**УДК 004.056.5**

# СПОСОБ ЗАЩИТЫ ТЕХНОЛОГИЧЕСКОЙ ИНФОРМАЦИИ О РАЗРАБАТЫВАЕМОЙ ПРОДУКЦИИ

Серпенинов О.В.

к.т.н., доцент кафедры Информационных технологий и защиты информации

serpeninov53@mail.ru

Лапсарь А.П.

к.т.н., доцент кафедры Информационных технологий и защиты информации

lapsar1958@mail.ru

Шейдаков Н.Е.

к.ф-м.н., доцент кафедры Информационных технологий и защиты информации

Лопаткин Г.А.

доцент кафедры Информационных технологий и защиты информации

Ростовский государственный экономический университет (РИНХ)

**Аннотация:** В современных условиях повышение конкурентноспособности высокотехнологической продукции обеспечивается за счет внедрения новых инновационных подходов при создании продукции. В связи с усилением конкуренции, возникает необходимость активизировать усилия по противодействию ведению промышленной разведки за разрабатываемой продукцией. Предлагается способ защиты важной технологической информации на основе формирования у конкурентов искаженного образа разрабатываемой продукции путем их дезинформации. Обоснована необходимость использования аппарата теории нечетких множеств при формировании мер защиты

**Ключевые слова:** конкурентное преимущество, промышленная разведка, дезинформация, объект прикрытия, нечеткие множества.

# THE WAY TO PROTECT TECHNOLOGICAL INFORMATION ABOUT THE DEVELOPED PRODUCTS

Serpeninov O.V.

Lapsar A.P.

Sheydakov N.E.

Lopatkin G.A.

**Abstract:** In modern conditions, increasing the competitiveness of high-tech products is ensured by innovative approaches in the creation of products. Due to increased competition, there is a need to increase efforts to counter the industrial intelligence for developed products. This paper proposes a method of protecting important technological information. It is based on creating a distorted image of the developed product for competitors through their misinformation. The necessity of using the apparatus of the theory of fuzzy sets in the formation of protective measures is substantiated.
**Keywords:** competitive advantage, industrial intelligence, misinformation, object of cover, fuzzy set.

В современных условиях отмечается значительное возрастание доли высокотехнологической продукции, создание и производство которой требует значительных инвестиционных вложений. Окупаемость новой продукции, получение прибыли, обеспечивается конкурентными преимуществами по сравнению с предлагаемой продукцией на рынке или разрабатываемой конкурентами. Однако, при этом на рынке складывается конфликтная ситуация между разработчиком и конкурирующими структурами, которые стремятся получить важную технологическую информацию о формировании новых свойствах продукции различными способами, включая методы промышленного шпионажа.

Разработчик обязан защищать свою важную технологическую информацию о разрабатываемой продукции, используя методы скрытия, которые хорошо известны и достаточно полно описаны во многих источниках [1,2]. В то же время, практически отсутствует анализ возможности использования в качестве мер противодействия методов дезинформации и методик оценки их эффективности.

Целью проводимого исследования является разработка способа защиты технологической информации за счет проводимых мероприятий по дезинформации конкурентов.

Для обеспечения устойчивого положения на рынке организация осуществляет разработку высокотехнологической продукции с улучшенными свойствами и более высокими качественными показателями, которая превосходит аналоги, как на внутреннем, так и внешнем рынке. Окупаемость

произведенных инвестиций и получение прибыли ожидается после реализации продукции на рынке в некоторый момент времени $T$. Обеспечить конкурентную способность разрабатываемой продукции (РП) планируется за счет ее более высокого качества:

$$K[Z^{н}(t)] > K[Z^{a}(t)],$$

где $K[Z^{н}(t)]$ – качество РП в момент времени $T$ появления ее на рынке;

$K[Z^{a}(t)]$– качество имеющегося аналога на этот же момент времени;

$Z(t)$ – набор качественных характеристик продукции.

Выполнение этого условия достигается за счет улучшения определенного набора характеристик продукции $z^{н}_{i}(t) \geq z^{a}_{i}(t)$ ($i=\overline{1,I}$, $I$ - количество качественных характеристик продукции), а также появления новых качественных характеристик.

С целью минимизации потерь от действий со стороны конкурентов за счет получении информации о РП, необходимо убедить конкурентов о нецелесообразности этих действий за счет методов дезинформации, т.е. они сочтут РП недостаточно качественной и, следовательно, она не сможет составить значительную конкуренцию аналогичной продукции.

Это достигается путем доведения до конкурентов заниженных характеристик объекта, синтез которого направлен на дезинформацию конкурентов и скрытие реальных характеристик РП. С этой целью формируется новый облик РП, который отличается от реального – объект прикрытия (ОП). При этом должно соблюдаться выполнение требования, чтобы качество формируемого образца $K[Z^{o}(t)]$ удовлетворяло соотношению:

$$K[Z^{н}(t)] > K[Z^{o}(t)] > K[Z^{a}(t)].$$

Следовательно, задача защиты экономически важной промышленной информации сводится к синтезу набора характеристик ОП в виде разработки аналогичной продукции к моменту времени $T$, получение информации о котором конкурентами, позволит минимизировать ущерб от реализации ими

мер противодействия $Q\{K[Z^н(t)]\}$. Он связан со снижением качества разрабатываемой продукции относительно продукции конкурентов в зависимости от реализации ими мер противодействия:

$$\Delta K[Z^н(t)] = K[Z^н(t)]|_{n=0} - K[Z^н(t)]|_{n=nj} ,$$

где под $n_j$ понимается используемый вариант противодействия со стороны конкурентов.

Поскольку интенсивность противодействия напрямую зависит от полученной конкурентами информации $U[Z^н(t)]$ о наборе характеристик продукции, то справедливо соотношение $\Delta K[Z^н(t)] = F\{U[Z^н(t)]\}$.

Требуется определить оптимальный перечень характеристик ОП $Z^o(t)$ и, для каждой из выбранных характеристик, определить ее численное значение, обеспечивающее решение задачи защиты информации и минимизацию ущерба от действий конкурентов.

Определение оптимального перечня характеристик ОП зависит от правильного определения важности информации о каждой из характеристик и обеспечения заданной достоверности доведения ложной информации о РП через различные каналы. Доведение до конкурентов подготовленной разработчиком информации могут использоваться различные источники: СМИ, рекламные продукты, специально организованные каналы утечки информации. При этом необходимо учитывать степень доверия к источникам информации.

Решение большинства подобных задач основывается на неформально-эвристических методах аппарата нечетких множеств [3].

Для оценки эффективности синтезированного ОП необходимо определить набор возможных мер противодействия $N=\{n_j\}$, ($j=\overline{1,J}$, $J$ - количество вариантов противодействия) и потенциальную опасность каждой из них. При определении опасности деструктивных действий в виде нечетких величин необходимо проводить экспертный анализ их опасности. Такой подход обладает возможностью наиболее адекватно оценивать реальную

опасность угроз противодействия. Различные эксперты по-разному оценивают значение параметра и часто затрудняются задать конкретное число, поскольку существует слишком большое количество факторов, влияющих на оцениваемые величины, многие из которых имеют вероятностную природу. Для корректного учета таких ситуаций используется аппарат нечетких множеств, при этом меры опасности задаются в виде нечетких чисел, способных принимать свои значения из определенного заданного интервала (множества) с различными значениями функций принадлежности [3,4].

Анализ набора возможных мер противодействия со стороны конкурентов $N = \{n_j\}$ позволяет получить оценочные значения затрат на реализацию каждой из них $C(n_j)$, а также определить время на ее реализацию.

Вывод. Разработанный способ дополняет основные подходы по защите информации о разрабатываемой продукции и используемых инновационных подходах путем дезинформации конкурентов. Способ реализуется с привлечением квалифицированных экспертов и основывается на использовании математического аппарата теории нечетких множеств.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Волков Е.И. Кибербезопасность цифрового бизнеса малого предприятия // Интеллектуальные ресурсы – региональному развитию. – 2019. – Т.5, №1. – С. 35-40.
2. Лапсарь А.П., Лапсарь С.А. Обеспечение безопасности инновационных разработок в условиях конкурентного противостояния // Финансы и кредит. – 2017. – Т.23, Вып. 1. – С. 49-62.
3. Serpeninov O.V., Fedorova Y.V., Lozina E.N. Application of the apparatus of fuzzy sets for ensuring the information infrastructures security // Soft models of management in terms of digital transformation: monograph / under the general ed/ Dr., Prof. I.G. Akperov. – Rostov-on-Don: PEI HE SU (IUBIP), 2019.
4. Ефимова Е.В., Серпенинов О.В., Черкезов С.Е., Щейдаков Н.Е. Анализ факторов экономической эффективности виртуальных бизнес-отношений в цифровой экономике // Интеллектуальные ресурсы – региональному развитию. – 2018. – Т.4, №1. – С. 184-191.