УДК 681.3.06

А.В. ПОТИЙ[1], Д.Ю. ПИЛИПЕНКО[2]

[1]*Харьковский университет Воздушных Сил им. И. Кожедуба, Украина*
[2]*Харьковский национальный университет радиоэлектроники «ХНУРЭ», Украина*

КОНЦЕПЦИЯ СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Приведено обоснование необходимости стратегического управления информационной безопасностью, указано состояние данного направления исследований, рассмотрены основные проблемные задачи. Предложена концепция трехуровневого стратегического набора предприятия, рассмотрены особенности формирования стратегий ИБ в данной иерархической системе. Отмечена необходимость удобного и эффективного инструмента практической реализации сформированных стратегий. В качестве подобного инструмента предложено использовать модифицированную концепцию системы сбалансированных показателей Д. Нортона и Р. Каплана. Предложена стратегическая карта информационной безопасности, согласованная с картой общей деятельности предприятия.

Ключевые слова: *стратегическое управление, информационная безопасность, функциональная стратегия, система сбалансированных показателей.*

Введение

На сегодняшний день подавляющая доля информации обрабатывается и хранится в информационных системах. Зачастую важность подобной информации носит критический характер. Для организации эффективного процесса обеспечения информационной безопасности (ИБ) сегодня уже недостаточно бессистемного применения существующих методов и средств защиты информации – необходимы подходы, позволяющие осуществлять эффективное стратегическое управление ИБ. Частично элементы стратегического управления уже рассматривались иностранными производителями и поставщиками услуг в сфере безопасности информации. На необходимость введения в практику ИБ такого понятия как стратегия ИБ также указывают исследования ведущих российских специалистов [1,2]. Некоторые рекомендации относительно стратегий в качестве элемента системы информационной безопасности рассматривались в международном стандарте ISO/IEC 13335 [3]. Однако в современной литературе уделяется недостаточное внимание вопросам разработки и формирования стратегий ИБ, которая сегодня должна стать одной из функциональных стратегий предприятия. Также не сформированной является концепция стратегического управления безопасностью: основные принципы, функции, методы и формы управления.

Отсутствие стратегического управления ИБ выливается в ряд проблем: без четко сформулированной стратегии процесс обеспечения ИБ носит несистемный характер; подавляющее количество важных решений по вопросам защиты информации осуществляется интуитивно, т.е. лицо, принимающее решение (ЛПР) опирается скорее на интуицию и редко рассматривает проблему дальше рамок краткосрочного планирования. Применение стратегического подхода к управлению предприятием позволит включить аспект безопасности (в том числе и информационной) в общую систему управления предприятием, что будет способствовать согласованию бизнес-целей предприятия с целями ИБ.

1. Методологические основы

Сегодня существует несколько точек зрения относительно интерпретации такого понятия как стратегия. Одни считаю, что стратегия базируется на конкретных действиях, которые предпринимаются для достижения необходимого результата. Другие полагают, что стратегия проистекает от общего планирования, разрабатываемого руководством для того, чтобы вести организацию согласно выбранной миссии и видению. Иногда стратегию рассматривают как схему последовательности действий на определенный промежуток времени. В целом же эти и прочие определения понятия «стратегия» разделяют общую идею о том, что стратегия это продуманная совокупность норм и правил, которые позволяют вырабатывать и принимать такие решения, которые оказывают влияние на состояние системы в буду-

щем с учетом ее зависимости от динамически меняющейся внешней среды. В работе [4] под стратегией понимается генеральная программа действий, которая определяет приоритетные проблемы и ресурсы для достижения главной цели. Она формирует главные цели и основные пути их достижения таким образом, что организация (предприятие) получает единое направление движения.

Другой взгляд на понятие «стратегия» можно найти в работе [5], где под стратегией понимают общую, рассчитанную на перспективу руководящую директиву, направленную на достижение наиболее важных целей деятельности предприятия путем наиболее рационального расхода доступных ресурсов. Зачастую, аспект ИБ остается за пределами стратегии предприятия. Потребности в защите в первую очередь зависят от критичности и объема информации, которая должны быть защищена, равно как и от условий ее хранения, обработки и использования. Как правило, организации располагают ограниченными ресурсами, или имеют потребность в достижении заданного уровня защиты. С этой позиции возможны два подхода к организации защиты:

– защита должна быть организована таким образом, чтобы при заданном количестве ресурсов был достигнут максимально возможный уровень безопасности (фокус на ограниченности ресурсов);

– требуемый уровень безопасности должен обеспечиваться при минимальных затратах ресурсов (фокус на требуемой защите).

Рассматривая данный вопрос с такой позиции, стратегию ИБ можно трактовать как совокупность мер по защите информации, при которой в течение всего срока функционирования системы (предприятия, организации) уровень безопасности будет соответствовать требуемому, а необходимые для этого ресурсы использоваться наиболее рациональным образом.

2. Суть стратегического управления информационной безопасностью

Деятельность по защите информации, которая осуществляется на предприятии, во всех ее проявлениях не может сводиться только к удовлетворению краткосрочных потребностей по защите. На предприятиях с высоким уровнем информатизации деловой активности и интеграции информационных технологий в производственные процессы, осознается необходимость управления ИБ с учетом перспективы и долгосрочных целей, необходимость согласования задач ИБ с общими целями деятельности предприятия. В данном контексте стратегическое управление ИБ может служить эффективным инструментом перспективного управления деятельностью по защите информации, которая подчинена процессу реализации стратегических целей предприятия в условиях динамически меняющейся среды безопасности. Актуальность разработки стратегии ИБ определяется такими факторами:

– интенсивность изменения внутреннего и внешнего состояния среды безопасности предприятия;

– высокая динамика развития и применения современных информационных технологий в деловой среде предприятия;

– возрастающая интенсивность отношений между субъектами деятельности предприятия;

– рост ценности нематериальных активов предприятия.

В таких условиях уже неприемлемо полагаться только лишь на накопленный ранее опыт и методы традиционного управления. Отсутствие разработанной стратегии, способной учитывать возможные изменения среды безопасности, может привести к тому, что решения, которые принимаются на различных уровнях иерархии предприятия, будут приводить к системным противоречиям, что в свою очередь приведет к общему падению эффективности защиты информации и прочих видов информационной деятельности. Одновременно с развитием технологий должно происходить и совершенствование деятельности по защите информации, однако данный процесс должен быть не стихийным, а носить прогнозируемый характер и подкрепляться четко сформулированной стратегией.

3. Стратегический набор предприятия в контексте обеспечения ИБ

Опираясь на общие подходы классификации стратегий, которые приняты в стратегическом менеджменте, предлагается следующая иерархия стратегий предприятия в контексте обеспечения ИБ. Предлагается декомпозировать стратегический набор на три уровня (рис. 1).

Первый уровень описывает общую корпоративную стратегию предприятия и его функциональные стратегии. Корпоративная стратегия определяет перспективы развития предприятия в целом и способствует достижению предприятием своего видения и выполнению миссии. Дальнейшее развитие корпоративная стратегия получает в виде функциональных стратегий предприятия, которые зависят от направления деятельности предприятия.

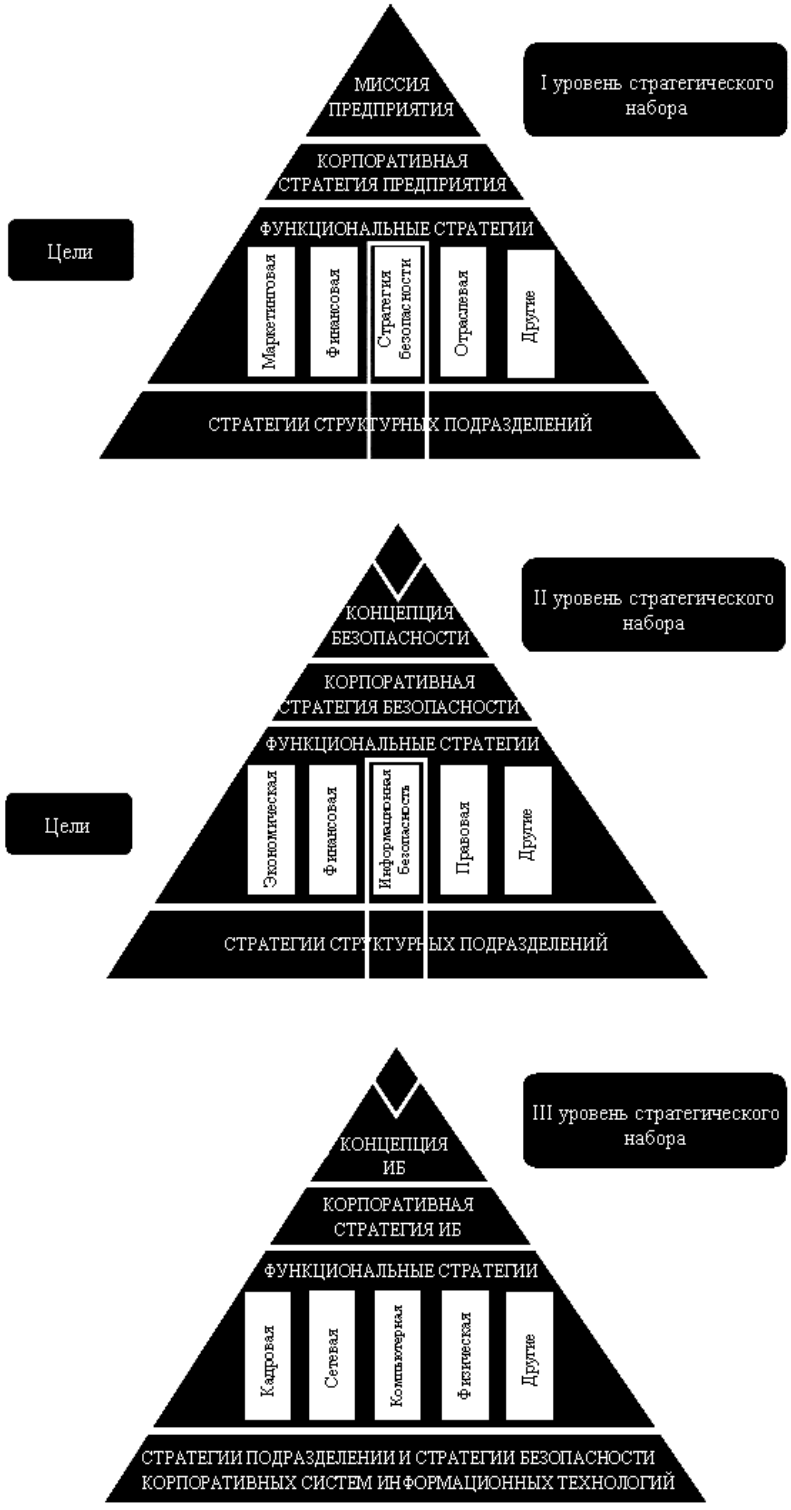

Рис. 1. Трехуровневая модель стратегического управления предприятием

Непосредственно на данном уровне формируется общая концепция безопасности предприятия. Функциональные стратегии одного уровня обладают горизонтальными связями и согласовываются между собой на уровне целей. Каждая функциональная стратегия первого уровня более детально проецируется на второй уровень стратегического набора.

На втором уровне формируется корпоративная стратегия безопасности, определяющая направления развития деятельности по защите интересов пред-

приятия в различных сферах деятельности. Корпоративная стратегия безопасности описывает, каким образом следует управлять и координировать усилия по различным направлениям аспекта безопасности. Она развивается функциональными стратегиями второго уровня, которые в свою очередь охватывают главные сферы стратегического управления предприятием в целом. Целесообразно выделять такие функциональные стратегии: стратегия финансовой безопасности, стратегия экономической безопасности, стратегия физической безопасности, стратегия ИБ.

Более детально стратегия ИБ рассматривается на третьем уровне стратегического набора. На этом уровне, основываясь на концепции информационной безопасности, формируется корпоративная стратегия ИБ, которая в свою очередь получает развитие в функциональных стратегиях третьего уровня. Функциональные стратегии третьего и последующих уровней рассматриваются как операционные стратегии. Среди основных направлений деятельности по защите информации целесообразно выделить кадровую безопасность, сетевую безопасность, физическую безопасность и другие. Именно по этим направлениям рекомендуется развивать операционные стратегии деятельности.

Рассмотренная выше стратегия ИБ является разновидностью функциональных стратегий предприятия. Разработка стратегии ИБ является важной функцией руководства в сфере безопасности и должна проводиться под непосредственным контролем высшего руководства предприятия. Стратегия ИБ охватывает все основные направления развития деятельности по защите информации и существенно влияет на информационные отношения предприятия. Только комплексный подход, учитывающий возможности предприятия в различных направлениях деятельности по защите информации позволяет в полной мере реализовать возможности стабильного роста уровня защищенности в долгосрочной перспективе. Разработка стратегии ИБ подразумевает выбор наиболее эффективных направлений для достижения поставленных целей безопасности. Подобный выбор становится возможным посредством поиска и оценки альтернативных вариантов возможных стратегических решений по вопросам безопасности и их соответствующим отбором на основе выбранных критериев.

Выработка корпоративных стратегий способна решить проблему согласования бизнес-целей предприятия и целей безопасности, сделать процесс организации защиты информации более системным и ввести задачи из долгосрочной перспективы в зону внимания высшего руководства. Однако, для полного раскрытия потенциала стратегического управления также необходим механизм, способный качественно или количественно оценить эффективность достижения установленных стратегических целей. Здесь наиболее перспективным подходом для оценки эффективности стратегий предприятия является методика Д. Нортона и Р. Каплана – сбалансированная система показателей (ССП) [6]. Основополагающим принципом данной методики является идея о том, что управлять можно только тем, что можно измерить. Для оценки эффективности авторы выделили четыре главных аспекта: финансы, клиенты, бизнес-процессы и обучение и рост. По каждому из данных аспектов предлагается определить ключевые показатели эффективности (Key Performance Indicator). Сами авторы делают акцент на нефинансовых показателях эффективности, что позволяет всестороннее оценить деятельность предприятия.

Несмотря на определенные трудности, касающиеся внедрения данного подхода на практике, он представляется весьма эффективным инструментом, способным адекватно оценивать эффективность реализации стратегии компании. Важной особенностью данного подхода является его гибкость – исходную концепцию из четырех аспектов можно без негативных последствий расширять или сужать, учитывая потребности и специфику каждого конкретного предприятия.

Таким образом, сочетая предложенный трехуровневый стратегический набор и сбалансированную систему показателей, можно добиться не только возможности формализовать стратегии развития предприятия, но и получить удобный инструмент для оценки эффективности реализации этих стратегий.

В первом приближении подобная система будет состоять из ядра, внутреннего и внешнего колец (рис. 2). В качестве ядра системы будем использовать концепцию ИБ, находящуюся на третьем уровне стратегического набора предприятия. Внутренне кольцо представляет собой показатели, сгруппированные по следующим направлениям: финансово-экономический аспект обеспечения информационной безопасности, процессы защиты информации, технологии защиты информации, безопасность бизнеса, развитие персонала. Направления деятельности предприятия, включенные во внутреннее кольцо, предназначены непосредственно для структурного подразделения, обеспечивающего безопасность информации предприятия. Наборы показателей для других структурных подразделений будут сгруппированы по другим направлениям, учитывающим специфику каждого конкретного подразделения. Внешнее кольцо состоит также из пяти групп показателей, охватывающих следующие аспекты деятельности предприятия: финансы, внутренние про-

цессы, информационные технологии, клиенты, персонал. Аспекты деятельности предприятия, формирующие внешнее кольцо являются общими для всех структурных подразделений предприятия.

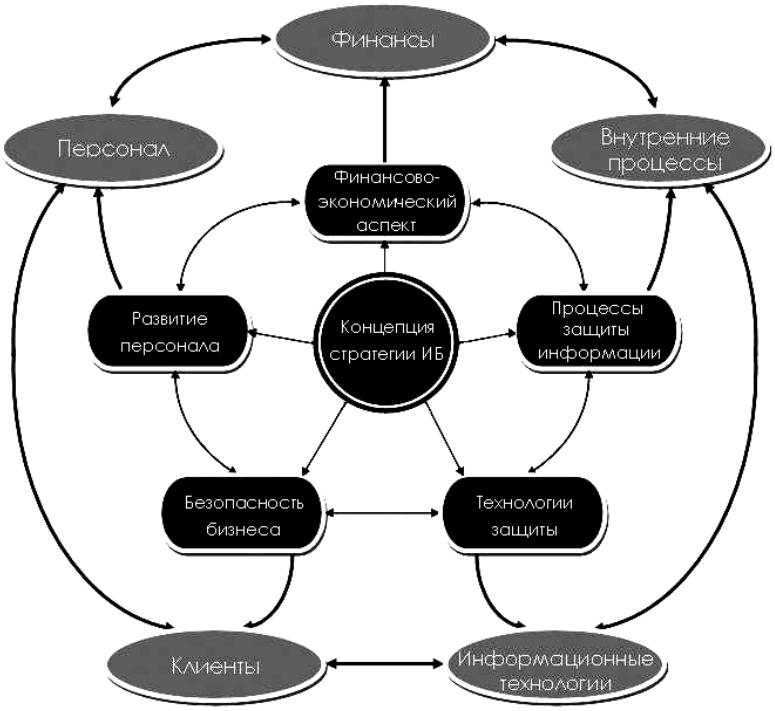

Рис. 2. Связь стратегической карты информационной безопасности с общей стратегической картой предприятия

Особенностью подобной системы показателей является ее способность охватить наиболее важные аспекты деятельности предприятия, таким образом, позволяя получить адекватное представление о деятельности по защите информации с различных сторон. Для каждого из аспектов деятельности необходимо выбрать ключевые показатели эффективности, с помощью которых будет производиться оценка эффективности выбранной стратегии и проводиться контроль достижения поставленных целей.

Рассмотрим наборы показателей внутреннего кольца более подробно. *Финансово-экономические показатели*: являются одной из групп финансовых показателей предприятия и оказывают влияние на финансовое благополучие предприятия. *Показатели процессов защиты информации*: процессы ЗИ представляют собой часть внутренних процессов предприятия, играют роль вспомогательных процессов для основных (бизнес) процессов предприятия. *Показатели технологий защиты*: технологии защиты является интегрированной составной частью информационных технологий предприятия. Средства защиты информации являются элементом, повышающим уровень доверия к информационным технологиями и формирующим уверенность в поддержке ИТС основных бизнес-процессов. *Показатели безопасности бизнеса*: данный аспект ориентирован в первую очередь на заинтересованных лиц. Показатели данной группы формируют положительный, основный на доверии, имидж предприятия у клиентов. *Показатели развития персонала*: является неотъемлемой частью формирования корпоративной культуры предприятия. Надежность, компетентность, лояльность и мотивированность персонала являются залогом кадровой безопасности.

Очевидно, что разработка стратегии деятельности предприятия является полезным шагом, однако без инструмента, способного оценить эффективность сформулированной стратегии, стратегическое управление в чистом виде не способно полностью раскрыть свой потенциал. В свою очередь, система сбалансированных показателей позволяет реализовать общую стратегию на любых уровнях иерархии предприятия. Описывая стратегические цели через ключевые показатели эффективности, предприятие получает возможность формализовать разработанный стратегический набор и в дальнейшем производить необходимые корректировки.

Заключение

Стратегия ИБ есть механизм реализации долгосрочных целей безопасности, равно как и общих целей развития предприятия в целом. Стратегия ИБ позволяет оценить возможности предприятия относительно защиты информации, обеспечить максимальное использование потенциала безопасности. Наличие подобной стратегии обеспечивает взаимосвязь между стратегическим и операционным

управлением деятельностью по защите информации. В информационной сфере крупных предприятий (состоящих из относительно самостоятельных подразделений) наблюдается эффект корпоратизации, т.е. совместного владения, распоряжения и использования информации. В таких условиях особенно важно иметь единую стратегию ИБ.

Предлагаемый стратегический набор обуславливает стратегическую гибкость предприятия. Количество стратегий может варьироваться в зависимости от структуры и размеров предприятия.

Для адекватного воплощения разработанных стратегий необходим инструмент, позволяющий оценивать эффективность реализации стратегического набора предприятия. В качестве такого инструмента представляется целесообразным использовать систему сбалансированных показателей Д. Нортона и Р. Каплана. Данная система прошла успешную проверку временем и зарекомендовала себя как мощный инструмент оценки различных сторон деятельности предприятий при помощи финансовых и нефинансовых наборов показателей. Гибкость данной системы позволяет модифицировать ее для оценки деятельности по защите информации предприятия.

Литература

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: Горячая линия – Телеком, 2004. – 280 с.

2. Герасименко В.А. Основы защиты информации / В.А. Герасименко, А.А. Малюк. – М.: МИФИ, 1997.

3. ДСТУ ISO/IEC TR 13335:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частини 1: Концепції та моделі безпеки інформаційних технологій. Частина 2: Керування та планування безпеки інформаційних технологій. Частина 3: Методи керування безпекою інформаційних технологій.

4. Анисимов О.С. Стратегии и стратегическое мышление (акмеологическая версия) / О.С. Анисимов – М.: Агро-Вестник, 1999.

5. Керцер Г. Стратегическое планирование для управления проектами с использованием модели зрелости / Г. Керцер. – М.: Компания АйТи, ДМКПресс, 2003. – 320 с.

6. Kaplan R.S. The balanced scorecard: measures that drive performance / R.S. Kaplan, D.P. Norton // Harvard Business Review, Jan-Feb 1992. – pp. 71-80.

Поступила в редакцию 1.03.2010

Рецензент: д-р технических наук, профессор И.Д. Горбенко, Харьковский национальный университет радиоэлектроники «ХНУРЭ», Харьков.

КОНЦЕПЦІЯ СТРАТЕГІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

О.В. Потій, Д.Ю. Пилипенко

Наведено обґрунтування необхідності стратегічного управління інформаційною безпекою, вказано стан даного напряму досліджень, розглянуто основні проблемні задачі. Запропонована концепція трирівневого стратегічного набору підприємства, розглянуто особливості формування стратегій ІБ в рамках даної ієрархічної системи. Відзначено необхідність зручного та ефективного інструменту практичної реалізації сформованих стратегій. У якості такого інструмента запропоновано використовувати модифіковану концепцію системи збалансованих показників Д. Нортона та Р. Каплана. Запропонована стратегічна карта інформаційної безпеки, узгоджена з картою загальної діяльності підприємства.

Ключові слова: стратегічне управління, інформаційна безпека, функціональна стратегія, система збалансованих показників.

THE CONCEPT OF INFORMATION SECURITY STRATEGIC MANAGEMENT

A.V. Potiy, D.J. Pilipenko

The substantiation of strategic management of information security necessity is given, the condition of this domain of research is described, and the major problems are considered. The concept of three-tier strategic set is proposed, the features of information security strategy design in the scope of this hierarchical structure are described. The necessity for convenient and effective tool of practical I mplementation of designed strategies is marked. The modified concept of Kaplan & Norton's Balanced Scorecard is proposed in the capacity of such tool. The information security strategic map aligned with general organization's activity strategic map is also proposed.

Key words: strategic management, information security, functional strategy, Balanced Scorecard.

Потий Александр Владимирович – д-р техн. наук, профессор, начальник кафедры радиоэлектронных систем пунктов управления Воздушных Сил Харьковского университета Воздушных Сил им. И. Кожедуба, Харьков, Украина, e-mail: potav@ua.fm.

Пилипенко Дмитрий Юрьевич – аспирант кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники «ХНУРЭ», Харьков, Украина.