействия, привлечение больших дополнительных трудозатрат для обеспечения должного уровня оперативности, достоверности и полноты информации; значительное запаздывание информационных потоков относительно материальных; отрыв информации от первоисточника, в результате, что приводит к низкой достоверности получаемой информации.

Скажем, в ежегодных отчетах по своей деятельности ОАО "ВБМ" указывает следующее. В течение 2008 г. были введены в эксплуатацию 19 новых компьютеров в подразделениях предприятия, в 2009 г. этот показатель составил 22 единицы. Были проведены работы по дальнейшему развитию локальной сети предприятия. Проводилась работа по развитию информационной системы предприятия: завершается 4-й этап разработки информационной Базы данных (БД) "Техническая подготовка долотного производства "SmarTeam". Тестирование разработок по 4-му этапу завершено в феврале 2009 г.; разработана программа складского учета дорогостоящих материалов (сталь, твердосплавные материалы, бронзы) на складах ОМТС. Несколько иная ситуация наблюдается в деятельности ОАО "Кузнецов". Распределение затрат по статьям расходов отражено на рис. 3.

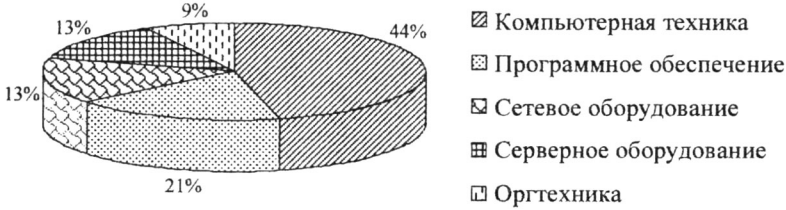

Рис. 3. **Структура затрат на информатизацию ОАО "Кузнецов"**

Инертность существующих информационных систем, низкое качество предоставляемой информации, "пакетный" режим обработки, незначительная диалоговая поддержка не обеспечивают эффективности использования информационных ресурсов. Повышение ее уровня видит-

ся в создании информационно совместимых технологий на предприятии, начиная с каждого рабочего места.

Достигнутые показатели в целом можно охарактеризовать как недостаточно эффективные. На предприятие поступает огромный объем информации, в основном внешней, которая не автоматизируется. Низкий уровень информационной емкости рабочих мест специалистов делает невозможным повышение информационного потенциала на качественно новом уровне. Неэффективность построения существующих ИТ является одной из причин неполной загрузки вычислительной техники.

Внедрение новых технологий и совершенствование имеющихся - наиболее эффективные средства достижения конкурентоспособных позиций на рынке и снижения издержек производства, и в то же время это основные факторы снижения информационной безопасности.

Для определения достигнутого уровня информационной безопасности промышленных предприятий построим диаграмму по системе ранее обозначенных требований (рис. 5). Соответствие требованиям, присутствующим в системе обеспечения информационной безопасности всех исследованных предприятий, отражать на диаграмме представляется нецелесообразным.

Рис. 5. **Уровень информационной безопасности промышленных предприятий**

На основе предложенных требований оценки анализа уровня информационного обеспечения управленческой деятельности и использования внешней информационной продукции были проведены исследования, результаты которых свидетельствуют о необходимости обеспечения информационной безопасности промышленных предприятий.

Таким образом, изучение количественных и качественных характеристик информационной деятельности предприятий показало следующие уровни и классы информационной безопасности (табл. 4).

Таблица 4

Достигнутый уровень информационной безопасности промышленных предприятий

Предприятие	Уровень безопасности (надежности)	Класс защищенности
ОАО "Кузнецов"	С	3
ОАО "ВБМ"	В	5
ЗАО "САМАРА-НАФТА"	В	4

Исследуемые предприятия не имеют достаточных возможностей для формирования системы обеспечения информационной безопасности, поэтому целесообразно активизировать информационные функции как в системе формирования, так и в системе использования информационных ресурсов, а также в системе обеспечения информационной безопасности. Сегодня многие российские промышленные предприятия решают задачи создания системы информационной безопасности, которая соответствовала бы лучшим практикам и стандартам в области ИБ и отвечала бы современным требованиям защиты информации по ее параметрам конфиденциальности, целостности и доступности. Причем этот вопрос важен не только для новых предприятий, развивающих свой бизнес с использованием современных информационных технологий управления. Не менее, а скорее и более важной эта проблема является для предприятий и организаций, давно работающих на рынке, которые приходят к необходимости модернизировать существующую у них систему ИБ. Необходимость повышения эффективности системы ИБ связана с обострением проблем защиты информации. Здесь можно упомянуть растущую потребность обеспечения конфиденциальности данных. Отечественные промышленные предприятия вслед за своими западными коллегами приходят к необходимости учитывать так называемые репутационные риски, ответственность по обеспечению конфиденциальности данных своих клиентов, субподрядчиков, партнеров.

Представляется целесообразным утверждать, что при подходах, которых придерживаются отечественные промышленные предприятия, проблема информационной безопасности не только не решается, но и зачастую усугубляется, поскольку принимаемые решения направлены на реализацию одной или нескольких специальных задач, но не являются системой взаимодействующих и взаимодополняющих друг друга элементов, которая способна в полной мере обеспечить требуемый уровень информационной безопасности.

5. Разработана матрица организационно-экономических мероприятий системы обеспечения безопасности информационных ресурсов промышленного предприятия, исходя из особенностей их создания, обработки, хранения и перераспределения в рамках реализации системы обеспечения информационной безопасности.

Разделение информационных ресурсов предприятия на классы, помимо объективно вытекающего отсюда разграничения доступа к ним, позволяет разработать подход к обеспечению защиты информационной системы предприятия от негативного воздействия на определенные классы информации, исходя из особенностей их создания, обработки, хранения и перераспределения, а также построить матрицу организационно-экономических мероприятий развития безопасности информационных ресурсов предприятия (табл. 5).

Для построения комплексной системы информационной безопасности предприятия следует определить характер процессов, происходящих в информационной системе организации, и специфику возникновения и реализации угроз, а также систему мер и методов для защиты информации различных классов. Поэтому необходимо проследить процесс возникновения и реализации угроз: очевидно, что существующий источник негативного воздействия, активизируясь, генерирует угрозу, которая для предприятия реализуется в атаке на его информационную систему, затем атака воздействует на уязвимость организации, что и приводит к возникновению ущерба.

В идеале комплексная система защиты собственных информационных ресурсов должна охватывать все стадии данного процесса, что позволит обеспечить максимальную защищенность информационной системы предприятия, не допустить наступления ущерба или свести его проявление к минимуму. Таким образом, в основу построения любой системы собственной информационной безопасности должна быть положена оборонительная стратегия, которая включает в себя комплекс мер защитного характера. По времени реализации защитные процедуры оборонительной стратегии подразделяются на реактивные, т.е. начинающие функционировать в связи с наступлением ущерба и направленные на его минимизацию, и единовременные, т.е. реагирующие на негативное воздействие на информационную систему и ориентированные на ее защиту. Целью единовременных мер является предотвращение возникновения ущерба как такового. Данный комплекс защитных мер служит фундаментом системы информационной безопасности предприятия, но эффективность этих мер снижается при появлении нового источника угроз, генерирующего атаку, ориентированную на другую уязвимость.

Таблица 5

Матрица организационно-экономических мероприятий обеспечения безопасности информационных ресурсов промышленного предприятия

Реакция системы				Воздействие на стабильность хозяйственной деятельности	Потенциальный ущерб		Форма воздействия угрозы	Характеристика объекта атаки	
Компенсационные мероприятия	Организационный уровень разрешения кризисной ситуации	Реактивные мероприятия	Меры управленческого воздействия на виновного		Потенциальные финансовые потери	Потенциальные моральные потери		Организационный уровень пользователя	Класс информационного ресурса
Требование компенсации ущерба через суд	Высший менеджмент предприятия, руководитель службы безопасности	Расследование и корректировка системы информационной безопасности	Увольнение	Фатальное	Критические	Критические	Нарушение конфиденциальности	Высший менеджмент предприятия	**Абсолютно конфиденциальная информация**
Требование компенсации ущерба через суд	Высший менеджмент предприятия, руководитель службы безопасности	Расследование и корректировка системы информационной безопасности	Строгое дисциплинарное воздействие	Разрушающее	Невосполнимые	Невосполнимые	Нарушение конфиденциальности целостности	Менеджеры среднего звена	**Строго конфиденциальная информация**
Экономичесс-кие, юридические и PR-акции	Менеджеры среднего звена, руководитель службы безопасности	Расследование и восстановление безопасности ресурса	Строгое дисциплинарное воздействие	Критическое	Восполнимые	Восполнимые	Нарушение конфиденциальности, целостности и доступности	Линейные менеджеры и авториз-ованные сотрудники	**Конфиденциальная информация**
Экономичес-кие	Линейные менеджеры, исполнители	Расследование и восстановление безопасности ресурса	Письменное предупреждение	Контролируемое	Незначитель-ные	Незначитель-ные	Нарушение целостности и доступности	Все сотрудники	**Служебная информация**
Нет	Линейные менеджеры, сотрудники службы безопасности	Восстановление безопасности ресурса	Устное преду-преждение	Раздражающее	Нет	Нет	Нарушение целостности	Все пользователи	**Открытая информация**

Для защиты информационных ресурсов, относящихся к 1-3 классам, помимо защитных мероприятий, необходимо введение контролирующих процедур. Их задача состоит в мониторинге информационной системы предприятия с целью распознания произошедших информационных инцидентов и анализа слабых мест информационной среды, что позволяет инициировать защитные мероприятия не по фактам негативного воздействия на уязвимость или возникновения ущерба, а с момента начала информационной атаки. Внедрение в систему информационной безопасности предприятия контролирующих мероприятий позволяет ему перейти к реализации наступательной стратегии, обеспечивающей широкую защиту информационных ресурсов организации по всему спектру уязвимостей от большинства атак. Но существует реальная угроза возникновения частичного ущерба вследствие появления нового источника угроз и его негативного влияния на информационную систему предприятия, что экономически недопустимо для строго конфиденциальной или абсолютно конфиденциальной информации, поскольку способно вызвать значительные финансовые потери или дискредитацию предприятия в целом в глазах контрагентов или государственных структур. В связи с этим для эффективной защиты информационных ресурсов 1-2-го классов необходимы обеспечение распознания источника информационной угрозы, осуществление контроля над его активностью и нейтрализация процесса возникновения ущерба еще на стадии информационного инцидента. Реализация комплекса превентивных мер составляет элемент упреждающей стратегии обеспечения информационной безопасности. Другим элементом данной стратегии являются защитные мероприятия опережающего характера, которые воздействуют непосредственно на процесс реализации угрозы на этапе начала атаки с целью ее нейтрализации или снижения риска возникновения ущерба до приемлемого уровня. Превентивные меры служат триггером, запускающим систему контролирующих и защитных стратегий разных уровней, создавая тем самым оптимальную готовность системы защиты собственных информационных ресурсов предприятия и ориентируя эту систему на конкретную угрозу, что позволяет снизить расходы на поддержание защитных процедур, готовых к отражению атаки.

Приведенная выше методика построения системы безопасности информационных ресурсов, которая предполагает как разделение информационных ресурсов внутрифирменного обращения на классы по степени их важности для осуществления основных видов деятельности предприятия и по степени уязвимости для негативного воздействия, так и определение конкретных направлений защиты информации в зависимо-

сти от характерных особенностей ее создания, обработки, хранения и перераспределения, позволяет создать на конкретном предприятии максимально гибкую и адекватную условиям функционирования систему защиты, которая способна обеспечить оптимальный уровень информационной безопасности при рациональном использовании материальных и кадровых ресурсов предприятия. Подводя итоги описанию и анализу основных форм и методов обеспечения стабильного функционирования информационной системы, отметим, что сам процесс обеспечения информационной безопасности хозяйствующего субъекта должен носить комплексный и системный характер.

ПУБЛИКАЦИИЙ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

В журналах, определенных ВАК

1. *Казакова, А.В.* Подходы к определению информационной безопасности промышленного предприятия [Текст] / А.В. Казакова // Вестн. ун-та. - М., 2011. - № 2. - С. 126-129. - 0,44 печ. л.

2. *Казакова, А.В.* Концепция информационной безопасности промышленных предприятий [Текст] / А.В. Казакова // Вестн. Самар. гос. ун-та. - Самара, 2011. - № 3 (84). - С. 128-135. - 0,5 печ. л.

3. *Казакова, А.В.* Развитие системы обеспечения информационной безпасности промышленных предприятий [Текст] / А.В. Казакова // Вестн. Самар. гос. экон. ун-та. - Самара, 2011. - № 5 (79). - С. 29-38. - 0,5 печ. л.

В других изданиях

4. *Казакова, А.В.* Разработка эффективности системы информационной безопасности предприятий промышленности [Текст] / А.В. Казакова // О научных проблемах, которые предстоит решать молодым : сб. материалов II Всерос. конф. студентов и молодых ученых "Новой экономике - новые подходы управления". - Самара : Изд-во Самар. ин-та управления, 2011. - С. 231-240. - 0,6 печ. л.

5. *Казакова, А.В.* Система защиты информационного пространства предприятия [Текст] / А.В. Казакова / Совершенствование управления научно-технологическим прогрессом в современных условиях : сб. ст. IX Междунар. науч.-практ. конф. / МНИЦ ПГСХА. - Пенза : РИО ПГСХА, 2011. - С. 39-44. - 0,35 печ. л.

6. *Казакова, А.В.* Обеспечения формирования эффективной системы информационной безопасности предприятий промышленности [Текст] / А.В. Балановская, А.В. Казакова // Власть, бизнес, бизнес-образование: интеграция на пути модернизации" : материалы II Междунар. науч.-практ. конф., 7 апр. 2011 г., г. Ульяновск. - Ульяновск, 2011. - С. 49-55. - 0,6/0,3 печ. л.

7. *Казакова, А.В.* Организационные механизмы разработки и управления информационной безопасностью промышленных предприятий [Текст] : моно-

графия / А.В. Балановская, А.В. Казакова. - Самара : Изд-во Самар. ин-та управления, 2010. - 138 с.: ил. - 10,0/5,0 печ. л.

8. *Казакова, А.В.* Инструменты информационного обеспечения стратегического управления [Текст] / А.В. Балановская, Т.В. Харитонова, А.В. Казакова // Менеджмент : учеб. пособие. - Самара: Изд-во Самар. ин-та управления, 2010. - Разд. 6.3. - С. 169-179. - 20,1/0,6 печ. л.

9. *Казакова, А.В.* Современное состояние подготовки специалистов по информационной безопасности [Текст] / А.В. Казакова // Образование и наука как основа модернизации социально-экономического развития региона: сб. науч. ст. региональной сессии Годовой тематической конф. Новой экономической ассоциации "Образование, наука и модернизация", 7 дек. 2010 г. / Уфим. гос. акад. экон. и сервиса. - Уфа, 2010. - С. 280-283. - 0,35 печ. л.

10. *Казакова, А.В.* Методические основы обеспечения информационной безопасности функционирования промышленных предприятий [Текст] / А.В. Казакова // Актуальные вопросы вузовской науки : сб. науч. и науч.-метод. ст. Вып. 5. - Самара : Изд-во Самар. ин-та управления, 2010. - С. 49-58. - 0,6 печ. л.

11. *Казакова, А.В.* Угрозы информационной безопасности предприятий. [Текст] / А.В. Казакова // Проблемы развития предприятий: теория и практика : материалы 9-й Междунар. науч.-практ. конф., 18-19 нояб. 2010 г. / редкол.: А.П. Жабин, Е.В. Зарова (отв. ред.) [и др.]. Ч. 1. - Самара : Изд-во Самар. гос. экон. ун-та, 2010. - С. 267-269. - 0,2 печ. л.

12. *Казакова, А.В.* Предпосылки и необходимость обеспечения информационной безопасности [Текст] / А.В. Балановская, А.В. Казакова // Инновационная экономика и промышленная политика региона (ЭКОПРОМ-2010) / под. ред. д-ра экон. наук, проф. А.В. Бабкина : тр. Междунар. науч.-практ. конф., 29 сент. - 3 окт. 2010 г. Т. 1. - СПб. : Изд-во Политехн. ун-та, 2010. - С. 65-69. - 0,25/0,2 печ. л.

13. *Казакова, А.В.* Теоретико-методологические аспекты информационного обеспечения стратегического управления промышленным предприятием [Текст] / А.В. Казакова // Совершенствование управления научно-технологическим прогрессом в современных условиях : сб. ст. VIII Междунар. науч.-практ. конф. / МНИЦ ПГСХА. - Пенза : РИО ПГСХА, 2010. - С. 64-70. - 0,7 печ. л.

14. *Казакова, А.В.* Роль информационной безопасности в деятельности предприятия [Текст] / А.В. Балановская, А.В. Казакова // Достижения ученых XXI века : сб. материалов 5-й Междунар. науч.-практ. конф., 20 июля 2010 г. - Тамбов : Изд-во ТАМБОВПРИНТ, 2010. - С. 44-47. - 0,3/0,2 печ. л.

15. *Казакова, А.В.* Маркетинговый подход к оценке информационного потенциала предприятия [Текст] / А.В. Балановская, А.В. Казакова // Актуальные вопросы вузовской науки : сб. науч. ст. Вып. 4. - Самара : Изд-во Самар. ин-та управления, 2009. - С. 5-20. - 0,7/0,35 печ. л.

16. *Казакова, А.В.* Организационные изменения в процессе информационного обеспечения стратегического управления [Текст] / А.В. Казакова // Стабилизация экономического развития Российской Федерации : сб. ст. VII Междунар. науч.-практ. конф. - Пенза : РИО ПГСХА, 2008. - С. 190-193. - 0,3 печ. л.

17. *Казакова, А.В.* Формирование информационной базы предприятия для принятия стратегических решений [Текст] / А.В. Балановская, А.В. Казакова // Стабилизация экономического развития Российской Федерации : сб. ст. VII Междунар. науч.-практ. конф. - Пенза : РИО ПГСХА, 2008. - С. 46-48. - 0,25/0,2 печ. л.

18. *Казакова, А.В.* Информационный ресурс в управление современным предприятием [Текст] / А.В. Казакова // О научных проблемах, которые предстоит решать молодым ... : сб. материалов Всерос. конф. студентов и молодых ученых "Новой экономике - новые подходы управления". - Самара : Изд-во Самар. ин-та управления, 2008. - С. 258-265. - 0,45 печ. л.

19. *Казакова, А.В.* Роль информационной безопасности в деятельности предприятий [Текст] / А.В. Балановская, А.В. Казакова // Экономика России в XII веке : сб. науч. тр. V Всерос. науч.-практ. конф. "Теоретические проблемы экономической безопасности России в XXI веке" / под ред. Г.А. Барышевой, С.А. Дукарт. - Томск : Изд-во Томск. политехн. ун-та, 2008. - С. 175-178. - 0,4/0,2 печ. л.

20. *Казакова, А.В.* Анализ и оценка информационного обеспечения управленческой деятельности / А.В. Балановская, А.В. Казакова // Проблемы совершенствования организации производства и управления промышленными предприятиями [Текст]: межвуз. сб. науч. тр. / редкол.: Н.А. Чечин, С.А. Ерошевский (отв. ред.) [и др.]. Вып. 2. Ч. 1. - Самара : Изд-во Самар. гос. экон. ун-та, 2008. - С. 34-42 - 0,8/0,4 печ. л.

Подписано в печать 25.05.2011.
Формат 60×84/16. Бум. писч. бел. Печать офсетная.
Гарнитура"Times New Roman". Объем 1,2 печ. л.
Тираж 150 экз. Заказ № 212.
Отпечатано в типографии СГЭУ.
443090, Самара, ул. Советской Армии, 141.