

Научная статья

Original article

УДК 338.2

doi: 10.55186/2413046X\_2023\_8\_2\_90

**ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ЭКОНОМИЧЕСКОЙ  
УСТОЙЧИВОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ В УСЛОВИЯХ  
ЦИФРОВИЗАЦИИ**

**STATE REGULATION OF ECONOMIC SUSTAINABILITY OF  
INDUSTRIAL ENTERPRISES IN THE CONDITIONS OF  
DIGITALIZATION**



**Медведева Дарья Алексеевна**, аспирант, ФГБОУ ВО «Омский государственный педагогический университет», Омск

**Скок Александр Дмитриевич**, ФГБОУ ВО «Омский государственный педагогический университет», Омск

**Мявлина Нурзидя Жаферовна**, доцент, кандидат экономических наук, доцент кафедры «Коммерция и торговое дело», Московского финансово-промышленного университета «Синергия»

**Охотников Илья Викторович**, доцент, кандидат экономических наук, доцент кафедры «Экономическая теория и менеджмент» Российского университета транспорта (МИИТ)

**Шведов Лев Александрович**, доцент, кандидат исторических наук, доцент кафедры «Экономическая теория и менеджмент» Российского университета транспорта (МИИТ)

**Medvedeva Daria Alekseevna**, graduate student, Federal State Budgetary Educational Institution of Higher Education "Omsk State Pedagogical University", Omsk, [daria\\_93@inbox.ru](mailto:daria_93@inbox.ru)

**Skok Alexander Dmitrievich**, Federal State Budgetary Educational Institution of Higher Education "Omsk State Pedagogical University", Omsk

**Myavlina Nurzidya Zhaferovna**, Docent, Candidate of Economic Sciences, Assistant Professor Department of the Moscow Financial and Industrial University Synergy, Russia, Moscow, e-mail: [nurzidy@mail.ru](mailto:nurzidy@mail.ru)

**Okhotnikov Ilya Viktorovich**, Docent, Candidate of Economic Sciences, Assistant Professor of the Economic Theory and Management Department of the Russian University of Transport (МИТ), Russia, Moscow, e-mail: [roat.miit@mail.ru](mailto:roat.miit@mail.ru)

**Shvedov Lev Alexandrovich**, Docent, Candidate of Historical Sciences, Assistant Professor of the Economic Theory and Management Department of the Russian University of Transport (МИТ), Russia, Moscow, e-mail: [roat.miit@mail.ru](mailto:roat.miit@mail.ru)

**Аннотация.** В целях совершенствования информационной безопасности промышленных предприятий в статье рассмотрено государственное регулирование экономической устойчивости. В рамках выделенных факторов, влияющих на информационную безопасность выделены основные функции, к которым необходимо проявить повышенное внимание для улучшения качества защиты информации от утечки и кибератак. Выявлен процесс развития экономической устойчивости промышленных предприятий. Проанализирован процесс утечки информации при кибератаках, последствия и способы предотвращения и восстановления данных. Особое внимание уделено угрозам информационной безопасности и защиты со стороны государства при условии природных катаклизмов. Описаны главные задачи информационной безопасности с учетом всех необходимых для высококачественной работы факторов. Рассмотрено определение «экономической устойчивости» разными авторами. Изучены отрасли, наиболее подверженные рискам утечки данных и

совершению кибератак. Предложены варианты совершенствования техник и действий по поддержанию информационной безопасности. Рассмотрены политические и правовые методы воздействий на экономическую устойчивость в сфере промышленности, после чего выделены необходимые условия и требования к развитию определенных направленностей разных областей деятельности. Дано определение цифровизации и информации, определена актуальность данных терминов в экономических отношениях и обеспечении информационной безопасности в промышленном секторе экономики. Выделены задачи информационных систем, обеспечивающих информационную безопасность и их взаимосвязь с экономической устойчивостью. Рассмотрено государственное регулирование экономической устойчивости, также способы, формы, методы и условия обеспечения ее рентабельности. Рассмотрены современные технологии и их условия работы, а также значимость в деятельности по обеспечению экономической устойчивости промышленных предприятий. Представлены диаграмма и рисунок в тематике кибератак и информационных взломов разных отраслей, также способы предотвращения и последствия после утечки и кражи информации при государственном регулировании и своевременном контроле информационной безопасности. Изучена теория рассмотрения вопроса информационной безопасности и ситуации утечки информации из промышленных предприятий в связи с природными катаклизмами и другими причинами, не связанными с работой хакера или нарушением трудовых функций служащих промышленных предприятий.

**Abstract.** In order to improve the information security of industrial enterprises, the article considers the state regulation of economic sustainability. Within the framework of the identified factors affecting information security, the main functions are highlighted, which require increased attention to improve the quality of information protection from leakage and cyberattacks. The process of development of

economic stability of industrial enterprises is revealed. The process of information leakage during cyberattacks, the consequences and methods for preventing and recovering data are analyzed. Particular attention is paid to the threats to information security and protection from the state under the condition of natural disasters. The main tasks of information security are described, taking into account all the factors necessary for high-quality work. The definition of "economic sustainability" by different authors is considered. The industries most exposed to the risks of data leakage and cyber attacks have been studied. Options for improving techniques and actions to maintain information security are proposed. The political and legal methods of influencing economic sustainability in the industry are considered, after which the necessary conditions and requirements for the development of certain areas of activity in different areas are identified. The definition of digitalization and information is given, the relevance of these terms in economic relations and ensuring information security in the industrial sector of the economy is determined. The tasks of information systems that ensure information security and their relationship with economic sustainability are identified. Considered state regulation of economic sustainability, as well as ways, forms, methods and conditions for ensuring its profitability. Modern technologies and their working conditions, as well as their importance in activities to ensure the economic sustainability of industrial enterprises, are considered. A diagram and a drawing are presented on the subject of cyber attacks and information hacking in various industries, as well as ways to prevent and consequences after leakage and theft of information under state regulation and timely control of information security. The theory of consideration of the issue of information security and the situation of information leakage from industrial enterprises due to natural disasters and other reasons not related to the work of a hacker or violation of the labor functions of employees of industrial enterprises has been studied.

**Ключевые слова:** информация, безопасность, государство, защита, контроль, государственное регулирование, промышленность

**Key words:** information, security, state, protection, control, state regulation, industry

Промышленный сектор – один из значимых секторов экономики страны, который развивается как с практической, так и с научной стороны. Важно отметить, что на современном уровне развития промышленного сектора структура и конкурентоспособность отрасли не отвечает потребностям, поставленным в обществе, а также перспективам развития стоящим перед страной.

Промышленный сектор напрямую работает через информацию, получаемую из внешней среды. Данный факт обязывает сделать вывод о том, что для эффективной работы промышленности необходимо обеспечить информационную безопасность. При успешном обеспечении безопасности необходимо поддержание и контроль работы информации в скрытом для внешней среды режиме. Для выполнения последнего условия важным становится вопрос о государственном регулировании информационной безопасности.

Актуальность статьи заключается в изучении государственного регулирования информационной безопасности при работе и создании трудовых условий промышленности Российской Федерации.

Целью статьи является рассмотреть деятельность государственного регулирования информационной безопасности и усовершенствовать факторы, влияющие на обеспечение безопасности промышленного сектора. Областью исследования статьи является информация, необходимая для работы промышленного сектора Российской Федерации.

Политические и правовые методы воздействий на социально-экономические отношения регионов в сферах развития и совершенствования

при условиях использования стратегий информационной безопасности на сегодняшний день используют системные параметры в своей деятельности. Самым известным способом защиты информационной безопасности при условии изучения современных стандартов, занимающихся поддержанием охраны информации, сохранением конфиденциальности данных разных инфраструктур деятельности считается межведомственная политика.

На современном этапе развития уровня цифровизации и в условиях конкурентной борьбы, инструменту квалификаций необходим комплексный подход к развитию определенных направленностей разных областей деятельности, также к способам и методикам регулирования всех процессов взаимодействия и обеспечения информационной безопасности.

Цифровизация – это использование действующих цифровых технологий в разных направленностях деятельности предприятий промышленного сектора [1].

Информация — это данные о людях, предметах, фактах, событиях и процессах. Связующим звеном между предприятиями промышленного сектора и внешней средой может быть информационная система, которая в большинстве случаев подвержена кибератакам. Если предприятие промышленного сектора экономики не получает, либо не выдает необходимую информацию, следует считать, что концепция несовершенна. Также следует сделать вывод, что для определенных предприятий промышленного сектора концепция выступает главным информатором для остальных существующих баз данных, так как имеет оперативную память и архив информации. При работе с информационной системой оперативного уровня работнику предприятия промышленного сектора становится легче увеличивать продуктивность и производительность работ инженеров и проектировщиков. Объединенное слияние сведений организаций и деятельность по обработке

бумажной информации становится основополагающим принципом в работе информационных систем [2].

Производительность экономики напрямую зависит от уровня развития информационных систем, тем более по мере трансформации индустриального общества в информационное. Также как и использование информационных систем возможно только в случае обеспечения информационной безопасности. На сегодняшний день системы защиты и охраны информации стремительно развиваются на промышленных предприятиях [3].

Задачами безопасности информационных систем и технологий может выступать:

—ограниченный доступ к действующим информационным системам и информационным технологиям;

—совершенствование системы защиты от вирусов и взломов;

—подобающее использование современных информационных систем и цифровых технологий в соответствии с нормами, актами и требованиями разработчиков информационных систем и информационных технологий;

—ликвидация негативных последствий при работе с современными информационными системами и цифровыми технологиями;

—создание и поддержание комфортной среды для трудовой деятельности при использовании современных информационных систем и цифровых технологий [4].

В настоящее время нет общепризнанного подхода к определению термина «экономическая устойчивость», также как и нет единых подходов к её оценке. Из этого вытекает возросший научный интерес и актуальность темы исследования.

Для того чтобы рассматривать вопросы экономической устойчивости, необходимо прежде всего разобраться, что представляет собой сам термин «устойчивость» [5,6].

А.Л. Гапоненко экономическую устойчивость понимает, как относительную неизменность основных параметров территориальной социально-экономической системы, ее способность сохранять их в заданных пределах при отклоняющихся (как негативных, так и позитивных) влияниях извне и изнутри.

А.М. Ляпунов отмечает экономическую устойчивость как способность системы возвращаться в состояние равновесия при возмущающих воздействиях внешней среды.

Ф.М. Сафин термин «Экономическая устойчивость» описывает как совокупность равновесий на различных уровнях – отдельных, единичных и частных равновесий.

В.А. Сумино определяет экономическую устойчивость как равновесное сбалансированное состояние экономических ресурсов, обеспечивающее стабильную прибыльность и нормальные условия для расширенного воспроизводства устойчивого экономического роста, в длительной перспективе, с учетом важнейших внешних факторов [7].

С.Н. Никешин дает следующее определение термину «Экономическая устойчивость» - это оптимальное соотношение между всеми элементами системы, связи между ними, которые позволяют максимально долго поддерживать жизненно важные параметры на заданном уровне, эффективно противодействуя возмущающему воздействию внешней среды

Авторы определяют экономическую устойчивость как способность объекта находиться в состоянии относительного равновесия при условии постоянного влияния факторов внутренней и внешней среды. Устойчивость тесно связана с разнообразием системы и ее способностью к адаптации [1].

Устойчивость представляет собой системное качество и может быть отражена в разных аспектах, например, экономическая, социальная,



политическая, экологическая устойчивость. В данном случае нас интересует экономическая устойчивость [8].

Понятие «экономическая устойчивость» возникло вследствие проблемы нехватки ресурсов, вызванной нефтяным и энергетическим кризисами 1973 и 1979 гг. [8].

Проанализировав различные взгляды определения экономической устойчивости, изложенные выше, необходимо отметить, что при определении экономической устойчивости необходимо учитывать следующие ключевые моменты:

– экономическая устойчивость объекта (в том числе региона) подразумевает как нахождение объекта в состоянии экономического равновесия и поддержание данного состояния, так и переход объекта к новому равновесному состоянию (развитие);

– экономическая устойчивость представляет собой динамическую категорию, отражающую способность изменять состояние объекта во времени и восстанавливать его до равновесного;

– уровень экономической устойчивости объекта определяется значениями количественных и качественных показателей. Причем у предприятий, отраслей и регионов будут свои показатели и критерии оценки [9].

Таким образом, под экономической устойчивостью необходимо понимать способность объекта (региона, предприятия) поддерживать на определенном уровне значения экономических показателей, который позволяет обеспечить его стабильное развитие, принимать первоначальное или приходиться в новое состояние равновесия после прекращения воздействий внешней и внутренней сред в настоящем и прогнозируемом будущем.

## II. Постановка задачи

На сегодняшний день создано и поддерживается большое число технологий, которые помогают обеспечивать информационную безопасность экономической устойчивости.

Авторы рассматривают защиту информационной безопасности экономической устойчивости в качестве системы биометрии современных технологий, деятельности экономической безопасности Министерства внутренних дел Российской Федерации, шифрования данных и персонального идентификационного номера конфиденциальных данных производства.

Важно отметить, что, несмотря на постоянное использование термина информация, наблюдается большое количество дискуссий на счет его определения, также как и разных смыслов в разных областях деятельности.

В статье термин «Информация» будет рассматриваться как знания или данные, которые поступают от одного лица к другому независимо от формы или способа передачи [8,9].

Для обучения, коммерческой деятельности, поддержания здорового образа жизни, отдыха, охраны национальной безопасности и других видов деятельности человеку нужна информация. Информационные системы определяются как главный ресурс, способствующий приумножению благосостояния граждан Российской Федерации. Важным условием успешного применения в любой трудовой деятельности поступающей достоверной информации является государственное регулирование и защита информации [10].

В современном мире большую роль в использовании информации играют цифровые технологии, которые также подвержены, взломан и нуждаются в защите баз данных.

К современным цифровым технологиям можно отнести смартфон-компьютер, планшеты, компьютер на стене, виртуальную реальность,

электронную книгу, дополненная реальность (среда работы смартфона) и так далее [11].

Информационную безопасность принято рассматривать как борьба с незаконным доступом, использованием, рассекречиванием, фальсификацией или уничтожением информации. Термин информационная безопасность применяется вне зависимости от формы информации, это может быть электронный, устный и любой другой вид информации.

К главным задачам информационной безопасности относится сохранение конфиденциальности, достоверности, полноты и приемлемость информации, при учете обоснованности использования и без убытков для производительности предприятия.

Несмотря на выделение информационной безопасности, как самостоятельного направления 5 октября 1999 г. на совещании членов Совета Безопасности Российской Федерации существует ряд причин, по которым информационная безопасность остается неустойчивой и подвержена реальным угрозам [12].

Факторы, которые тормозят развитие безопасности и совершенствование информационных систем могут выступать высокие издержки при принятии решений, существенная разница между техническим обеспечением, недостаток соответствующего персонала и слабая система защиты информации.

Главным фактом, который затормаживает усовершенствование систем защиты и применение цифровых технологий для защиты информационной безопасности в России считается отсутствие соответствующей законодательной базы.

В статье определено место информационной безопасности в системе экономических отношений и специфика государственного регулирования рассматриваемого определения.

Для регулирования сбоя и своевременной реакции на работу цифровой среды государству необходимы инструменты, при помощи которых становится возможным своевременный контроль и обеспечение национальной безопасности сферы цифровизации.

Создание цифровой среды является главной задачей государства при обеспечении высокого уровня администрирования, наблюдение и контроля цифрового пространства, где каждый участник имеет закрепленные за ним возможности и задачи, которые создают определенные отношения между государством и обществом [8].

На диаграмме 1 показаны в процентном соотношении отрасли, наиболее подверженные рискам утечки данных и совершению кибератак.



Диаграмма 1 - Отрасли, наиболее подверженные рискам утечки данных и совершению кибератак.

По диаграмме 1 видно, что первым сектором кибератак является сектор социальных сетей, после него наиболее подвержен взломам сектор банков и после государственный сектор.

К сектору социальная жизнь относятся: фармацевтика (в том числе аптеки), спортивные организации, автомобильная отрасль и производство товаров.

К сектору пассажирские перевозки относятся перевозки любым способом, а именно авиалинии, жд перевозки, такси и т.д.

По диаграмме видно, что более 30% кибератак выдерживает государственный сектор, что превышает атаки на банковскую сферу, которая по мнению многих экспертов считается главной целью кибератак [8-10].

Для примера кибератак в сфере государства можно выделить информацию с голосований или обороной страны.

Особое внимание привлекает свод законов в сфере защиты информационной безопасности, при своевременном исполнении которого информация, содержащая государственную тайну, не сможет покинуть стены компании, а доступ к ней внутри предприятия останется ограниченным.

На рисунке 1 показан алгоритм выявления утечки информации на предприятиях.

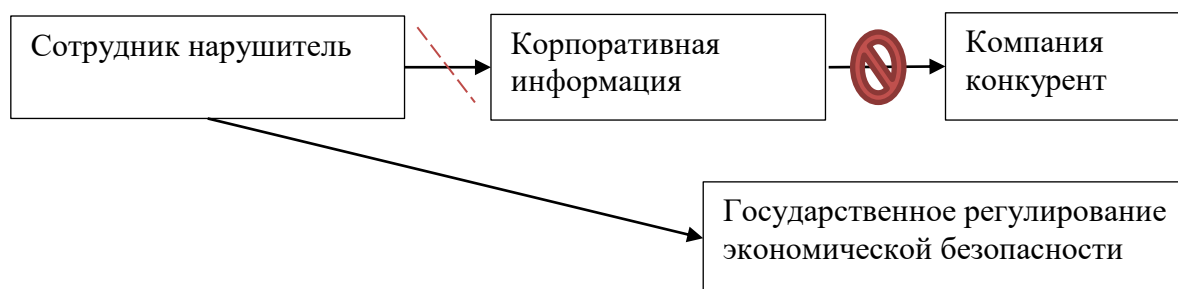


Рисунок 1 - Алгоритм безопасности информации.

На рисунке 1 показан алгоритм безопасности информации, при котором происходит анализ информации, который учитывает морфологические признаки и речевые ошибки, изображений, голосовых сообщений и звонков, распознавание речи, распознавание пересылаемых банковских карт, фото

паспорта, внутренних документов [11]. На рисунке 1 красной прерывистой линией между сотрудником нарушителем и корпоративной информацией показана система защиты информации в виде биометрии современных технологий, деятельности экономической безопасности Министерства внутренних дел Российской Федерации, шифрования данных и персонального идентификационного номера конфиденциальных данных производства. По рисунку 1 можно сделать вывод, что на сегодняшний день при попытке взлома информационной безопасности «хакер» в 96,7% (по статистике) попадают в службу государственного регулирования экономической безопасности и привлекаются к ответственности перед законодательством Российской Федерации.

### III. Экономическая безопасность при природных катаклизмах.

Информационная безопасность подвержена не только кибератакам на практике. Во многих методических изданиях выделяются такие ситуации с существующими угрозами, как:

1. Природные явления, такие как наводнения, пожары и другие. В ходе данных катаклизмов происходит потеря информации;
2. шпионаж;
3. несанкционированный доступ и нарушение техники безопасности приводит к программным ошибкам и кражи информации сотрудниками предприятий;
4. неподготовленные к определенной деятельности сотрудники также создают угрозу к уязвимости, распространению и атакам информации;
5. нарушения гражданских прав, нарушение личных данных, передача информации неавторизованным лицам, кража личных данных [12,13,14].

Результатами от проведенных мероприятий, указанных в пункте II можно считать достижение таких задач, как:

1. Подготовка и принятие законодательных и иных нормативно-правовых актов в области защиты информации.
2. Обеспечение контроля за их исполнением.
3. Финансовое и кадровое обеспечение мероприятий по защите информации.
4. Обеспечение эффективного управления системой защиты информации.
5. Анализ и оценка угроз безопасности, охраняемой законом информации.

Вывод о внедрение цифровой рабочей среды вытекает из каждого пункта, описанного в статье. Цифровая среда государственного контроля информационной безопасности на сегодняшний день считается одним из значимых элементов современных трудовых отношений.

Совершенствование работы уровня цифровой среды упрощает контроль и защиту информации со стороны государства [15-18].

#### V. Выводы

Цифровая среда в странах с развитой экономикой активно используется государством для охраны информации для государства с одной стороны, для эффективной работы промышленного сектора с другой стороны.

При этом мониторинг информации в сфере безопасности не теряет своей актуальности. Государственные органы регулярно работают над разработкой и совершенствованием системы управления информационной безопасности. Система управления информационной безопасности в свою очередь включает методы управления рисками информационных угроз, методы обучения сотрудников центра безопасности и предприятий, выбор мер безопасности и обмен опытом с более квалифицированными и опытными служащими.

Усиленная работа над повышением уровня защиты информационной безопасности цифровых управленческих процессов сопряжена напрямую со

структурным функционалом компании и нормативно-правовыми актами промышленных предприятий. Деятельность по обеспечению информационной безопасности напрямую зависит от стратегических решений, направленных на увеличение рентабельности от деятельности промышленности, также от применения инновационных цифровых форм защиты информации и создание единой цифровой базы информационной безопасности.

#### **Список источников**

1. Экономический анализ : учебник для вузов / Н. В. Войтоловский [и др.] ; под редакцией Н. В. Войтоловского, А. П. Калининой, И. И. Мазуровой. — 8-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 631 с.
2. Зарубина, Н. Н. Экономическая социология : учебник и практикум для вузов / Н. Н. Зарубина. — 3-е изд. — Москва : Издательство Юрайт, 2022. — 378 с. — (Высшее образование). — ISBN 978-5-534-00974-3.
3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8.
4. Кафтан, В. В. Противодействие терроризму : учебное пособие для вузов / В. В. Кафтан. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 261 с. — (Высшее образование). — ISBN 978-5-534-00322-2.
5. Кузнецова Е. И. Экономическая безопасность : учебник и практикум для вузов / Е. И. Кузнецова. — 2-е изд. — Москва : Издательство Юрайт, 2022. — 336 с. — (Высшее образование). — ISBN 978-5-534-14514-4.
6. Кочои С. М. Терроризм и экстремизм: уголовно-правовая характеристика. — М.: Проспект, 2005. — 176 с
7. Ляхов Е. Г., Попов, А.В. Терроризм: национальный, региональный и международный контроль: монография. — М: Ростов-на-Дону. РЮИ МВД России, 2017. — 118 с.



8. Медведева Д.А., Скок А.Д., Охотников И.В., Сибирко И.В. Искусственный интеллект в государственном регулировании теплоэнергетических систем промышленных предприятий // Московский экономический журнал. 2022. № 10. URL: <https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-10-2022-62/>.
9. Медведева, Д.А. Информационная безопасность в условиях цифровизации / Д.А. Медведева // Фундаментальные и прикладные исследования молодых ученых. Сборник материалов V Международной научно-практической конференции студентов, аспирантов и молодых учёных. Омск, 2021. С. 128-132.
10. Морозов Г.И. Терроризм — преступление перед человечеством. М.: ИМЭ и МО РАН, 2017. – 161 с.
11. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с.
12. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование).
13. Савина А. Д. Бюджет на террористов: Как ИГИЛ влияет на мировую экономику // Секрет фирмы – 2017. - № 10. – С. 5.
14. Уразгалиев, В. Ш. Экономическая безопасность : учебник и практикум для вузов / В. Ш. Уразгалиев. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 725 с. — (Высшее образование). — ISBN 978-5-534-09982-9.
15. Федеральный закон "О противодействии терроризму" от 06.03.2006 N 35-ФЗ.
16. Экономическая дипломатия в 2 ч. Часть 1 : учебник и практикум для вузов / Р. И. Хасбулатов [и др.] ; под редакцией Р. И. Хасбулатова. — Москва: Издательство Юрайт, 2022. — 282 с. — (Высшее образование). — ISBN 978-5-534-05293-0.

17. Hanan Alon. Countering Palestinian Terrorism in Israel: toward a policy analysis of countermeasures; RAND Corporation. 1980. 271 p.

18. Nathanson, S. Terrorism and the Ethics of War. Cambridge: Cambridge University Press. 2010. pp. 11-23.

### References

1. Economic analysis: a textbook for universities / N. V. Voitlovsky [and others]; edited by N. V. Voitlovsky, A. P. Kalinina, I. I. Mazurova. - 8th ed., revised. and additional - Moscow: Yurayt Publishing House, 2023. - 631 p.

2. Zarubina, N. N. Economic sociology: textbook and workshop for universities / N. N. Zarubina. - 3rd ed. - Moscow: Yurayt Publishing House, 2022. - 378 p. - (Higher education). - ISBN 978-5-534-00974-3.

3. Zenkov, A. V. Information security and protection of information: a textbook for universities / A. V. Zenkov. - Moscow: Yurayt Publishing House, 2022. - 104 p. - (Higher education). — ISBN 978-5-534-14590-8.

4. Kaftan, V. V. Countering terrorism: a textbook for universities / V. V. Kaftan. — 2nd ed., corrected. and additional - Moscow: Yurayt Publishing House, 2022. - 261 p. - (Higher education). - ISBN 978-5-534-00322-2.

5. Kuznetsova E. I. Economic security: textbook and workshop for universities / E. I. Kuznetsova. - 2nd ed. - Moscow: Yurayt Publishing House, 2022. - 336 p. - (Higher education). - ISBN 978-5-534-14514-4.

6. Kochoi S. M. Terrorism and extremism: criminal law characteristics. - M.: Prospect, 2005. - 176 p.

7. Lyakhov E.G., Popov, A.V. Terrorism: national, regional and international control: a monograph. - M: Rostov-on-Don. RUI of the Ministry of Internal Affairs of Russia, 2017. - 118 p.

8. Medvedeva D.A., Skok A.D., Okhotnikov I.V., Sibirko I.V. Artificial Intelligence in State Regulation of Heat and Power Systems of Industrial Enterprises // Moscow

Economic Journal. 2022. No. 10. URL: <https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-10-2022-62/>.

9. Medvedeva, D.A. Information security in the context of digitalization / D.A. Medvedeva // Fundamental and applied research of young scientists. Collection of materials of the V International scientific-practical conference of students, graduate students and young scientists. Omsk, 2021, pp. 128-132.

10. Morozov G.I. Terrorism is a crime against humanity. M.: IME and MO RAN, 2017. - 161 p.

11. Organizational and legal support of information security: textbook and workshop for universities / edited by T. A. Polyakova, A. A. Streltsov. - Moscow: Yurayt Publishing House, 2022. - 325 p.

12. Suvorova, G. M. Information security: a textbook for universities / G. M. Suvorova. - Moscow: Yurayt Publishing House, 2022. - 253 p. - (Higher education).

13. Savina A. D. Budget for terrorists: How ISIS affects the global economy // Secret of the firm - 2017. - No. 10. - P. 5.

14. Urazgaliev, V. Sh. Economic security: textbook and workshop for universities / V. Sh. Urazgaliev. - 2nd ed., revised. and additional - Moscow: Yurayt Publishing House, 2022. - 725 p. - (Higher education). - ISBN 978-5-534-09982-9.

15. Federal Law "On Combating Terrorism" dated March 6, 2006 N 35-F3.

16. Economic diplomacy at 2 pm Part 1: textbook and workshop for universities / R. I. Khasbulatov [and others]; edited by R. I. Khasbulatov. - Moscow: Yurayt Publishing House, 2022. - 282 p. - (Higher education). - ISBN 978-5-534-05293-0.

17. Hanan Alon. Countering Palestinian Terrorism in Israel: towards a policy analysis of countermeasures; RAND Corp. 1980. 271 p.

18. Nathanson, S. Terrorism and the Ethics of War. Cambridge: Cambridge University Press. 2010. pp. 11-23.

**Для цитирования:** Медведева Д.А., Скок А.Д., Мьялина Н.Ж., Охотников И.В. Шведов Л.А., Государственное регулирование экономической устойчивости

Московский экономический журнал. № 2. 2023  
Moscow economic journal. № 2. 2023

промышленных предприятий в условиях цифровизации // Московский  
экономический журнал. 2023. № 2. URL: [https://qje.su/ekonomicheskaya-  
teoriya/moskovskij-ekonomicheskij-zhurnal-2-2023-43/](https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-2-2023-43/)

© *Медведева Д.А., Скок А. Д., Мяслина Н.Ж., Охотников И.В. Шведов  
Л.А., 2023. Московский экономический журнал, 2023, № 2.*