ISSN 2311-8709 (Online)
ISSN 2071-4688 (Print)

Стоимость бизнеса

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИННОВАЦИОННЫХ РАЗРАБОТОК В УСЛОВИЯХ КОНКУРЕНТНОГО ПРОТИВОСТОЯНИЯ

Алексей Петрович ЛАПСАРЬ[a,•], Сергей Алексеевич ЛАПСАРЬ[b]

[a] кандидат технических наук, доцент, доцент кафедры информационных технологий и защиты информации, Ростовский государственный экономический университет, Ростов-на-Дону, Российская Федерация
lapsar1958@mail.ru

[b] консультант Фонда перспективных исследований, Москва, Российская Федерация
greyser1982@yandex.ru

• Ответственный автор

История статьи:
Принята 17.11.2016
Принята в доработанном виде 01.12.2016
Одобрена 15.12.2016
Доступна онлайн 16.01.2017

УДК 004.056.5:659.441(045)
JEL: C18, C44, D81

Ключевые слова:
инновационные разработки, критическая информация, конкуренция, виртуальный образ

Аннотация

Предмет. Поскольку в настоящее время вопросы влияния конкурентов на процессы продвижения высокотехнологичной продукции исследованы недостаточно полно, синтез методов обеспечения безопасности инновационных разработок в условиях жесткого конкурентного противостояния является актуальным.

Цели. Синтез метода повышения безопасности инновационных разработок в условиях жесткой конкуренции на базе оценки возможных мер противодействия со стороны конкурентов и защиты критической информации о разрабатываемой продукции.

Методология. С использованием аппарата математической статистики, теории эффективности и экспертных методов проанализированы возможности парирования мер противодействия со стороны конкурирующих структур по дискредитации инновационной продукции и предложен метод защиты, позволяющий повысить безопасность и эффективность долгосрочных инвестиций в ее разработку.

Результаты. Синтезирован метод обеспечения безопасности инновационных разработок и последовательность его реализации. Метод включает в себя: прогнозирование возможной реакции конкурентов на информацию о инновационных разработках и оценку последствий от реализации мер противодействия; создание способов защиты информации о проводимых разработках; формирование вариантов виртуального образа разрабатываемой инновационной продукции; оценку правдоподобия предлагаемого образа; выбор оптимального варианта. Предлагаемый метод является экономичным, его использование не требует высокой квалификации или специальной подготовки.

Выводы. Оригинальный метод повышения безопасности инновационных разработок применим в условиях жесткой или недобросовестной конкуренции. Он может развиваться в направлении оценки уровня осведомленности конкурентов о текущем состоянии разработок, методики выбора источников доведения требуемой информации до конкурирующих организаций, а также синтеза формализованного математического аппарата назначения количественных показателей характеристик ложного объекта и их допустимых отклонений.

Введение

Процессы глобализации наряду с позитивными факторами развития мировой экономики сопровождаются повышением конкуренции в различных секторах. При этом центр конкурентного противостояния перемещается в область инновационной высокотехнологичной продукции (ИВП)[1]. Крупные иностранные национальные и транснациональные корпорации стремятся противодействовать продвижению новой российской высокотехнологичной, зачастую уникальной, продукции [1]. В настоящее время к конкурентоспособной российской продукции можно отнести современные образцы вооружения и военной техники, аэрокосмические системы и комплексы, энергетическое оборудование и т.д. Разработка

[1] *Гольдштейн Г.Я.* Стратегический инновационный менеджмент. Таганрог: ТРТУ, 2004. 267 с.

и производство названной продукции требуют значительных инвестиций с продолжительным временем окупаемости[2].

При этом разработчики ИВП решают ряд взаимосвязанных задач[3]: создание соответствующего научно-технического и технологического задела; разработка инновационной продукции (проведение научно-исследовательских и опытно-конструкторских работ, проектирование, изготовление опытных образцов, испытания, опытное производство); производство разработанной продукции в целях удовлетворения потребностей заказчиков на внутреннем рынке и организации экспорта.

В случае конкурирования на рынке высокотехнологичной уникальной продукции противодействие со стороны возможных конкурентов происходит еще на этапе ее проектирования[4]. Противодействие российским разработкам может привести к опережающему выводу на мировые рынки аналогичной или разработанной конкурентами более совершенной продукции. Кроме того, конкурирующие структуры могут использовать нерыночные методы, например, дискредитацию разрабатываемой продукции, закрытие отдельных сегментов рынка сбыта, стимулирование введения различных санкций и ограничений: на современные технологии, на сырье и комплектующие элементы, а также лоббирование своих интересов как среди поставщиков, так и среди возможных потребителей [2].

Для снижения интенсивности противодействия со стороны конкурентов российские разработчики ИВП вынуждены принимать меры по защите своих интересов [3]. При невозможности оказания прямого влияния на конкурентов целесообразным является использование методов, основанных на защите собственных разработок от целенаправленного воздействия конкурирующих структур. В этих условиях основным методом противодействия является защита критически важной для разработчика информации. К ней можно отнести информацию о направленности проводимых разработок, о полученных и планируемых результатах, о возможных сроках завершения разработок и начала массового производства, другую конфиденциальную информацию. В настоящее время вопросы снижения влияния конкурентов на процесс разработки ИВП исследованы недостаточно полно, поэтому синтез методов обеспечения безопасности в данной сфере представляется актуальным в условиях усилившегося конкурентного противостояния.

Так как при современном уровне развития информационных технологий сам факт проведения разработок ИВП скрыть невозможно, разработчик может организовать дезинформацию конкурентов, чтобы либо убедить их в низкой конкурентоспособности своей продукции, либо исказить планируемые сроки вывода продукции на рынок[5] [4–10]. Для достижения поставленных целей разработчик должен убедить конкурента принять отличный от реального виртуальный образ (ВО) разрабатываемой ИВП. То есть довести до конкурента (навязать ему) искаженное в соответствии с выбранной стратегией защиты критической информации представление о важнейших характеристиках разрабатываемой продукции: ее характеристиках, показателях качества, потребительских свойствах и сроках выхода на рынок.

Считается [3, 11], что в каждый момент времени конкуренты имеют некоторое представление о разрабатываемой ИВП, ее свойствах и характеристиках, а также принимают меры по уточнению значений основных ее характеристик, то есть ведут промышленную разведку. На основе полученной информации конкуренты могут реализовать меры противодействия,

[2] *Андрейчиков А.В., Андрейчикова О.Н.* Стратегический менеджмент в инновационных организациях. М.: ИНФРА-М, 2013. 396 с.

[3] *Баринов В.А., Харченко В.Л.* Стратегический менеджмент. М.: Инфра-М, 2009. 238 с.

[4] *Галкин В.В.* Промышленный шпионаж в системе недобросовестной конкуренции. URL: http:/www.vadim-galkin.ru/business-basics/unfair-competition/spying/

[5] *Минаев Г.А.* Безопасность организации. М.: Логос, 2008. 368 с.

направленные на замедление разработок, а также на дискредитацию разрабатываемой ИВП [2].

При доведении до конкурентов искаженного представления о разрабатываемой продукции в зависимости от этапа разработки ИВП возможно использование ложной информации, формируемой с учетом следующих очевидных положений. На этапах исследований, проектирования и выпуска опытного образца продукции возможно доведение до конкурентов заведомо завышенных по сравнению с разрабатываемой продукцией характеристик виртуального образа ИВП. В этом случае попытка конкурентов создать продукцию с лучшими характеристиками, чем у виртуального образа разрабатываемой продукции, приведет к неэффективному использованию различного вида ресурсов и потере времени из-за направления исследований по ложному руслу.

На этапе испытаний и в дальнейшем при изготовлении первых образцов инновационной продукции подтвердить заявленные завышенные характеристики практически невозможно. В этом случае целесообразно доводить до конкурентов заниженные по сравнению с разрабатываемой ИВП свойства и характеристики виртуального образца. Конкуренты, считая, что разрабатываемая ими продукция превосходит аналог, снижают интенсивность реализации мер противодействия. При этом до момента появления разрабатываемой продукции на рынке должно выполняться очевидное условие: эффективность разработанной конкурентами продукции при имеющейся у них информации о характеристиках виртуального образца ИВП должна превышать его эффективность.

Вместе с тем по мере проработки реального облика разрабатываемой продукции могут изменяться ее реальные характеристики, в том числе и с учетом противодействия со стороны конкурентов. Для обеспечения конкурентоспособности и поддержания требуемого уровня защищенности продукции требуется корректировка виртуального образца разрабатываемой ИВП с учетом реальных (реализуемых) и прогнозируемых мер противодействия со стороны конкурентов[6] [3].

Задача настоящего исследования – синтезировать метод повышения безопасности инновационных разработок в условиях жесткой конкуренции на базе оценки возможных мер противодействия со стороны конкурентов и защиты критической информации о разрабатываемой продукции.

Последовательность реализации метода обеспечения безопасности инновационных разработок

Считаем, что в течение некоторого продолжительного периода времени разработчик выполняет работы по созданию ИВП. В техническом задании на нее определены основные свойства, показатели качества, а также технические, эксплуатационные и другие характеристики $Z(H)$: $H(t)=\left| h_i(t) \right|, i=\overline{1,N}$, определяющие эффективность $Э^{ИВП}$ (Т) разрабатываемой ИВП на момент появления ее на мировых рынках. Конкуренты в момент времени t_0 имеют некоторое представление о разрабатываемой ИВП, в результате чего ими сформирован возможный образ продукции $Z_К(H_0)$: $H_0(t_0)=\left| h_j(t) \right|, j=\overline{1,M}, M \le N$, который в той или иной мере соответствует реальному. Информация конкурентов о *j*-й характеристике разрабатываемой ИВП может быть представлена количественными или качественными, единичными, множественными или интервальными значениями, которые изменяются (уточняются) по мере накопления информации о продукции[7].

В целях исключения или существенного снижения возможного ущерба от действий конкурентов осуществляется защита разрабатываемой ИВП. Для реализации соответствующих мероприятий синтезируется виртуальный образ ИВП, который должен обеспечить требуемую эффективность

[6] *Мишин В.М.* Управление качеством. М.: ЮНИТИ-ДАНА, 2005. 463 с.

[7] Там же.

разрабатываемой продукции в течение заданного времени, как правило, совпадающего с моментом появления продукции на мировых рынках [12, 13]. Таким образом, необходимо определить набор характеристик виртуального образа разрабатываемой ИВП $Z(H) \rightarrow L(H)$, который после доведения его до конкурентов обеспечит принятие ими образа ИВП $L(H) \rightarrow Z_K(H)$, способного привести к минимальному ущербу от снижения эффективности разрабатываемой ИВП в результате мер противодействия:

$$Э^{Z0}(H) - Э^{L}(H) \rightarrow min,$$

где $Э^{Z0}(H)$ – эффективность ИВП при условии полного отсутствия у конкурентов информации о разрабатываемой ИВП и, следовательно, при отсутствии мер противодействия с их стороны;

$Э^{L}(H)$ – эффективность ИВП при условии наличия у конкурентов информации о разрабатываемой ИВП в виде ее виртуального образа и выбранных на его основе мерах противодействия.

Задача разработчика состоит в обеспечении выполнения условия:

$$Э^{ИВП}(T, H, H_0, L) > Э^{K}(T, H, H_0, L),$$

где $Э^{K}(T, H, H_0, L)$ – эффективность создаваемой конкурентами аналогичной продукции в течение заданного времени, определяемого скоростью насыщения рынка разрабатываемой ИВП.

Таким образом, итогом мероприятий по доведению до конкурентов виртуального образа ИВП является изменение их представления о разрабатываемой продукции в соответствии с замыслом защиты:

$$Z_K(H_0) \rightarrow Z_K(H_1) = L(H) \pm \Delta L(H)$$

где $\Delta L(H)$ – погрешность доведения нужной информации до конкурентов.

Реакция конкурентов заключается в формировании набора мер противодействия (ускорении и изменении плана проведения собственных разработок, дискредитирующих и санкционных мероприятий и др.) при условии принятия ими предлагаемого виртуального образа ИВП в качестве реального. Виртуальный образ ИВП синтезируется с учетом правдоподобия, которое характеризуется его достоверностью и является обязательным условием достижения поставленных целей по защите информации о разрабатываемой продукции [3, 12].

Метод повышения безопасности инновационных разработок в условиях глобальной конкуренции должен обеспечивать заданный уровень правдоподобия виртуального образа ИВП и учитывать возможную реакцию конкурентов на этот образ.

Поставленную задачу будем решать в следующей последовательности: прогнозирование возможной реакции конкурентов на информацию о разработках ИВП и оценка последствий от реализации мер противодействия; создание способов защиты информации о проводимых разработках; формирование некоторого набора возможных вариантов виртуального образа разрабатываемой ИВП; оценка правдоподобия предлагаемого виртуального образа; выбор оптимального (предпочтительного) варианта.

Прогнозирование возможной реакции конкурентов на разработку ИВП и оценка последствий от реализации мер противодействия

Реакция конкурентов во многом обусловлена наличием у них информации о проводимых разработках ИВП. Под реакцией конкурентов будем понимать меры противодействия, направленные на снижение эффективности разрабатываемой ИВП. Названные меры могут быть пассивными, связанными с изменением стратегии собственных разработок, либо активными, направленными против организации-разработчика [2, 13, 14].

Как отмечалось ранее, оптимальным результатом реализации мероприятий по защите критической информации является сохранение эффективности разрабатываемой ИВП на время до выхода ее на мировые рынки. Кроме того, в целях ограничения

ресурсов, непосредственно не связанных с разработкой ИВП, и повышения ее рентабельности, необходимо минимизировать затраты на доведение ее виртуального образа до конкурентов. Таким образом, синтезированный виртуальный образ ИВП, должен обеспечить минимальное снижение эффективности разрабатываемой продукции. Первоначальная оценка возможного снижения эффективности определяется при формировании главной идеи защиты и является основой при оценке ущерба от действий конкурентов применительно к вариантам виртуального облика[8]. Возможный ущерб, который может быть нанесен разработчику, определяется назначением разрабатываемой ИВП и потребностями рынка, инновационностью использованных технических решений, показателями качества, техническими и другими характеристиками продукции, степенью превышения эффективности разрабатываемой ИВП над имеющимися аналогами, а также осведомленностью конкурентов о реальных свойствах и характеристиках разрабатываемой продукции.

Ущерб в результате действий конкурентов при имеющейся у них информации об ИВП $Z_K(H)$ определяется как сумма

$$U_K(Z_K)=\sum_{i=1}^{n} U_{Ki}(Z_K),$$

где $U_{Ki}(Z_K)$ – ущерб, наносимый конкурентами разработчику в различных областях: технической, технологической, экономической и других.

Поскольку конкуренты реализуют меры противодействия в соответствии с собственными интересами, идущими вразрез с интересами разработчика, возникает классическая конфликтная ситуация. Конкуренты, имея некоторое начальное представление $Z_K(H_0)$ об объекте, осуществляют меры противодействия в отношении разрабатываемой продукции. При этом данные действия могут привести к нанесению ущерба организации-разработчику в размере $U_K(Z_K)$. Получение конкурентами дополнительных сведений о разрабатываемой ИВП изменяет объем имеющейся у них информации и приводит к изменению существующего образа разрабатываемой продукции $Z_K(H)$. При изменении образа конкуренты могут принимать решения об изменении стратегии своего поведения как в области собственных разработок, так и в области воздействия на разработчика ИВП. В этом случае ущерб, который может быть нанесен организации, также изменится: $U_K(Z_{K0}) \rightarrow U_K(Z_K)$. Следовательно, для определения изменения возможного ущерба при доведении до конкурентов некоторого виртуального образа ИВП необходимо спрогнозировать возможные изменения в действиях конкурентов и оценить последствия данных изменений.

В настоящее время слабо формализованные задачи, к которым следует отнести и оценку возможной реакции конкурентов на полученную информацию о разрабатываемой ИВП, решаются преимущественно методами экспертной оценки[9]. Для устранения недостатков таких методов, связанных в основном с квалификацией экспертов, предлагается следующий формальный подход к решению задачи прогнозирования реакции конкурентов на разработку ИВП.

Прогнозирование возможной реакции (мер противодействия) конкурентов на имеющуюся информацию о разрабатываемой ИВП основано на критерии опасности данной продукции для конкурентов [15]. Критерий опасности характеризуется превышением эффективности разрабатываемой ИВП над эффективностью уже существующей аналогичной продукции, а также находящейся в разработке продукции конкурентов на некоторую пороговую величину:

$$\Theta^{ИВП}(T, H, H_0, L) - \Theta^{K}(T, H, H_0, L) > \\ > \Delta\Theta_{\min}. \quad (1)$$

Очевидно, что решение о необходимости реализации мер противодействия принимается

[8] *Аполлонский С.М., Куклев Ю.В.* Надежность и эффективность электрических аппаратов. М.: Лань, 2011. 448 с.

[9] *Шикин Е.В., Шикина Г.Е.* Исследование операций. М.: Проспект, 2006. 280 с.; *Светозаров В.В.* Основы статистической обработки результатов измерений. М.: МИФИ, 2005. 40 с.

конкурентами в случае наличия у них такой информации, которая позволяет сделать вывод о выполнении указанного условия (1).

Исходными данными для прогнозирования реакции конкурентов на навязываемый облик объекта является множество возможных мер противодействия $Q(t)=\{Q_i(t)\}, i=\overline{1,L}$ и характеристика каждой из них, позволяющие определить эффективность, а также требуемые сведения о разрабатываемой ИВП и предполагаемое время их реализации.

Для каждой ИВП возможна реализация конкурентами мер противодействия, выбранных из множества $Q(t)$ допустимых. Решение об их реализации применительно к разрабатываемой продукции принимается на базе следующих показателей: $Э^K(Z, Q_i)$ – эффективность i-й контрмеры применительно к объекту, имеющему образ $Z(H)$; $T^K(Q_i)$ – срок реализации меры противодействия; $In^K(Q_i)$ – множество характеристик объекта, знание которых необходимо конкурентам для реализации i-й меры противодействия; $C^K(Q_i)$ – стоимость i-й меры противодействия.

Решение задачи предполагаемого выбора мер противодействия может быть решено экспертными методами, которые достаточно тривиальны и в работе не рассматриваются. Проанализируем возможный формальный алгоритм выбора мер противодействия конкурентами при условии соблюдения ограничений $C^K(Q_i)<C^K_{доп.}(Q_i)$.

Для каждого набора из множества возможных мер противодействия проводится анализ необходимых данных о характеристиках объекта, множество данных характеристик $In^{контр.}(Q_i)$ сравнивается с множеством характеристик виртуального образа продукции $H_L(t)$. Из множества $Q(t)$ возможных мер противодействия выбираются те, для которых выполняется условие включения множества требуемых характеристик в множество характеристик облика $In^{контр.}(Q_i)\subset Z_L(H), j=\overline{1,L_1}$. Для набора возможных мер противодействия $Q_1=\{Q_j\}\subset Q$, удовлетворяющих данному условию, проводится оценка временных параметров реализации данных мер:

$$T^{МП}(Q_i)\le t_{окон.}, \qquad (2)$$

где $t_{окон.}$ – предполагаемое время разработки ИВП.

Из множества мер противодействия, удовлетворяющих названному условию (2) $Q_1=\{Q_j\}\subset Q$, проводится комплектация вариантов выбранных мер, обеспечивающих требуемое с точки зрения конкурентов снижение эффективности ИВП.

$$V_j=\{Q_{s1j}, Q_{s2j}, \dots, Q_{Sj}\}, \ j=\overline{1,J},$$

где V_j – вариант неизбыточного набора мер противодействия, при реализации которых обеспечивается снижение эффективности ИВП $Z(H)$ ниже допустимого уровня, то есть удовлетворяющий условиям (1) и (2):

$$Э^{МП}(Z, Q_i)>Э^{об.}(Z)-Э^{об.}_{доп.}(Z, Q_i),$$

где $Э^{МП}(Z, Q_i)=Э^{МП}(Z, Q_{s1j}, Q_{s2j}, \dots, Q_{Sj})=$
$=F^W(Э^{МП}(Z, Q_{s1j}), Э^{МП}(Z, Q_{s2j}), \dots)$;
$s1j$, $s2j$, …, Sj – номера мер противодействия, вошедших в j-ую группу; $F^W(Э^{МП}(Z, Q_{s1j}), Э^{МП}(Z, Q_{s2j}), \dots)$ – функционал, определяющий эффективность набора мер противодействия.

Таким образом, реакцией конкурентов на доведенный до них виртуальный образ ИВП объекта может быть реализация одного из вариантов возможных мер. Наиболее вероятным является вариант, обеспечивающий минимальные сроки реализации названных мер:

$$V(Z)=\min_j\left(\max_{Sj} T^{МП}(Z, Q_{Sj})\right).$$

Результатом применения конкурентами алгоритма прогнозирования является множество групп наиболее возможных мер для каждого достоверного варианта виртуального образа ИВП соответственно. Последствия мер противодействия оцениваются в виде возможного ущерба разработчику. Его оценка

проводится на основе известных методов оценки эффективности[10] [12].

Для разрабатываемой продукции $Z(H)$ возможной реакцией конкурентов является реализация некоторого варианта мер противодействия $V_j = \left| Q_{s1}, Q_{s2}, \ldots, Q_S \right|$. В связи с их реализацией возможно нанесение ущерба в результате снижения эффективности защищаемой ИВП в размере:

$$\Theta^{ущ.}(V(Z), Z_L) = \Theta^K(Z_L, Q_{s1}, Q_{s2}, \ldots, Q_S) = \\ = F^W(\Theta^K(Z_L, Q_{s1}), \Theta^K(Z_L, Q_{s1j}), \ldots).$$

Данный показатель характеризует возможность использования виртуального образа $L(H)$ для защиты реальной продукции $Z(H)$. Применительно к решаемой задаче итогом исследования являются оценки возможного ущерба при доведении до конкурентов допустимых вариантов виртуального образа ИВП. Выбор предпочтительного варианта виртуального образа ИВП основан на критерии минимизации снижения эффективности ИВП при его доведении до конкурентов: $\Delta \Theta^Z(Z_L, t_1) \rightarrow \min$. Предпочтительный облик объекта прикрытия формируется как совокупность его характеристик: $L(H) = \left| h_{L1}, h_{L2}, \ldots, h_{LN} \right|$.

Если спрогнозировать реакцию конкурентов на полученную информацию о виртуальном образе ложного объекта прикрытия, можно перейти непосредственно к разработке оптимального варианта виртуального образа разрабатываемой ИВП, выбрать наиболее целесообразный метод защиты критической информации о проводимых разработках.

Методы защиты информации о проводимых разработках

Для защиты критической информации о разрабатываемой ИВП могут быть использованы следующие методы:

1) скрытие критической информации от конкурентов. Этот метод может быть реализован только до начала полномасштабных натурных испытаний продукции;

2) дезинформация конкурентов. Может быть применена на всех этапах разработки ИВП. Должна быть использована в сочетании со скрытием. Какие-то свойства и характеристики должны быть безоговорочно защищены от раскрытия конкурентами, а другие, скрыть которые невозможно, искажены таким образом, чтобы создать у конкурентов виртуальный образ продукции в соответствии с общим замыслом защиты разработок;

3) опережающие темпы создания и вывода на рынок ИВП. В этом случае можно вообще не защищать информацию о разработках. Однако такой подход является антипродуктивным, весьма затратным и не гарантирует конечного результата;

4) комбинированный метод, сочетающий в себе первые два.

Комбинированный метод наиболее эффективен, так как может быть использован на всех этапах разработки и производства ИВП и позволяет получить наилучшие результаты по критерию «эффективность – стоимость».

Как отмечалось ранее, при доведении до конкурентов виртуального образа ИВП возможно использование двух основных подходов. Первый состоит в обеспечении условия

$$\Theta_L(L, H, H_0) \gg \Theta_Z(L, H, H_0),$$

где $\Theta_L(L, H, H_0)$ – эффективность виртуального образа разрабатываемого ИВП;

$\Theta_Z(L, H, H_0)$ – эффективность имеющейся на рынке ИВП. То есть доводимые до конкурентов свойства и характеристики виртуального образа значительно превосходят достигнутые в известной продукции и, как правило, практически недостижимы на современном уровне развития техники. Как отмечалось ранее, попытка конкурентов превзойти характеристики виртуального

[10] *Аполлонский С.М., Куклев Ю.В.* Надежность и эффективность электрических аппаратов. М.: Лань, 2011. 448 с.

образа ИВП приведет к перерасходу различного вида ресурсов и потере времени из-за направления исследований и разработок по ложному руслу.

При реализации второго подхода к доведению до конкурентов виртуального образа разрабатываемой ИВП организация-разработчик стремится к обеспечению выполнения условия:

$$Э_{L0}(L, H, H_0) < Э_L(L, H, H_0) < Э_Z(L, H, H_0).$$

Решение задачи обоснования виртуального образа разрабатываемой ИВП включает совокупность работ по формированию множества возможных вариантов образа, оценке достоверности данных вариантов, анализу реакции конкурентов на получение информации о различных вариантах виртуального образа и выбора наилучшего из них.

Результатом решения задачи разработки виртуального образа разрабатываемой ИВП является его детализированное описание в виде значений и точности определения характеристик, определяющих его образ.

Обоснование виртуального образа разрабатываемой ИВП включает в себя следующие основные этапы:

– формирование набора возможных вариантов виртуального образа разрабатываемой ИВП;

– оценка правдоподобия сформированных вариантов виртуального образа разрабатываемой ИВП;

– прогнозирование возможных последствий доведения до конкурентов вариантов виртуального образа разрабатываемой ИВП и выбор предпочтительного варианта.

Рассмотрим основное содержание решения задачи обоснования виртуального образа более подробно.

Формирование набора возможных вариантов виртуального образа разрабатываемой ИВП

Для формирования различных вариантов виртуального образа разрабатываемой ИВП и выделения их из области существования проводится дискретизация значений технических характеристик. Затем на основе комбинирования полученных значений формируется множество вариантов. Критерием выбора интервала дискретизации непрерывных и дискретно-непрерывных характеристик служит степень их влияния на возможную реакцию конкурентов. Для характеристик, имеющих дискретные или точечные значения, дискретизация не проводится. Интервалы дискретизации задаются исходя из чувствительности реакции конкурентов к значению рассматриваемой характеристики [16].

Исходными данными для формирования множества возможных вариантов виртуального образа разрабатываемой ИВП являются характеристики, составляющие виртуальный образ разрабатываемой ИВП $L(H) \to Z_K(H): H(t) = \{ h_j(t) \}$, $j = \overline{1, M}$ с ограничением и требуемым уровнем правдоподобия, а также интервалы дискретизации значений непрерывных и дискретно-непрерывных характеристик $\{ \Delta h_j(t) \}$, $j = \overline{1, M}$. Результатом применения процедуры формирования является множество $L_R(H)$ возможных виртуальных образов разрабатываемой ИВП.

Выбор рациональных вариантов проходит следующим образом. Вначале проводится дискретизация значений непрерывных и дискретно-непрерывных характеристик, составляющих виртуальный образ разрабатываемой ИВП в соответствии с выбранным интервалом дискретизации (например, $H_1 = \{ h_{l0,} h_{\text{lN}} 1 \}$ преобразуется в $H_1 = \{ h_{l0,} h_{l1,..}, h_{\text{lN}} 1 \}$, $h_{1h} - h_{1n-1} \le \Delta H_1$, $n = \overline{1, N_1}$). Интервалы определяются с учетом заданных ограничений. Далее значения характеристик о ИПК комбинируются в наборы допустимых виртуальных образов разрабатываемой ИВП L_{RM}:

$$H^{L_{RM}} = \{ h_{1N1,} h_{2N2,..}, h_{MNM} \},$$

где L_{RM} – количество вариантов комбинаций значений характеристик виртуального образа.

На заключительной стадии проводится проверка возможных комбинаций характеристик виртуального образа на непротиворечивость.

Варианты комбинаций значений характеристик, удовлетворяющие всем ограничениям, формируют множество реализуемых вариантов виртуального образа разрабатываемой ИВП L_R:

$$H^L = \left\{ h_1^{L_R}, x_2^{L_R}, \ldots, x_M^{L_R} \right\},$$

где R – количество вариантов виртуального образа.

В целях снижения трудоемкости и времени выбора рациональных вариантов формирование наборов допустимых виртуальных образов разрабатываемой ИВП и проверка сформированных комбинаций на выполнение ограничений, определяющих их непротиворечивость, проводится одновременно. Формирование наборов характеристик и проверка условий их реализуемости проводится циклически при включении на каждом цикле в набор дополнительно по одной характеристике. Таким образом, реализуется возможность неполного перебора значений характеристик виртуального образа разрабатываемой ИВП[11] [16].

Оценка правдоподобия вариантов виртуального образа разрабатываемой ИВП

Правдоподобие вариантов виртуального образа разрабатываемой ИВП обеспечивается относительным соответствием доводимого до конкурентов виртуального образа разрабатываемой ИВП имеющемуся у них представлению на момент начала реализации мероприятий по дезинформации. Обязательными условиями обеспечения правдоподобия доводимого до конкурентов представления являются достоверность и техническая реализуемость виртуального образа разрабатываемой ИВП. Достоверность как степень соответствия имеющегося у конкурентов и доводимого до них представлений должна превышать минимально допустимый уровень ($D_{\min}$):

$$D[Z(H_0), L(H)] \geq D_{\min}.$$

Реализуемость обеспечивается выполнением ограничений, связанных с физическими принципами функционирования элементов продукции рассматриваемого класса, тенденциями ее развития, традициями разработчиков и т.д.:

$$\omega_i = (x_{1,} x_{2,} \ldots) \leq \Omega_i, \; i = \overline{1, I},$$

где $\omega_i = (x_{1,} x_{2,} \ldots)$ – функция от значений характеристик виртуального образа разрабатываемой ИВП;

Ω_i – максимально достижимое значение функции $\omega_i = (x_{1,} x_{2,} \ldots)$ в соответствии с i-м ограничением. При оценке показателя достоверности возможно использование известного математического аппарата, применяемого в теории распознавания образов[12].

Оценка достоверности отдельного варианта виртуального образа разрабатываемой ИВП осуществляется следующим образом. На начальном этапе оценивается достоверность значения каждой характеристики из сформированного набора, составляющего виртуальный образ разрабатываемой ИВП. Затем оценки достоверности значений характеристик объединяются в интегральный показатель, характеризующий достоверность варианта виртуального образа в целом.

Достоверность количественных характеристик рассчитывается по формуле:

$$D_{Z_m^{Lr}} = 1 - \left| \Pi_{Z_m}^{\text{ном.}} - h_m^{Lr} \right| \left(\Pi_{Z_m}^{\text{ном.}} \right)^{-1},$$

где $D_{Z_m^{Lr}}$ – достоверность характеристики, соответствующей $L_r(Z)$ варианту виртуального образа разрабатываемой ИВП;

$\Pi_{Z_m}^{\text{ном.}}$ – номинальный обобщенный показатель осведомленности о m-ой характеристике виртуального образа разрабатываемой ИВП;

h_m^{Lr} – значение m-ой характеристики L_r варианта виртуального образа разрабатываемой ИВП.

[11] *Светозаров В.В*. Основы статистической обработки результатов измерений. М.: МИФИ, 2005. 40 с.

[12] *Шикин Е.В., Шикина Г.Е.* Исследование операций. М.: Проспект, 2006. 280 с.; *Вентцель Е.С., Овчаров Л.А.* Теория случайных процессов и ее инженерные приложения. М.: Академия, 2003. 272 с.

Достоверность качественных характеристик рассчитывается как вероятность того, что конкуренты имеют некоторое представление об этой характеристике $D_{Z_m^{Lr}} = P_{Z_m}\left(H_m = h_m^{Lr}\right)$.

Значения вероятностей оцениваются на основе экспертных методов, методов статистической обработки и других аналогичных [4, 11]. При этом проводится нормирование значений вероятностей $P_{Z_m}\left(H_m = h_m^{Lr}\right)$. и обеспечение выполнения следующих постулатов:

– если по мнению конкурентов возможны несколько равновероятных вариантов показателей $H_m = h_{0m}^{Br}$, то для них всех $P_{Z_m} = 1$;

– если по мнению конкурентов значение характеристики $H_m = h_{0m}^{Br}$ кратно $H_m = h_{1m}^{Br}$, то $P_{Z_m}\left(H_m = h_{0m}^{Lr}\right) = 1$, а $P_{Z_m}\left(H_m \neq h_{1m}^{Lr}\right) = \frac{1}{k}$, где k – коэффициент кратности;

– если по мнению конкурентов возможно одно значение показателя $H_m = h_{0m}^{Br}$, то $P_{Z_m}\left(H_m = h_{0m}^{Lr}\right) = 1$, а $P_{Z_m}\left(H_m \neq h_{0m}^{Lr}\right) = 0$.

Для оценки возможности использования варианта отдельной характеристики ИВП необходима интегральная оценка достоверности виртуального образа разрабатываемой ИВП в целом. Интегральная оценка определяется как средневзвешенное достоверностей значений, соответствующих рассматриваемому варианту виртуального образа разрабатываемой ИВП:

$$D(L_r) = \sum_m \alpha_m D_{Z_m^{Lr}}, \sum_m \alpha_m = 1, \alpha_m \in [0,1],$$

где α_m – коэффициент важности m-й характеристики.

Варианты, для которых выполняется это условие, выделяются в множество $LD = \left\{ L_{1,..}, L_{RD} \right\}$ достоверных вариантов:

$$LD = \left\{ L_r \subset L : D(L_r) \geq D_{\min} \right\},$$

где $D_{\min}$ равно достоверности истинного образа ИВП или задается априори.

Прогнозирование возможных последствий доведения до конкурентов различных вариантов виртуального образа разрабатываемой ИВП и выбор предпочтительного варианта

Предпочтительный вариант виртуального образа разрабатываемой ИВП должен обеспечить минимизацию снижения эффективности ИВП при доведении до конкурентов его виртуального образа [12]:

$$\Delta \Theta^Z(L, t_1) \rightarrow \min,$$

где t_1 – время вывода ИВП на мировые рынки.

В результате выбирается предпочтительный виртуальный образ разрабатываемой ИВП в виде совокупности характеристик $H^L = \left\{ h_1^L, h_2^L, ..., h_N^L \right\}$.

Выбор предпочтительного варианта базируется на обеспечении условия (1) и осуществляется с использованием показателя эффективности защиты критической информации о ИВП $\Delta \Theta_L^Z(Z, L)$. В качестве названного показателя возможно использовать либо разность между превышением качества разрабатываемой ИВП над продукцией конкурентов на момент вывода ее на рынок в случае реализации защиты информации и без защиты, либо разность эффективности продукции конкурентов в случае получения ими истинного $Э_K(Z)$ и ложного $Э_K(L)$ образа ИВП:

$$\Delta \Theta_L^Z(Z, L) = \Delta \Theta_{защ.}^{Z,K}(Z, L) - \Delta \Theta_{без\ защ.}^{Z,K}(Z) = \\ = \Theta^K(Z) - \Theta^K(L) \rightarrow \max.$$

Непосредственно для оценки указанных показателей и эффективности защиты необходимо спрогнозировать возможные изменения в действиях конкурентов при их дезинформации в соответствии с вариантами виртуального образа разрабатываемой ИВП и оценить их последствия. Методы решения данных задач индивидуальны для каждого вида продукции и особенностей конкурентной борьбы. Для определения предпочтительного $L_{пред.}(H)$ варианта виртуального образа

разрабатываемой ИВП для целенаправленной дезинформации конкурентов необходимо из множества достоверных вариантов $L_D(H)$ выбрать тот, который обеспечивает максимум эффективности дезинформации (минимальный ущерб организации-разработчику), то есть $L_{пред.}(H) = L_r(H)$, для которого $\Delta \Im_L^Z(L_r, Z) \rightarrow \max$.

После выбора варианта виртуального образа разрабатываемой ИВП осуществляется его доведение до конкурентов через специально организованные каналы (средства массовой информации, сотрудники компании, технические каналы утечки и др.).

Заключение

Разработка инновационной продукции сопровождается финансированием и выделением различных ресурсов для проведения организационных мероприятий и создание технических средств, связанных с обеспечением безопасности конфиденциальной для разработчика информации[13]. Повышение эффективности инвестиционных вложений может осуществляться за счет снижения затрат, непосредственно не связанных с научными исследованиями и техническими разработками. В частности, за счет снижения ассигнований на защиту информации.

Синтезированный в ходе исследования метод повышения безопасности инновационных разработок в условиях конкурентного противостояния, в основу которого положена защита критической информации о разрабатываемой продукции, базируется на известном и достаточно эффективном аппарате математической статистики[14] [14, 17]. Использование предлагаемого метода не требует высокой квалификации или специальной подготовки специалистов и может быть реализовано достаточно просто при тщательном подборе экспертов и формировании экспертных групп. Разработанный метод является весьма экономичным по сравнению с методами скрытия конфиденциальных сведений, которые требуют разработки и применения технических средств и выполнения организационных мероприятий.

Использование предлагаемого метода должно осуществляться в комплексе с другими методами защиты критически важной для разработчика информацией: правовыми, организационными, техническими и т.д. Дальнейшее развитие предложенного в работе подхода к повышению безопасности и эффективности инновационных разработок может идти по пути создания прикладных методик оценки возможного ущерба от действий конкурентов для конкретной продукции, методов оценки уровня осведомленности конкурентов о текущем состоянии разработок, а также методики выбора источников доведения требуемой информации до конкурирующих организаций. Еще одним из направлений дальнейших исследований может быть выбран синтез формализованного математического аппарата назначения количественных (численных) значений характеристик ложного объекта и их допустимых отклонений для обеспечения достоверности доведения до конкурентов через различные источники информации.

[13] *Кузнецов. И.Н*. Информация: сбор, защита, анализ. М.: Яуза, 2001. 105 с.

[14] *Вентцель Е.С., Овчаров Л.А*. Теория случайных процессов и ее инженерные приложения. М.: Академия, 2003. 272 с.

Список литературы

1. *Судоплатов А.П., Лекарев С.В.* Безопасность предпринимательской деятельности. М.: Олма-Пресс, 2001. 384 с.
2. *Панарин И.Н.* Информационная война и власть. М.: Мир безопасности, 2001. 223 с.
3. *Доронин А.И.* Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности предприятия. Тула: Гриф и Ко, 2000. 116 с.
4. *Гришина Н.В.* Организация комплексной системы защиты информации. М.: Гелиос АРВ, 2007. 256 с.
5. *Щегловская К.А.* Разработка политики информационной безопасности субъекта инновационной деятельности путем создания службы защиты информации // Актуальные вопросы экономических наук. 2013. № 31. С. 130–134.
6. *Валетдинова Э.Н.* Разработка инновационной системы предприятия в условиях экономической безопасности // Экономические науки. 2011. № 74. С. 232–235.
7. *Линг В.В., Гайнутдинова М.Т.* Экономическая безопасность бизнеса // Экономика и предпринимательство. 2015. № 12-3. С. 1137–1140.
8. *Захарченко А.Д., Шилов А.К.* Информационная безопасность как стойкий риск для бизнеса // Теория и практика современной науки. 2015. № 3. С. 75–77.
9. *Селиванов Е.А.* Информационная безопасность бизнеса // Сборники конференций НИЦ Социосфера. 2011. № 21. С. 39–41.
10. *Ефимов Е.Н., Лапицкая Г.М.* Информационная безопасность и бизнес-процессы компании // Известия ЮФУ. Технические науки. 2013. № 12. С. 253–260.
11. *Шлыков В.В.* Комплексное обеспечение экономической безопасности предприятия. СПб.: Алетейя, Санкт-Петербургский университет МВД России, Рязанский институт права и экономики МВД России, 1999. 144 с.
12. *Ильичев А.В.* Эффективность проектируемой техники: основы анализа. М.: Машиностроение, 1991. 336 с.
13. *Баяндин Н.И.* Технологии безопасности бизнеса: введение в конкурентную разведку. М.: Юристъ, 2002. 320 с.
14. *Азгальдов Г.Г., Райхман Э.П.* Экспертные методы в оценке качества товаров. М.: Экономика, 1974. 151 с.
15. *Рейльян Я.Р.* Аналитическая основа принятия управленческих решений. М.: Финансы и статистика, 1989. 208 с.
16. *Гермейер Ю.Б.* Введение в теорию исследований операций. М.: Наука, 1971. 384 с.
17. *Рябушкин Т.В.* Статистические методы анализа экспертных оценок. М.: Наука, 1977. 384 с.

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

ISSN 2311-8709 (Online)
ISSN 2071-4688 (Print)

Business Value

SAFETY OF INNOVATION UNDER COMPETITIVE STRUGGLE

Aleksei P. LAPSAR'[a,•], Sergei A. LAPSAR'[b]

[a] Rostov State University of Economics, Rostov-on-Don, Russian Federation
lapsar1958@mail.ru

[b] Advanced Research Foundation, Moscow, Russian Federation
greyser1982@yandex.ru

• Corresponding author

Article history:
Received 17 November 2016
Received in revised form
1 December 2016
Accepted 15 December 2016
Available online
16 January 2017

JEL classification: C18, C44, D81

Keywords: innovative developments, critical information, competition, virtual image

Abstract

Importance The article considers the synthesis of methods to ensure the innovation safety under tough competition.

Objectives The aim of the study is to create a method to enhance the safety of innovation under fierce competition based on assessment of feasible measures of counteraction by competitors and protection of critical information on developed products.

Methods Using the tools of mathematical statistics, the theory of efficiency and expert methods, we explore possibilities to counteract the measures of competitors on innovative product discredit, and offer a method of protection, enabling to increase the safety and efficiency of long-term investment in innovation development.

Results We offer a method to provide for innovation safety and the sequence of its implementation. The method includes forecasting a possible reaction of competitors to the information on innovative developments and assessing the consequences of the counteraction; developing the methods of information security; choosing the optimal variant. The method is efficient, its use does not require high qualification or special training.

Conclusions Our original method to increase the safety of innovation is applicable under tough or unfair competition. It may be used to assess the awareness of competitors of the current status of developments, to choose a source of information communication to competing organizations.

References

1. Sudoplatov A.P., Lekarev S.V. *Bezopasnost' predprinimatel'skoi deyatel'nosti* [Business security]. Moscow, Olma-Press Publ., 2001, 384 p.
2. Panarin I.N. *Informatsionnaya voina i vlast'* [Information warfare and the power]. Moscow, Mir bezopasnosti Publ., 2001, 223 p.
3. Doronin A.I. *Razvedyvatel'noe i kontrrazvedyvatel'noe obespechenie finansovo-khozyaistvennoi deyatel'nosti predpriyatiya* [Intelligence and counterintelligence support to financial and economic activities of the entity]. Tula, Grif i Ko Publ., 2000, 116 p.
4. Grishina N.V. *Organizatsiya kompleksnoi sistemy zashchity informatsii* [Organization of a complex system of information protection]. Moscow, Gelios ARV Publ., 2007, 256 p.
5. Shcheglovskaya K.A. [Developing the information security policy of innovative companies through establishment of information security service]. *Aktual'nye voprosy ekonomicheskikh nauk = Topical Issues of Economic Sciences*, 2013, no. 31, pp. 130–134. (In Russ.)
6. Valetdinova E.N. [Developing the innovative system of the enterprise under economic security]. *Ekonomicheskie nauki = Economic Sciences*, 2011, no. 74, pp. 232–235. (In Russ.)

7. Ling V.V., Gainutdinova M.T. [Economic security of business]. *Ekonomika i predprinimatel'stvo = Economy and Entrepreneurship*, 2015, no. 12-3, pp. 1137–1140. (In Russ.)

8. Zakharchenko A.D., Shilov A.K. [Information security as a persistent risk to business]. *Teoriya i praktika sovremennoi nauki = Theory and Practice of Modern Science*, 2015, no. 3, pp. 75–77. (In Russ.)

9. Selivanov E.A. [Information security of business]. *Sborniki konferentsii NITs Sotsiosfera = Proceedings of Science Publishing Centre Sociosphere*, 2011, no. 21, pp. 39–41. (In Russ.)

10. Efimov E.N., Lapitskaya G.M. [Information security and business processes of a company]. *Izvestiya YuFU. Tekhnicheskie nauki = Izvestiya SFedU. Engineering Sciences*, 2013, no. 12, pp. 253–260. (In Russ.)

11. Shlykov V.V. *Kompleksnoe obespechenie ekonomicheskoi bezopasnosti predpriyatiya* [Integrated support to economic security of the enterprise]. St. Petersburg, Aleteiya Publ., 1999, 144 p.

12. Il'ichev A.V. *Effektivnost' proektiruemoi tekhniki: osnovy analiza* [Efficiency of designed equipment: basic principles of analysis]. Moscow, Mashinostroenie Publ., 1991, 336 p.

13. Bayandin N.I. *Tekhnologii bezopasnosti biznesa: vvedenie v konkurentnuyu razvedku* [Technologies of business security: Introduction to competitive intelligence]. Moscow, Yurist" Publ., 2002, 320 p.

14. Azgal'dov G.G., Raikhman E.P. *Ekspertnye metody v otsenke kachestva tovarov* [Expert methods in product quality evaluation]. Moscow, Ekonomika Publ., 1974, 151 p.

15. Reil'yan Ya.R. *Analiticheskaya osnova prinyatiya upravlencheskikh reshenii* [Analytical basis for managerial decision-making]. Moscow, Finansy i statistika Publ., 1989, 208 p.

16. Germeier Yu.B. *Vvedenie v teoriyu issledovanii operatsii* [Introduction to the theory of operations research]. Moscow, Nauka Publ., 1971, 384 p.

17. Ryabushkin T.V. *Statisticheskie metody analiza ekspertnykh otsenok* [Statistical methods to analyze expert estimates]. Moscow, Nauka Publ., 1977, 384 p.

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.