



# Организационно-экономический механизм противодействия информационным угрозам

Глотина И.М.<sup>1</sup>

<sup>1</sup> Пермский государственный аграрно-технологический университет им. акад. Д. Н. Прянишникова, Пермь, Россия

## АННОТАЦИЯ:

Настоящая статья посвящена проблеме противодействия информационным угрозам экономической безопасности в условиях цифровой экономики. Предложен ряд стратегических мероприятий, ориентированных на повышение эффективности взаимодействия государственных структур, бизнеса и граждан страны в информационной сфере. Представлено авторское видение структурных элементов механизма реализации стратегических мероприятий. Изложен ряд основополагающих принципов. Важнейшим элементом механизма реализации стратегических мероприятий является деятельность государственных структур, бизнеса и граждан страны, направленная на выполнение защитной, регулятивной и превентивной функций. Это позволит исключить возможность негативного влияния на экономическую безопасность страны.

**КЛЮЧЕВЫЕ СЛОВА:** информационные угрозы, экономическая безопасность, стратегические мероприятия, организационно-экономический механизм.

## Organizational-economic mechanism to counter cyber threats

Glolina I.M.<sup>1</sup>

<sup>1</sup>Perm State Agrarian and Technological University, named after D. N. Pryanishnikov, Russia

### Введение

В условиях цифровой экономики все ключевые сферы деятельности государства, министерств и ведомств, предприятий и граждан страны находятся под влиянием стремительного развития информационно-коммуникационных технологий, а интернет становится системообразующим фактором устойчивого экономического развития. Активное использование информационных ресурсов гражданами, хозяйствующими субъектами, органами государственной власти и управления определяет новые возможности, но при этом и порождает новые угрозы, направленные на нанесение ущерба правам, интересам и жизнедеятельности субъектов информационных отношений. В силу сказанного, одной из важных задач системы управления экономической безопасностью государства является противодействие информа-

ционными угрозам с целью недопущения нанесения ими ущерба социально-экономическому развитию страны.

С учетом разнообразия информационных угроз круг задач управления системой экономической безопасности должен быть скорректирован, для этого автором предлагается ряд стратегических мероприятий, направленных на повышение уровня экономической безопасности государства.

### Стратегические мероприятия и механизм их реализации

Прежде всего, совершенствование нормативно-правовой базы в информационной сфере должно осуществляться с учетом современных достижений и перспективных разработок в области информационно-коммуникационных технологий. Необходимо законодательно признать использование киберпространства в целях совершения преступления повышающим общественную опасность обстоятельством.

Требуется подготовить правовую базу и механизм ее реализации с целью обязательной идентификации пользователей в сети Интернет [1] (*Glaz'ev, 2018*).

С целью выявления и пресечения противоправных действий целесообразно ввести ответственность владельцев и пользователей социальных сетей, информационных ресурсов, размещенных в сети Интернет, за размещение недостоверной информации на основании ст. 3 «Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации» Федерального закона № 149-ФЗ [7].

#### ABSTRACT:

This article is devoted to the problem of the countering information threats to the economic security in the digital economy. The author proposes strategic measures aimed at improving the efficiency of interaction between government agencies, business and citizens of the country in the information sphere. The author's vision of the structural elements of the mechanism of implementation of strategic measures is presented. A number of fundamental principles are outlined. The most important element of the mechanism for the implementation of strategic measures is the activity of state structures, business and citizens of the country, aimed at performing protective, regulatory and preventive functions. This will exclude the possibility of a negative impact on the economic security of the country.

**KEYWORDS:** information threats, economic security, strategic measures, organizational and economic mechanism

JEL Classification: O30, O33, O38

Received: 21.07.2019 / Published: 30.11.2019

© Author(s) / Publication: CREATIVE ECONOMY Publishers  
For correspondence: Glotina I.M. (glotina-i@yandex.ru)

#### CITATION:

Glotina I.M. [2019] Organizatsionno-ekonomicheskiy mekhanizm protivodeystviya informatsionnym ugrozam [Organizational-economic mechanism to counter cyber threats]. Kreativnaya ekonomika. 13. (11). – 2227-2236. doi: [10.18334/ce.13.11.41292](https://doi.org/10.18334/ce.13.11.41292)

Следует разработать процедуру добровольной сертификации социальных сетей и интернет-ресурсов на предмет размещения достоверного и безопасного контента.

Правоохранительным органам важно совершенствовать деятельность, направленную на проведение профилактических мероприятий и повышение культуры информационной безопасности среди населения страны, выявление и пресечение преступных действий в сети Интернет, введение ограничений использования этой среды в целях преступной деятельности.

Федеральной службе государственной статистики необходимо определить систему индикаторов, таких как количество зарегистрированных утечек информации, распределение утечек информации по источнику, по типу данных, по каналам, по отраслям; разработать методику сбора, обработки и анализа данных, отражающих ущербы, нанесенные гражданам, предприятиям и отраслям экономики в результате реализации информационных угроз.

Целесообразно создать передовые научно-технические центры для проведения прикладных и фундаментальных исследований в области кибербезопасности и оказывать им адресную государственную поддержку.

Образовательные учреждения всех уровней должны проводить планомерную работу с детьми и молодежью, направленную на укрепление базовых ценностей общества.

Средствам массовой информации необходимо учитывать современные противоречия в работе по информированию граждан об актуальных киберугрозах и схемах мошенничества в сети, о средствах защиты, проблемах кибербезопасности и путях их решения. Со стороны СМИ требуется обеспечение информационной поддержки проводимым в Российской Федерации семинарам, выставкам, форумам по вопросам информационной безопасности в целом и кибербезопасности в частности.

Роскомнадзору необходимо совершенствовать деятельность, направленную на анализ, фильтрацию и блокирование контента, способного нанести моральный, материальный и физический ущерб гражданам страны.

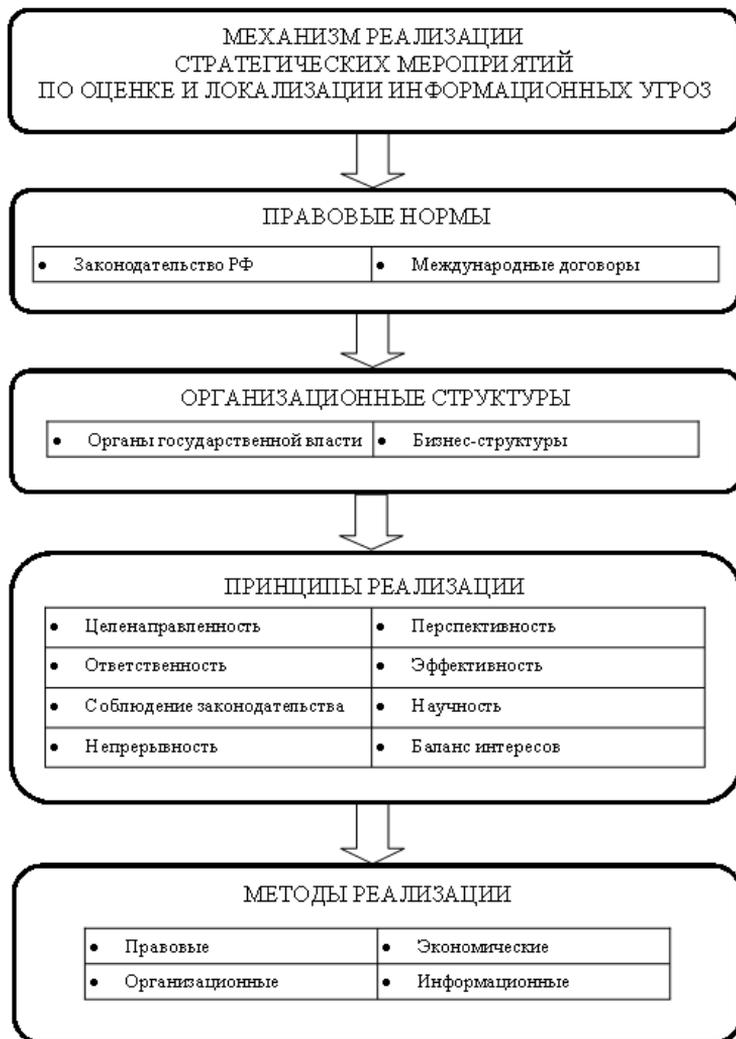
Механизм реализации стратегических мероприятий представляет собой совокупность правовых норм, организационных структур, принципов и методов управления [5] (*Mahotaeva et al., 2014*). Сущность механизма заключается в целенаправленном комплексном взаимодействии органов государственной власти совместно с другими заинтересованными субъектами для достижения намеченного результата [2] (*Glaz'ev, 2015*).

#### **ОБ АВТОРЕ:**

*Глотина Ирина Михайловна*, кандидат экономических наук, доцент, доцент кафедры информационных систем и телекоммуникаций [glotina-ir@yandex.ru]

#### **ЦИТИРОВАТЬ СТАТЬЮ:**

Глотина И.М. Организационно-экономический механизм противодействия информационным угрозам // Креативная экономика. – 2019. – Том 13. – № 11. – С. 2227-2236. doi: 10.18334/ce.13.11.41292



**Рисунок 1.** Структурные элементы механизма реализации стратегических мероприятий  
*Источник:* составлено автором.

Реализация стратегических мероприятий должна основываться на созидательных и ограничительных нормах российского и международного права (рис. 1). Важнейшим элементом механизма реализации стратегических мероприятий является деятельность государственных структур, бизнеса и граждан страны, направленная на выполнение защитной, регулятивной и превентивной функций. Ключевым государственным органом в механизме противодействия информационным угрозам экономической без-

опасности является Министерство внутренних дел Российской Федерации, реализующее широкий круг задач по предупреждению, выявлению и раскрытию преступлений в сфере компьютерной информации.

Федеральная служба безопасности и Федеральная служба технического и экспортного контроля Российской Федерации решают задачи по обеспечению безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ от кибератак.

В противодействии информационным угрозам в СМИ и сети Интернет важную роль играют Министерство связи и массовых коммуникаций и подведомственная ему Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), в области образовательной деятельности – Министерство просвещения и Министерство науки и высшего образования РФ. Министерство юстиции РФ участвует в реализации противодействия информационным угрозам экономической безопасности в рамках реализации надзорных полномочий за субъектами информационных отношений.

Важную роль в системе противодействия информационным угрозам играют негосударственные субъекты – общественные объединения, СМИ, владельцы и администраторы интернет – сайтов, блоггеры и иные пользователи интернета. Характер современных информационных угроз показывает необходимость объединения усилий государства, общества и личности по защите Российской Федерации, что предполагает участие граждан в обеспечении экономической безопасности государства [8] (*Fedotova, 2017*). Роль государства заключается в сотрудничестве с ними, применении методов стимулирования общественно полезной гражданской активности [6] (*Sudiev et al., 2014*).

Формирование механизма реализации должно опираться на систему принципов [3, 4] (*Mihajlenko, 1996; Burkov, 2001*). При этом, по мнению автора, должны соблюдаться следующие принципы и инструменты:

- принцип целенаправленности состоит в том, что управленческие решения по обеспечению экономической безопасности, принимаемые на различных уровнях управления, направлены на достижение единых целевых ориентиров;
- принцип ответственности предполагает установление ответственности органов управления и их должностных лиц за результаты своей работы в целом, с учетом распределения следующих сфер ответственности:
- государство – правовое регулирование в информационной сфере; координация действий участников информационных отношений; международное сотрудничество;
- бизнес – обеспечение безопасности критически важных информационных ресурсов и информационной инфраструктуры, находящейся в частной собственности; внедрение и соблюдение стандартов информационной безопасности;
- соблюдение законодательства предполагает принятие решений, основанных

на российских законах, гарантирующих соблюдение конституционных прав и свобод граждан в области получения информации и пользования ею, и международных соглашениях, регулирующих отношения в информационной сфере на межгосударственном уровне;

- принцип непрерывности предполагает корректировку управленческих решений на основе мониторинга внутренних и внешних информационных угроз;
- принцип перспективности означает, что решения принимаются с учетом текущего состояния и перспектив развития информационно-коммуникационных технологий;
- эффективность управления – степень соответствия результата деятельности объекта управления целям субъекта управления;
- принцип научности выражается в использовании современных научных методов в процессе мониторинга, диагностики, оценки, предупреждения, нейтрализации и устранения информационных угроз;
- соблюдение баланса интересов означает, что реализация стратегических мероприятий должна осуществляться с учетом интересов всех участников информационного взаимодействия.

Практическое выполнение стратегических мероприятий предполагает создание и обеспечение эффективного функционирования механизма их реализации (рис. 2).

Главной целью механизма реализации стратегических мероприятий, по мнению автора, является создание оптимальных условий для жизнедеятельности граждан, социально-экономического развития страны, сохранения целостности и государственности России.

В ходе работы механизма могут возникать сбои, проявляющиеся в противоречии интересов в информационной сфере между субъектами управления и объектами безопасности. Это необходимо учитывать при разработке конкретных рычагов механизма и методов их применения.

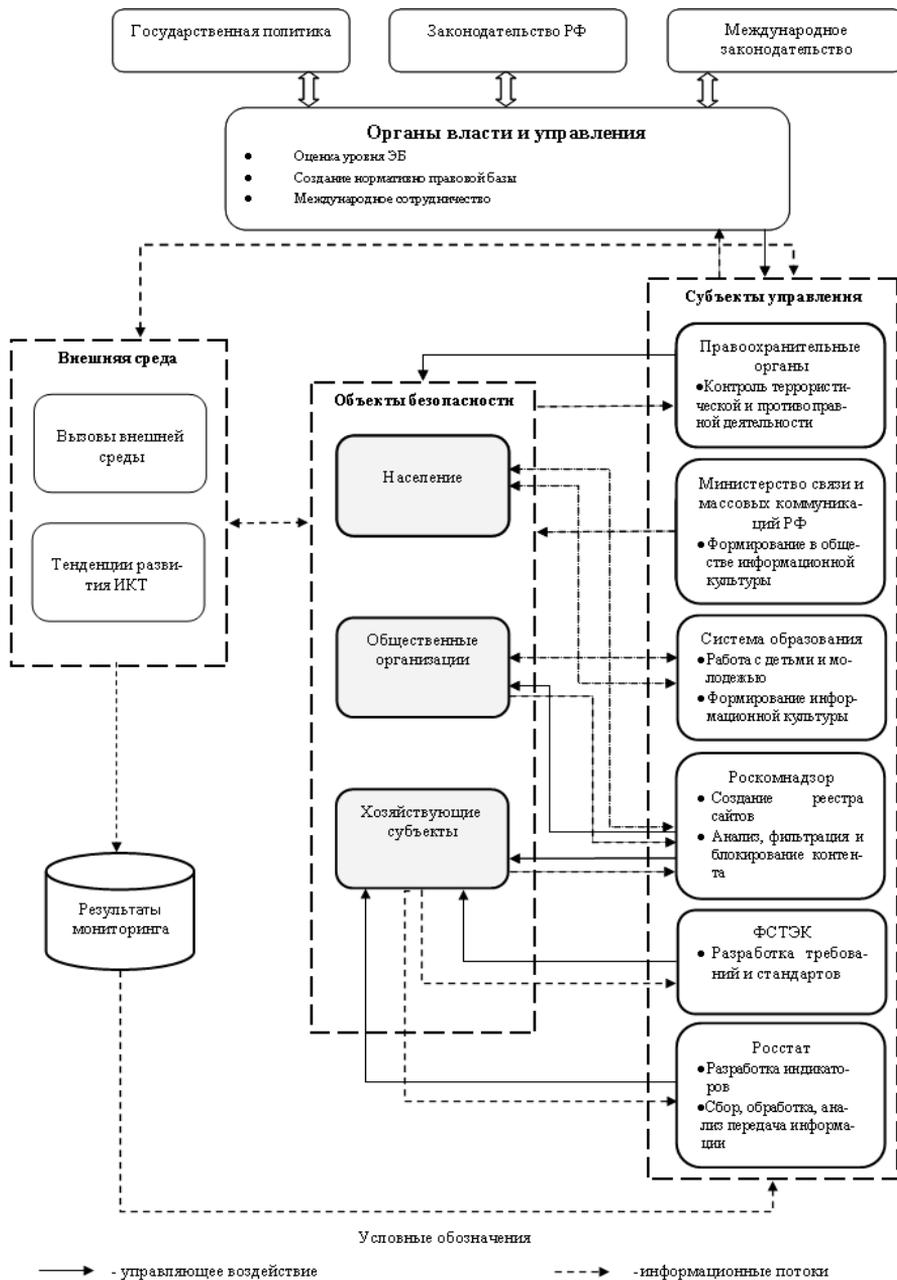
## Заключение

Социально-экономическое развитие страны и уровень ее экономической безопасности все больше зависят от возможностей современных информационных технологий и степени их использования.

При этом знание информационных угроз и умение организовать противодействие им является важным элементом системы экономической безопасности.

Предложенные выше стратегические мероприятия, направлены на укрепление экономической безопасности страны и ориентированы, в основном, на повышение эффективности взаимодействия государственных структур, бизнеса и граждан страны в информационной сфере.

Организационно-экономический механизм реализации стратегических мероприятий должен базироваться на совокупности основополагающих принципов, что



**Рисунок 2.** Механизм реализации стратегических мероприятий  
 Источник: составлено автором.

создаст условия для объективной оценки информационных угроз как внутреннего, так и внешнего характера, позволит исключить возможность прямого и косвенного негативного влияния на социально-экономические процессы. Своевременное реагирование на возникающие информационные угрозы исключит хаотичный характер противодействий заинтересованных лиц, снизит реальный и возможный ущерб от влияний и последствий информационного характера.

### ИСТОЧНИКИ:

1. Глазьев С.Ю. Информационно-цифровая революция // Евразийская интеграция: экономика, право, политика, 2018. – № 1 (236).
2. Глазьев С.Ю. Создание системы обеспечения экономической безопасности и управления развитием России // Менеджмент и бизнес-администрирование, 2015. – № 4.
3. Михайленко А. Механизм обеспечения экономической безопасности России // Мировая экономика и международные отношения, 1996. – № 7.
4. Бурков В.И. и др. Модели и механизмы управления безопасностью. Монография. – Москва: СИНТЕГ, 2001.
5. Махотаева М.Ю., Фихтнер О.А., Григорьева О.В. Механизм реализации стратегии инновационного развития // Вестник Псковского государственного университета. Серия: Экономические и технические науки, 2014. – № 4.
6. Судиев И.Ю., Смирнов А.А., Кундетов А.И., Федотов В.П. Теория и практика информационного противодействия экстремистской и террористической деятельности. – Вологда: Полиграф-Книга, 2014.
7. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 19. 12. 2016) «Об информации, информационных технологиях и о защите информации». Консультант Плюс. [Электронный ресурс]. URL: <http://www.consultant.ru>.
8. Федотова Ю.Г. Теоретико-правовой анализ участия граждан в противодействии информационным угрозам безопасности государства // Вестник Уральского финансово-юридического института, 2017. – № 3(9).

### REFERENCES:

- Burkov V.I. i dr. (2001). *Modeli i mekhanizmy upravleniya bezopasnostyu* [Models and mechanisms security management] Moscow: SINTEG. (in Russian).
- Fedotova Yu.G. (2017). *Teoretiko-pravovoy analiz uchastiya grazhdan v protivodeystvii informatsionnym ugrozam bezopasnosti gosudarstva* [Theoretical-legal analysis of citizens ' participation in combating information security threats to state]. *Bulletin of Ural Financial and Law Institute*. (3(9)). (in Russian).
- Glazev S.Yu. (2015). *Sozдание sistemy obespecheniya ekonomicheskoy bezopasnosti i upravleniya razvitiem Rossii* [Creating a system of economic management and security developments in Russia]. *Management and Business Administration*. (4). (in Russian).

- Glazev S.Yu. (2018). *Informatsionno-tsifrovaya revolyutsiya* [Information and digital revolution]. *Eurasian Integration: Economics, Law, Politics*. (1(236)). (in Russian).
- Makhotaeva M.Yu., Fikhtner O.A., Grigoreva O.V. (2014). *Mekhanizm realizatsii strategii innovatsionnogo razvitiya* [Mechnism of innovative development strategy implemenyayion]. *Vestnik Pskovskogo gosudarstvennogo universiteta. Seriya: Ekonomicheskie i tekhnicheskie nauki*. (4). (in Russian).
- Mikhaylenko A. (1996). *Mekhanizm obespecheniya ekonomicheskoy bezopasnosti Rossii* [The mechanism of ensuring economic security of Russia]. *World Economy and International Relations*. (7). (in Russian).
- Sudiev I.Yu., Smirnov A.A., Kundetov A.I., Fedotov V.P. (2014). *Teoriya i praktika informatsionnogo protivodeystviya ekstremistskoy i terroristicheskoy deyatel'nosti* [Theory and practice of information counteraction of extremist and terrorist activities] Vologda: Poligraf-Kniga. (in Russian).

