танционное телефонное подслушивающее устройство имеет два демаскирующих свойства: во-первых, в момент подслушивания телефонный аппарат абонента отключен от телефонной линии, во-вторых, даже при положенной телефонной трубке и включенном подслушивающем устройстве напряжение питания телефонной линии составляет менее 20 Вольт, в то время как она должно составлять 60.

ВЫВОДЫ

Таким образом, для сохранения коммерческой тайны необходимо во всех служебных помещениях предприятия, в первую очередь там, где функционирует экономическая информационная система, организовать работу по выявлению и локализации возможных каналов утечки информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Савицкая Г.В. Анализ хозяйственной деятельности предприятия / Г.В. Савицкая. – М.: МГУ, 2010. – 282 с.

2. Шеремет А.Д. Управленческий учет / А.Д. Шеремет. – М.: МГУ, 2010. – 240 с.

3. Лошкарев В.Г. Организация бизнеса с нуля./В.Г. Лошкарев – М.: Изд-во РИА, 2010. – 204 с.

4. Введение в современную информатику / [М.М. Дивизинюк, Б.С. Бусыгин, Г.М. Коротенко и др.]. – Севастополь: СНУЯЭиП, 2005. – 392 с.

5. Методи керування інформаційною безпекою / [Ю.Ю. Гончаренко, М.М. Дівізінюк, В.О. Хорошко та ин.]. – Севастополь: СНУЯЕтаП, 2010. – 328 с.

6. Типизация моделей технологических решений провайдинга Интернет / [М.М. Дивизинюк, Е.В. Азаренко, С.С. Азаров и др.]. – Севастополь: СНУЯЭиП, 2005. – 112 с.

7. Проектирование систем технической защиты информации / [Ю.Ю. Гончаренко, М.М. Дивизинюк, И.Н. Павлов и др.]. – Севастополь: СНУЯЭиП, 2011. – 235 с.

8. Герасимов Б.М. Системы піддержки принятия решений / Б.М. Герасимов, М.М. Дивизинюк, И.Ю. Субач. – Севастополь: Гос. океанариум, 2004. – 318 с.

УДК 681.3

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК СОСТАВНАЯ ЧАСТЬ ДЕЯТЕЛЬНОСТИ РУКОВОДИТЕЛЯ ПРЕДПРИЯТИЯ

Ожиганова М.И.

Анализируются теоретические аспекты возможного ущерба при потере коммерческой и технологической информации, а также оптимальные затраты на предотвращение таких потерь. Рассматриваются вопросы информационной безопасности в повседневной деятельности руководителя предприятия.

Ключевые слова: *предприятие, менеджмент, информация, информационная безопасность, руководитель предприятия.*

Обеспечение безопасности информации, циркулирующей на предприятиях, а также между предприятиями и государственными учреждениями – одна из составных частей информационной безопасности государства, в частности, и национальной безопасности государства в целом [1]. Исходя из этого менеджмент информационной безопасности является актуальной научной задачей, решение которой осуществляется и компетентными государственными структурами, и руководителями предприятий различных форм собственности, выполняющими государственные заказа [2].

Известно, что конфиденциальная (коммерческая и технологическая) информация, циркулирующая на предприятии, может быть похищена или повреждена с использованием глобальных и локальных компьютерных сетей даже в случае пунктуального соблюдения нормативных правил сотрудниками – пользователями персональных ЭВМ [3,4]. Потеря информации возможна и по так называемому речевому (акустическому) каналу утечки информации [5], когда сотрудники ведут разговоры, содержащие служебную и конфиденциальную информацию, в местах, не имеющих специальных средств акустической защиты (курилках, туалетных комнатах, коридорах), а также на балконах [6] или других открытых площадках, находящихся внутри охраняемого периметра [7]. Управленческие решения, принимаемые в интересах информационной безопасности, должны носить, в соответствии с классическими управленческими теориями [8], стратегический (перспективный) и оперативный (постоянно действующий) характер.

Целью данной работы является рассмотрение вопросов менеджмента информационной безопасности как составной части деятельности руководителя предприятия. Для достижения поставленной цели необходимо решить следующие научные задачи. Во-первых, проанализировать теоретические аспекты возможного ущерба при потере коммерческой и технологической информации. Во-вторых, рассмотреть вопросы управления информационной безопасностью в повседневной деятельности руководителя.

Решение комплексной научной проблемы экономической безопасности требует привлечения специалистов различного профиля. В процессе решения используются различные теории, такие как кибернетика, теории автоматического управления, статистики, безопасности и др. Каждая из теорий имеет свою аксиоматику, методологию, математический аппарат и область приложения, отличную от области приложений других теорий. Поэтому по сути каждая из подобных теорий локальна и решает определенную часть задач без учета связи с решениями других задач. Объединение решений частных задач в общий алгоритм решения проблемы не может выполнить ни одна локальная теория. Обычно общий алгоритм решения проблемы разрабатывает высококвалифицированный специалист, объединяющий частные решения в единое системное решение на логико-экспертном уровне.

Негативным последствием логико-экспертного подхода к решению проблемы является невозможность построить математическую модель управления сложными комплексными объектами. В свою очередь, это ведет к невыполнимости оптимизации и, как следствие, к опасности больших экономических потерь. Решение комплексной научной проблемы управления безопасностью предприятия как сложного объекта может быть достигнута на основе системного подхода. Системность должна основываться на аксиоматическом положении о невозможности решения комплексной проблемы на базе одной какой-либо технологии. Системная теория должна содержать методологию управления, обеспечивающую структурный синтез локальных теорий, а также соответствующий математический аппарат, позволяющий разработать алгоритм управления по критериям эффективности и реализовать управление в виде наукоемкой технологии. При этом данная теория выполняет функцию оптимизационной стыковки локальных теорий в общий алгоритм управления безопасностью предприятия по критериям эффективности.

Для реализации системного подхода обеспечения экономической и технологической эффективности предприятия как сложной системы необходима разработка методологических положений управления безопасностью при условии минимизации затрат на безопасность. С этой целью следует учесть методологические ограничения экспертного подхода к управлению безопасностью, в том числе влияние человеческого фактора, который в технологии управления информационной безопасностью человеко-машинных систем не ограничивается оценкой качества подготовки пользователя (исполнителя, оператора и т.д.). Такое влияние следует рассматривать только как один, но далеко не самый важный из факторов проблемы технологического управления безопасностью человеко-машинной системы. В целом это проблема соотношения творческой и алгоритмической составляющих труда человека, а также эффективности их использования в технологических процессах управления. Поэтому важно рассмотреть событие утечки, потери или повреждения определенного количества информации, которая может привести к технологическому сбою. Это событие будем называть «информационным инцидентом» или просто инцидентом.

Теперь подчеркнем, что при внедрении современных технологий и организационных мер обеспечения информационной безопасности основная их направленность состоит в недопущении всех потенциально возможных инцидентов. Как правило, эти меры носят сугубо экспертный характер, в их основе отсутствует методология экономической эффективности.

Необходимо отметить, что безопасность является целью оптимального управления, а затраты определяют практические возможности обеспечения безопасности. Минимизация затрат на безопасность – необходимое условие конкурентноспособности предприятия. Взятый сам по себе тезис «максимальная безопасность» не имеет ни теоретического, ни практического смысла. С учетом конкуренции предприятие может существовать только при условии обеспечения необходимой прибыли и себестоимости продукции. В себестоимость входят и расходы на обеспечение безопасности, включая информационную безопасность. Другими словами, необходимым условием практического обеспечения безопасности является минимизация затрат на нее как один из элементов максимизации прибыли.

Принципы «предотвращения инцидентов» и «ослабления инцидентов» недостаточны для оптимального управления информационной безопасностью. Логично, что уменьшение значения риска инцидента требует увеличения затрат. В то же время нельзя обосновать оптимальное значение показателя риска инцидента и соответствующий ему минимум затрат на безопасность. Известно, что теория вероятностей изучает стохастические закономерности массы (совокупности) однотипных явлений в условиях стохастической устойчивости. Другими словами, оно означает периодическую повторяемость обстоятельств и причин появления информационного инцидента. Следовательно, принятие вероятностной модели события инцидента равносильно постулированию вероятностной закономерности, стопроцентной априорной неизбежности появления инцидента в течение определенного промежутка времени.

Результаты опросов тысяч менеджеров, которые проводятся статистическими управлениями различных стран, показывает на редкость стабильные результаты. Из каждой сотни менеджеров только один имеет достаточно времени, десятерым требуется не менее 10% времени дополнительно, сорока нужно еще не менее 25%, остальным не хватает примерно 50% дополнительного времени. Это связано, главным образом, с тем, что руководитель должен определять решаемые им задачи по приоритетам и соответствующим образом тратить на них время.

Наиболее яркой иллюстрацией этого метода управления является принцип Д.Эйзенхауэра (президент США, 1953-1961г.г.). В зависимости от степени важности и срочности задачи различаются по четырем гипотетическим оценкам. Задачи «А» выполняются без промедления, задачи «Б» выполняются в предварительно установленные сроки, задачи «В» выполняются теми, кому руководитель их поручает, а остальные задачи выбрасываются в корзину для бумаг.

Практически это может выглядеть так: руководитель при планировании своего рабочего времени, исходя из критерия значимости, срочности, важности задач, выделяет три группы. Первая «А» - наиболее важная, значимая, срочная, вторая «Б» - важные, значимые, срочные, третья «В» - менее важные, менее значимые и не срочные. Затем в соответствии с иерархией задач в своем рабочем плане выстраивает их в соответствующий ряд и определяет время и сроки выполнения. Вопросы информационной безопасности не могут быть ниже класса «Б». Это объясняется, главным образом, ограниченностью наших знаний о природе возможных (гипотетических, виртуальных) информационных инцидентов. Как было сказано выше, теоретически никогда нельзя исключить инцидент. Он возможен и в том виде, для которого отсутствуют стохастические закономерности в настоящем и в принципе их нельзя определить в будущем. Поэтому всегда нужен компромисс между технологией предупреждения информационных инцидентов, для которых известны детерминистические и стохастические закономерности, с одной стороны, с другой страхованием – технологией устранения последствий непредвиденных информационных инцидентов.

ВЫВОДЫ

Существующие теории и системный подход к информационной безопасности как составной части экономической безопасности предприятия не позволяет исключить появление информаци-

онных инцидентов, связанных с утечкой, потерей или повреждением коммерческой и технологической информации.

Вопросы информационной безопасности должны быть в числе приоритетных у руководителя предприятия. Предупреждение информационных инцидентов должно сочетаться со страхованием – технологией устранения последствий непредвиденных (гипотетических) инцидентов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Закон України «Про основи національної безпеки України» від 19.06.03. – №964 – IV/

2. Хорошко В.О. Методи керування інформаційною безпекою / [Ю.Ю. Гончаренко, М.М. Дівізінюк, В.О. Хорошко та ин.]. – Севастополь: СНУЯЕтаП, 2010. – 328 с.

3. Типизация моделей технологических решений провайдинга Интернет / [М.М. Дивизинюк, Е.В. Азаренко, С.С. Азаров и др.]. – Севастополь: СНУЯЭиП, 2005. – 112 с.

4. Андреев В.И. Проектирование систем технической защиты информации / [В.И. Андреев, Ю.Ю. Гончаренко, М.М. Дивизинюк и др.]. – Севастополь: СНУЯЭиП, 2011. – 235 с.

5. Дидковский В.С. Акустическая экспертиза каналов речевой коммуникации / В.С. Дидковский, М.В. Дидковская, А.Н. Продеус. –К.: Наукова думка, 2008. – 420 с.

6. Гончаренко Ю.Ю. Оценка дальности регистрации речевой информации с открытых площадок // Сучасний захіст інформації. – №4. – К.: ДУІКТ, 2011. – С. 72 – 76.

7. Дивизинюк М.М. О проблеме расчета дальности приема акустической информации с открытых площадок / М.М. Дивизинюк, Ю.Ю. Гончаренко, Д.Г. Гончаренко // Правове, нормативне та метрологічне забезпечення системи захісту інформації в Україні. – Вип. 1(23). – К.: НТУ «КПІ», 2012. – С. 29 – 35.

8. Герасимов Б.М. Системы поддержки принятия решений / Б.М. Герасимов, М.М. Дивизинюк, И.Ю. Субач. – Севастополь: Гос. океанариум, 2004. – 318 с.

УДК 330.101.541:534.4:563

ОСНОВНІ НАПРЯМКИ ВДОСКОНАЛЕННЯ СИСТЕМИ ВИДАТКІВ МІСЦЕВИХ БЮДЖЕТІВ

Цугунян А.М.

Описані джерела підвищення ефективності системи місцевих видатків, проблеми фінансової децентралізації, бюджетної самостійності, впровадження моніторингу результативності місцевих видатків, а також вплив середньострокового планування та системи бюджетування, орієнтованого на результат, на витрачання коштів на місцевому рівні.

Ключові слова: *місцевий бюджет, витрати, фінансова децентралізація, моніторинг, середньострокове планування, самостійність місцевого бюджету, бюджетування, орієнтоване на результат.*

Місцеві бюджети є визначальною ланкою місцевих фінансів, за рахунок яких відбувається формування, розподіл і використання грошових та інших фінансових ресурсів для забезпечення місцевими органами влади покладених на них власних та делегованих функцій і завдань. В умовах ринкових перетворень та інтеграційних процесів в Україні, виникає потреба у перегляді традиційно сформованих підходів до визначення цілей, завдань, принципів і механізму розподілу видатків місцевих бюджетів.

Місцеві бюджети здійснюють важливу роль в процесі соціально – економічного розвитку регіону, забезпечуючи фінансування основної мережі дошкільних установ, шкіл, медичних та соціальних установ. Проблемам формування видаткової частини місцевих бюджетів присвятили праці