

Министерство образования Республики Беларусь

**УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ПИЩЕВЫХ И ХИМИЧЕСКИХ
ТЕХНОЛОГИЙ»**

**СЕВЕРО-КАВКАЗСКИЙ ИНСТИТУТ (ФИЛИАЛ) ФГБОУВО
«ВСЕРОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ЮСТИЦИИ»
(РПА МИНЮСТА РОССИИ)**

**РОСТОВСКИЙ ИНСТИТУТ (ФИЛИАЛ «ВСЕРОССИЙСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ЮСТИЦИИ»
(РПА МИНЮСТА РОССИИ)**

**Проблемы обеспечения экономической,
продовольственной и информационной безопасности
Союзного государства Беларуси и России
в современных условиях**

**Материалы
II Международной научно-практической конференции**

15–16 мая 2024 года

© Учреждение образования
«Белорусский государственный университет
пищевых и химических технологий», 2024

Научное электронное издание

Редакционная коллегия:

- Александрова Ольга Ивановна – канд. юрид. наук, доц.,
ректор ВГУЮ (РПА Минюста России);
- Киркор Максим Александрович – канд. тех. наук, доц., ректор БГУТ;
Магомедов Багавдин Магомедович – канд. юрид. наук,
проф. директор РИВГУЮ (РПА Минюста России);
- Бизенков Евгений Александрович – генеральный директор ООО «Издательский дом
«Академический», выпускающий редактор журнала «Управленческий учет»;
Магомедов Гусейн Багавдинович – канд. юрид. наук, доц.,
директор СКИВГУЮ (РПА Минюста России);
- Алибеков Шахизин Ильмуудинович – д-р. экон. наук, проф. СКИВГУЮ
(РПА Минюста России), главный научный редактор журнала «Управленческий учет»;
- Носиков Александр Степанович – канд. тех. наук, доцент, первый проректор БГУТ;
Акулич Александр Васильевич – д-р тех. наук, проф., проректор по научной работе БГУТ;
Козлова Елена Алексеевна – канд. экон. наук, доц., декан инженерно-экономического
факультета БГУТ;
- Ефименко Антонина Григорьевна – д-р. экон. наук, проф., заведующий кафедрой
экономики и организации производства БГУТ;
- Миренков Анатолий Анатольевич – канд. экон. наук, доц., заведующий кафедрой
бухгалтерского учета, анализа и аудита БГУТ;
- Никулина Марина Алексеевна – канд. философ. наук, доц., зам. директора РИ ВГУЮ
(РПА Минюста России);
- Банцевич Евгений Еживич – канд. экон. наук, доц., доцент кафедры бухгалтерского учета,
анализа и аудита БГУТ

Содержание и качество докладов являются прерогативой авторов

Проблемы обеспечения экономической, продовольственной и информационной безопасности Союзного государства Беларуси и России в современных условиях: материалы II Междунар. науч. - практ. конф., Могилев, 15–16 мая 2024 г.: Учреждение образования «Белорусский государственный университет пищевых и химических технологий»; редкол.: А.А. Миренков (отв.ред.) [и др.]. – Могилев: БГУТ, 2024. – 151с.

Сборник включает доклады участников Международной научно-практической конференции «Проблемы обеспечения экономической, продовольственной и информационной безопасности Союзного государства Беларуси и России в современных условиях», посвященной актуальным проблемам информационной и продовольственной безопасности.

Дата создания 26.08.2024. Объем 2,09 Мб. Заказ №28.

Учреждение образования
«Белорусский государственный университет пищевых
и химических технологий».
Пр-т Шмидта, 3, 212027, Могилев. <http://www.bgut.by>.

УДК 338.43

**ПРОИЗВОДСТВО МОЛОКА В РЕГИОНЕ В КОНТЕКСТЕ ПРЕДЕЛЬНОГО АНАЛИЗА
MILK PRODUCTION IN THE REGION IN THE CONTEXT OF LIMIT ANALYSIS**

Алексеева Наталья Анатольевна, ФГБОУ ВО Удмуртский ГАУ, Россия, 426069, г. Ижевск, ул. Студенческая, 11.

Alekseeva Natalya Anatolyevna, FSBEI HE Udmurt GAU, Russia, 426069, Izhevsk, st. Student, 11.

Аннотация. Рассмотрены итоги работы молочного подкомплекса АПК в Удмуртской Республике за последние годы, в том числе в сравнении с другими регионами ПФО. Отмечены положительные стороны специализации сельского хозяйства региона на молочном скотоводстве. Предложено дополнить анализ производства молока показателями предельного дохода, предельных затрат, среднего дохода и средних затрат, приходящихся на производство и реализацию 1 ц дополнительно произведенного молока. Приведены формулы для расчета показателей. Подчеркнуто значение анализа предельных величин. Выявлена динамика рекомендованных к анализу показателей за длительный анализируемый период. Обсуждены итоги расчетов предельных показателей, среди которых отмечен значительный скачок в улучшении дохода и прибыли от производства дополнительного 1 ц молока. Сделаны выводы относительно перспектив роста масштабов производства хозяйств, сумм государственной поддержки отрасли.

Ключевые слова: молоко, предельный доход, предельные затраты, центнер, сельское хозяйство, регион, себестоимость.

Abstract. The results of the work of the dairy sub-complex of the agro-industrial complex in the Udmurt Republic in recent years, including in comparison with other regions of the Volga Federal District, were considered. Positive aspects of the region's agriculture specialization in dairy cattle breeding were noted. It is proposed to supplement the analysis of milk production with indicators of marginal income, marginal costs, average income and average costs attributable to the production and sale of 1 kg of additionally produced milk. Formulas for calculating indicators are given. The importance of limit analysis is emphasized. The dynamics of indicators recommended for analysis for a long period of analysis was revealed. The results of calculations of limit indicators were discussed, among which there was a significant jump in improving income and profits from the production of additional 1 kg of milk. Conclusions were drawn regarding the prospects for growth in the scale of production of farms, the amount of state support for the industry.

Key words: milk, marginal income, marginal costs, centner, agriculture, region, cost.

Производство молока в регионах – это один из самых регулярно отслеживаемых параметров развития национальной экономики с точки зрения достижения продовольственной безопасности и один из важнейших показателей самообеспеченности региона, который задан в национальных документах стратегического планирования и нормативных документах федеральных министерств. Например, в 2022 г. в России потребление молока на душу населения составило 241 кг. По рекомендации Минздрава России рациональной нормой потребления молока и молочных продуктов считается их потребление в объеме 325 кг в год (данные за 2016 г.) [9]. В Удмуртии потребление молока и молочных продуктов составило 286 кг в год за 2022 г. или 89% от нормы [10].

Среди 14-ти регионов Приволжского федерального округа Удмуртская Республика занимала в 2018-2022 гг. третье место по производству молока (957,2 тыс. т в 2022 г., средняя продуктивность коров в 2022 г. – 7224 кг в год), несмотря на то, что по производству зерновых и зернобобовых культур, которые являются кормовой базой для крупного рогатого скота, за тот же период находилась на 11-12 месте (889 тыс. т в 2022 г.). Индексы объемов производства молока увеличивались по отношению к 2015 г. на 8,4% в 2018 г. и на 32,8% в 2022 г. И это к тому же на фоне снижения сумм государственной поддержки отрасли почти на 300 млн. руб. в 2022 г. (1164 млн. руб.) по сравнению с 2021 г. (1453 млн. руб.). Это свидетельствует о высокопродуктивном молочном скотоводстве в регионе.

Проблемам эффективного производства молока, оптимизации размеров молочных ферм, развитию рынков молочной продукции, совершенствованию форм и направлений государственной поддержки молочных подкомплексов АПК посвящены многочисленные исследования [1, 3, 6, 8, 11-15].

Нам представляется, что эффективность производства и целесообразность наращивания мощностей в региональных молочных комплексах необходимо осуществлять не только посредством структурных и динамических экономических показателей, сравнения с нормативными показателями и данными из других регионов, но и с помощью анализа предельных величин доходов и затрат, средних величин доходов и затрат на производство и реализацию молока [2, 4, 5, 7].

Предельные величины затрат показывают, на сколько изменилась полная производственная себестоимость дополнительно произведенного 1 ц молока (1).

$$MC_{t_2-t_1} = \frac{S_{полн.t_2} - S_{полн.t_1}}{Q_{произ.t_2} - Q_{произ.t_1}} \quad (1)$$

где $MC_{t_2-t_1}$ - предельные затраты на производство дополнительного 1 ц молока, руб.;

$S_{полн.t_2}$, $S_{полн.t_1}$ - полная себестоимость производства 1 ц молока в году t_2 и году t_1 ;

$Q_{произ.t_2}$, $Q_{произ.t_1}$ - количество произведенного молока в году t_2 и году t_1 , ц.

Предельный доход от производства молока показывает дополнительную выручку на 1 ц произведенного молока (2).

$$MR_{t_2-t_1} = \frac{B_{реализ.t_2} - B_{реализ.t_1}}{Q_{реализ.t_2} - Q_{реализ.t_1}} \quad (2)$$

где $MR_{t_2-t_1}$ - предельный доход от реализации дополнительного 1 ц молока, руб.;

$B_{реализ.t_2}$, $B_{реализ.t_1}$ - выручка от реализации 1 ц молока в году t_2 и году t_1 ;

$Q_{реализ.t_2}$, $Q_{реализ.t_1}$ - количество реализованного молока в году t_2 и году t_1 , ц.

Средние затраты на производство молока показывают, какова средняя полная производственная себестоимость 1 ц молока, например, за отчетный год и за предыдущий годы (3).

$$AC_{t_2-t_1} = \frac{S_{полн.t_2} + S_{полн.t_1}}{Q_{произ.t_2} + Q_{произ.t_1}} \quad (3)$$

где $AC_{t_2-t_1}$ - средние затраты на производство 1 ц молока, руб.;

$S_{полн.t_2}$, $S_{полн.t_1}$ - полная себестоимость производства 1 ц молока в году t_2 и году t_1 ;

$Q_{произ.t_2}$, $Q_{произ.t_1}$ - количество произведенного молока в году t_2 и году t_1 , ц.

Средний доход на производство молока показывает, каков средний доход, приходящийся на 1 ц молока, например, за отчетный и предыдущий годы (4).

$$AR_{t_2-t_1} = \frac{B_{реализ.t_2} + B_{реализ.t_1}}{Q_{реализ.t_2} + Q_{реализ.t_1}} \quad (4)$$

где $AR_{t_2-t_1}$ - средний доход от реализации 1 ц молока, руб.;

$B_{реализ.t_2}$, $B_{реализ.t_1}$ - выручка от реализации 1 ц молока в году t_2 и году t_1 ;

$Q_{реализ.t_2}$, $Q_{реализ.t_1}$ - количество реализованного молока в году t_2 и году t_1 , ц.

Следует заметить, что анализ предельных величин в животноводстве возможен не только по годовым данным, но по ежемесячной отчетности, если таковая имеется в распоряжении аналитика.

Поскольку в сельском хозяйстве существуют высокие риски получения доходов, при сравнении данных разных лет возможно получение отрицательных величин. По этой причине рекомендуется анализировать предельные величины затрат и доходов за более продолжительный период (табл. 1, 2).

Таблица 1 – Анализ ежегодных предельных и средних величин по производству молока в Удмуртской Республике

Годы	MC, руб. / кг	MR, руб. /кг	AC, руб. /кг	AR, руб. /кг
2015-2014	61,8	20,0	16,0	19,2
2016-2015	49,7	74,8	17,7	20,3
2017-2016	44,7	68,6	18,9	22,3
2018-2017	-0,1	-80,4	19,1	21,9
2019-2018	36,1	55,1	19,3	22,0
2020-2019	42,0	57,5	20,1	23,9
2021-2020	41,4	61,0	21,1	25,6
2022-2021	83,1	179,3	23,9	30,6

Таблица 2 – Анализ предельных и средних величин по производству молока в Удмуртской Республике нарастающим итогом

Годы	MC, руб. / кг	MR, руб. /кг	AC, руб. /кг	AR, руб. /кг
2014-2020	39,9	41,1	19,0	21,8
2014-2021	40,2	45,1	19,7	22,5
2014-2022	47,0	66,3	21,3	24,1

Ежегодная динамика предельных затрат и предельного дохода показала, что в молочном комплексе региона примерно с 2019 г. наблюдалась стабильность в производстве молока. В этот период доходы превышали расходы на дополнительно произведенное молоко на все большую величину. Рекордным стал 2022 г., в котором предельный доход больше предельных затрат на 96, 2 руб. за 1 кг молока. Средний доход за два анализируемых года также всегда превышал средние расходы, и этот разрыв увеличился особенно в 2022 г. – на 6,7 руб. за 1 кг молока (табл. 1).

Прибыльность год от года дополнительно производимого молока увеличивалась: в 2014-2020 гг. она составляла 1,2 руб. за 1 кг молока, за 2014-2022 гг. – уже 19,3 руб. за 1 кг молока (табл. 2).

Значение анализа предельных величин в том, что видна поступательная положительная динамика затрат и доходов, приходящихся всякий раз на дополнительное количество произведенного молока. Классическая кривая предельных затрат на производство молока начала свой рост с отрицательной отметки в 2019 г., и ближе к концу 2019 г. была получена нулевая предельная прибыль. В дальнейшем рост предельной прибыли от производства молока только увеличивался.

Все это свидетельствует о том, что:

- пределы роста масштабов производства в хозяйствах региона еще не достигнуты;
- средства государственной поддержки отрасли, вложенные в развитие производственной инфраструктуры сельскохозяйственных организаций, фермеров и индивидуальных предпринимателей, в цифровизацию управления, в улучшение социальных параметров жизни на селе начали приносить долгосрочную отдачу;
- в этих условиях возможна и дальнейшая оптимизация средств на государственную поддержку отрасли.

Список литературы.

1. Алексеева, Н. А. Макроэкономические параметры российской экономики в период экономических санкций / Н. А. Алексеева, О. Ю. Абашева, В. Л. Редников // *Russian Economic Bulletin*. – 2022. – Т. 5, № 3. – С. 67-74.
2. Алексеева, Н. А. Оценка уровня концентрации производства в сельскохозяйственных производственных кооперативах Удмуртской Республики / Н. А. Алексеева // *Вектор экономики*. – 2020. – № 1(43). – С. 75. – EDN VCVGDB.
3. Анализ показателей производства молока в аспекте обеспечения продовольственной безопасности России / С. В. Панасенко, Н. М. Сурай, А. Л. Таточенко [и др.] // *Молочная промышленность*. – 2022. – № 5. – С. 43-48.
4. Алексеева, Н. А. Сравнительный анализ затрат на производство зерна, молока и приростов крупного рогатого скота на примере Удмуртской Республики (Россия) / Н. А. Алексеева // *Тенденции экономического развития в XXI веке : Материалы IV Международной научно-практической конференции, Минск, 01 марта 2022 года*. – Минск: Белорусский государственный университет, 2022. – С. 139-141.
5. Алексеева, Н. А. Предельные и средние издержки в производстве молока / Н. А. Алексеева, В. А. Соколов // *Управление эффективностью и безопасностью деятельности хозяйствующих субъектов и публичных образований : Материалы Международной научно-практической конференции, посвященной памяти заслуженного экономиста Российской Федерации, д.э.н., профессора М.И. Шишкина , Ижевск, 25 января 2022 года*. – Ижевск: Общество с ограниченной ответственностью "Издательство "Шелест", 2022. – С. 474-477.
6. Дозорова, Т. А. Оценка размещения и концентрации производства молока в регионе / Т. А. Дозорова, Н. А. Утьманова // *Экономика сельского хозяйства России*. – 2021. – № 5. – С. 87-92.
7. Инструментарий предельных величин в анализе сельскохозяйственного производства / Н. А. Алексеева, О. А. Тарасова, З. А. Миронова, Е. В. Александрова // *Конкурентоспособность в глобальном мире: экономика, наука, технологии*. – 2022. – № 2. – С. 5-7.
8. Колесников, А. В. Оценка эффективности производства молока в Белгородской области / А. В. Колесников, И. А. Зигаева // *АПК: экономика, управление*. – 2021. – № 4. – С. 57-66.
9. Минздрав РФ: норма потребления молочной продукции – 325 кг на человека в год. – URL: https://milknews.ru/index/Minzdrav_RF_norma_potreblenija_molochnoj_produkcii_325_kg_na_cheloveka_v_god.html?ysclid=lvn2y64wvo371298111 (дата обращения 20.04.2024 г.
10. Приволжский федеральный округ. Удмуртская Республика. – URL: <https://data.milknews.ru/regions/udmurtiya?ysclid=lvn37rogec229714570> (дата обращения 20.04. 2024 г.
11. Старкова, О. Я. Проблемы развития производства молока в Российской Федерации / О. Я. Старкова // *Экономика сельского хозяйства России*. – 2022. – № 3. – С. 75-78.
12. Столяров, Г. Оценка эффективности производства молока в современных условиях / Г. Столяров // *Аграрная экономика*. – 2020. – № 4(299). – С. 66-72.
13. Соколов, О. В. Экономическая эффективность производства молока: факторы, состояние и направления роста / О. В. Соколов, О. В. Саблин, М. А. Рогов // *Наука и Образование*. – 2020. – Т. 3, № 4. – С. 415.
14. Тенденции и перспективы развития производства молока / Н. Р. Александрова, А. К. Субаева, Л. М. Мавлиева, Н. Л. Титов // *Вестник Казанского государственного аграрного университета*. – 2020. – Т. 15, № 1(57). – С. 94-98. – DOI 10.12737/2073-0462-2020-94-98. – EDN VUZIFL.
15. Цыпин, А. П. Производство молока как фактор обеспечения продовольственной безопасности Оренбургской области / А. П. Цыпин, М. М. Шайлиева // *Наука и Образование*. – 2020. – Т. 3, № 3. – С. 123.

СОСТОЯНИЕ МИРОВОГО РЫНКА ПИЩЕВОЙ ПРОМЫШЛЕННОСТИ И ЕГО ВЛИЯНИЕ НА ПРОДОВОЛЬСТВЕННУЮ БЕЗОПАСНОСТЬ КАЗАХСТАНА

Ахметова А.А., Кожахметова А.Г., Мажитова Б.Б.
Казахстан, г.Астана, Евразийский гуманитарный
институт им. Кусайнова А.К., ул.Жумабаева 4
Akhmetova A.A., Kozhakhmetova A.G., Mazhitova B.B.
Kazakhstan, Astana, Eurasian Humanitarian
Institute named after A.K. Kusainov, Jumabaeva st.4

Аннотация. В современных условиях наиважнейшей стратегической задачей в жизнедеятельности любого государства является обеспечение национальной безопасности, в частности продовольственной. Понятие «национальная безопасность» включает в себя защищенность человека, общества и государства от внутренних и внешних угроз. Данные угрозы нарушают конституционные права, свободы, качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие страны, обороны и безопасности государства. Одним из важных направлений национальной безопасности является обеспечение продовольственной безопасности. В статье представлены теоретические и аналитические результаты исследования мирового рынка пищевой промышленности, развития сельского хозяйства РК, агропромышленного комплекса. Особое внимание уделено анализу современного состояния отраслей отечественного агропромышленного комплекса, выявлены проблемы и представлены пути решения данных проблем. Проведен сравнительный анализ состояния сельского хозяйства среди стран Центральной Азии.
Ключевые слова: мировая экономика, пищевая промышленность, сфера услуг, сельское хозяйство, продовольственная безопасность.

Abstract. In modern conditions, the most important strategic task in the life of any state is to ensure national security, in particular food security. The concept of “national security” includes the protection of individuals, society and the state from internal and external threats. These threats violate constitutional rights, freedoms, quality and standard of living of citizens, sovereignty, territorial integrity and sustainable development of the country, defense and security of the state. One of the important areas of national security is ensuring food security. The article presents the theoretical and analytical results of the study of the world market of the food industry, the development of agriculture in the Republic of Kazakhstan, the agro-industrial complex. Particular attention is paid to the analysis of the current state of the branches of the domestic agro-industrial complex, problems are identified and ways to solve the countries of Central Asia has been carried out.

Key words: world economy, food industry, service sector, agriculture, food security.

Главным фактором устойчивости государства в мировом обществе в социально-экономическом направлении является продовольственная безопасность. Она служит необходимым материальным условием жизни человека, группы людей и общества в целом, реализуя функции и возможности для политического, социально-экономического, демографического, культурного и интеллектуального развития. Спектр специфических проявлений продовольственной проблемы достаточно широк: от временного недостатка определенных продуктов до голода, от локализации части государства до международных масштабов [1].

В условиях глобализации цель всемирной продовольственной безопасности, как системы состоит в борьбе с голодом, в обеспечении мирового сообщества продуктами питания, постоянным расширением ассортимента, повышения качества посредством создания благоприятных экономических условий и привлечения соответствующих ресурсов. Процессы глобализации, которые развивались в последние десятилетия, оказали значительное влияние на ситуацию в агропромышленном комплексе развитых и развивающихся стран.

В настоящее время проблема продовольственной безопасности любой страны стоит очень остро и задача экономической науки, рассматривая данные вопросы необходимо представить пути решения

данных вопросов и применения их на практике. Так казахстанские ученые в лице Ахметовой К.А., Есполова Т.И., Накиповой Г.Н. и др. в своих работах рассматривают состояние агропромышленного комплекса Казахстана и дают ему оценку, а также предложения по его модернизации. Обращаясь к трудам зарубежных авторов, как Алтухов В.А., Серов Е.В., Дюрфельд Г. мировых агентств, Всемирного банка, АБР можно адаптировать опыт зарубежных стран в области развития и эффективности сельского хозяйства и АПК.

Мировая экономика представляет собой совокупность национальных хозяйств. Глобализация отражается на экономике стран-производителей зерновых и масличных культур, когда неурожай провоцирует изменение ценовой ситуации на сельскохозяйственных и продовольственных рынках. Увеличение мировых цен на зерно привел к росту цен на жизненно необходимые продукты питания: хлеб, яйца, мясо и молочные продукты, растительное масло и т.д. Для государств важным является постоянный анализ проблем обеспечения продовольственной безопасности, как на государственном, так и на региональном уровнях.

Структура и состояние отдельно взятого хозяйства страны зависит от многих факторов. Также, влияет уровень развития самого государства, природные условия и ресурсы, другие внешние причины. На сегодняшний день выделяют три сектора экономики: промышленность, сфера услуг и сельское хозяйство. Каждый сектор состоит из множества отраслей. Развитие легкой и пищевой промышленности имеет важное значения для населения.

Пищевая промышленность непосредственно связана с сельским хозяйством и является неотъемлемой частью агропромышленного комплексного государства. Производство продуктов питания напрямую влияет на решение продовольственной проблемы человечества. Данная отрасль присутствует во всех странах мира, однако резко отличается не только по уровню своего развития, где безусловное лидерство принадлежит экономически развитым странам, но и по её международной специализации.

Согласно прогнозам мировых экспертов, совокупное потребление сельскохозяйственной продукции в мире к 2050 году повысится на 69 %, а рост населения с 7 до 9 млрд. человек [2]. Основной прирост придется на азиатский регион: Китай, Индонезию, Филиппины, Пакистан и Индию, которая станет самой густонаселенной страной. Китай при этом является самой ближайшей страной для Казахстана, а Пакистан и Индия находятся на границе со странами Центральной Азии. На 70% придется увеличить производственный потенциал сельскохозяйственным компаниям, чтобы удовлетворить имеющийся спрос (в быстро развивающихся странах – почти на 100 %). Для этого агропромышленные компании должны будут радикально изменить методы производства и повысить эффективность своей деятельности. Ожидается, что к 2024 году рынок пищевой промышленности достигнет примерно 4,1 триллиона долларов США при среднегодовом темпе роста 4,3% с 2021 по 2024 год. Основными драйверами этого рынка являются растущий спрос на готовые к употреблению пищевые продукты, изменение образа жизни и рост потребления со стороны малых семей и работающих женщин. Согласно, исследованиям Всемирного Банка, «Горячие точки» продовольственной безопасности, географические районы, подвергающиеся наибольшему риску, кризисов отсутствия продовольственной безопасности, в ближайшие время сосредоточены в 12 странах: Афганистан, Буркина-Фасо, Демократическая Республика Конго, Эфиопия, Гаити, Нигер, Нигерия, Сомали, Южный Судан, Судан, Йемен и Зимбабве. Все эти страны, кроме одной, включены в список уязвимых и конфликтных ситуаций (FCS) Всемирного банка [3].

Сельское хозяйство в настоящее время сталкивается с растущей трудностью удовлетворения многих из наших самых необходимых потребностей, подвергаясь при этом новым рискам. Первичные потребности – от продовольствия до сырья и энергии – растут по всему миру по мере увеличения численности населения и доходов, изменения образа жизни и резкого роста потребления. Сельскому хозяйству стало сложнее удовлетворять эти потребности. Климат меняется, ресурсы истощаются, а сельское хозяйство с каждым годом сталкивается с более острой конкуренцией за землю и воду. Мировая торговля растениями и животными подвергла сельское хозяйство и основные производимые запасы, угрозе распространения вредных организмов и болезней, которые они могут переноситься по всей территории мирового сообщества.

Проблема голода существовала всегда, но пандемия COVID-19 усугубила данную ситуацию: по оценкам ФАО, число недоедающих увеличилось с 624 миллионов человек в 2014 году до 688 миллионов в 2021 году. Движущие силы, лежащие в основе этой тенденции, включают экстремальные климатические явления, конфликты и другие потрясения для экономических возможностей. Так, вспышка саранчи усугубляет этот кризис в 23 странах, и другие зоозоны представляют постоянную угрозу [4]. Мировые эпидемии, потрясения для здоровья человека и социально-экономические результаты пандемии коронавирусной болезни (COVID-19), голод привлекли интерес к необходимости управления данными возможностями и их минимизации. Поскольку озабоченность по поводу стабильности и повышенной уязвимости из-за перемещения товаров и мобильности населения увеличивается, необходимо также усилить сопротивляемость вредителям и болезням, и увязать данные меры с зеленой экономикой.

Развитие и расположение пищевой отрасли определяются размещением населения и сельскохозяйственного производства. Наибольшее развитие отрасль получила в районах высокой концентрации населения и крупного сельскохозяйственного производства. Крупнейшими отраслями пищевой промышленности являются плодоовощная, мясная, молочная, рыбная.

В таблице 1 представлена доля сельского хозяйства в пяти странах Центральной Азии, показывающая, роль сельского хозяйства в экономиках этих стран.

Таблица 1–Доля сельского хозяйства в экономике стран Центральной Азии за 2021 год(%)

Страны	Доля сельского хозяйства в ВВП	Доля сельского хозяйства в занятости	Доля сельского хозяйства в стоимости экспорта
Казахстан	4,5	15,8	5,9
Узбекистан	28	23,9	13,5
Туркменистан	9,3	19,9	1,1
Кыргызстан	12,1	21,2	14,7
Таджикистан	20,9	44,9	15,6

Анализ таблицы 1 показывает, что доля сельского хозяйства в таких странах как Узбекистан, Таджикистан, Кыргызстан занимает преобладающее место в экономиках государств (28%, 20,9% и 12,1% соответственно). Так же можно отметить, что наибольшая доля занятости в сельском хозяйстве отмечается в Таджикистане -44,9%. Это говорит о том, что страны независимо от территориального расположения являются аграрными странами. Анализируя экспортную составляющую, наименьшая доля составляет у Туркменистана 1,1%, это связано с закрытостью экономики данной страны. Доля экспорта соответствующая доли сельского хозяйства к ВВП в таких странах как Узбекистан, Таджикистан и Кыргызстан составляет 13,5 %, 15,6% и 14,7% соответственно, это говорит о том, что в этих странах развитие сельского хозяйства на должном уровне, и они занимаются экспортом сельскохозяйственной продукцией, что положительно сказывается на отрасли и экономике в целом.

К сожалению, казахстанское сельское хозяйство занимает очень маленькую долю в ВВП экономики страны и соответственно экспорт составляет незначительную долю.

Узбекистан является основным экспортером фруктов и овощей в Центральной Азии с объемом 606,5 млн. долларов США. Основной экспортный регион в Узбекистане находится в северной части страны, которая граничит с Казахстаном.

Анализируя экспорт и импорт Казахстана, можно отметить, что экспорт продуктов животного и растительного происхождения, т.е. продукция сельского хозяйства, составляет всего лишь 8,3% от общего объема экспорта товаров. В импорте наибольшее увеличение отмечено по пшенице и масличных культур – рост в 1,7 раза. Все это показывает, что сельскому хозяйству Казахстан есть

куда стремиться и над чем работать, т.е. Правительству необходимо активизировать работу в этом направлении.

Однако, несмотря на положение экспорта продукции сельского хозяйства внутреннее производство овощей в разрезе регионов страны показывает рост за 2020-2022 годы (таблица 2). Общее производство свежих фруктов и овощей в Казахстане в 2020 году составило приблизительно 10,3 млн. тонн, несмотря на то, что нет точной статистики сельскохозяйственного производства для большинства сельскохозяйственных культур, особенно фруктов и овощей. Производство овощей в Казахстане сосредоточено в основном в Алматинской (24,3%), Туркестанской (24,0%) и Жамбылской областях (20,8%), чья совокупная доля составляет около 69% от общего производства овощей в стране. Около 68% картофеля производится в 5 регионах Казахстана: Алматинской (19,3%), СКО (15,5%), Павлодарской (12,6%), ВКО (11,2%) и Карагандинской областях (9,4%). Более 80% дынь выращивается в трех южных регионах страны: Туркестанской (60,2%), Жамбылской (14,1%) и Кызылординской областях (6,8%). Около 97% всех сортов винограда производится в Туркестанской (75%), Алматинской областях (19%) и в г. Шымкент (3%); и 87% всех фруктов производится в 3 регионах: Туркестанской области (39,5%), Алматинской области (37,8%) и Жамбылской области (9,5%). Две трети (68%) ягод и других фруктов в Казахстане производятся в 5 регионах страны: ВКО (19,8%), СКО (18,4%), Алматинской области (11,8%), Актюбинской области (10,4%) и Карагандинской области (7,5%) [7].

Таблица 2- Производство овощей в разрезе регионов РК в 2020-2022 гг., млн. тг

Овощи, тыс. тонн	2020	2021	2022	Динамика 2022 к 2020 г. (%)
1	2	3	4	5
Алматинская	993,1	995,4	1032,6	104
Туркестанская	981,1	1095,6	1144,4	116,6
Жамбылская	847,3	976,9	1067,8	126,0
ВКО	259,1	241,5	269,9	104,2
СКО	207,8	203,7	204,3	98,3(-)
Павлодарская	200,2	226,3	256,7	128,2
Другие регионы	593,3	615,8	615,2	103,7
Всего	4 081,9	43255,2	4590,9	112,5
Картофель, тыс. тонн				
Алматинская	732,9	757,8	785,8	107,2
СКО	590,0	605,5	592,3	100,4
Павлодарская	478,9	513,1	545,6	113,9
ВКО	427,7	425,3	435,8	101,9
Карагандинская	357,9	381,7	392,6	109,7
Другие регионы	1 219,6	1228,7	1254,7	102,9
Всего	3 807,0	3912,1	4006,8	105,2
Бахчевые, тыс. тонн				
Туркестанская	1 290,8	1375,5	1420,0	110,0
Жамбылская	302,2	374,6	408,3	135,1
Кызылординская	144,7	148,8	155,2	107,2
Алматинская	118,1	120,6	112,2	95,0(-)
ВКО	119,2	181,0	149,9	125,7
Другие регионы	167,5	181,6	178,5	106,6
Всего	2 142,5	2382,1	2425,1	113,2
Виноград, тыс. тонн				
Туркестанская	66,2	67,8	72,5	109,5
Алматинская	16,9	17,8	17,9	105,9
г. Шымкент	2,6	2,1	1,9	73,1(-)
Другие регионы	2,8	2,7	2,8	100
Всего	88,5	90,4	95,1	107,5

Продолжение таблицы

1	2	3	4	5
Фрукты, тыс. тонн				
Туркестанская	110,3	108,5	131,3	119,0
Алматинская	105,7	108,8	130,3	123,3
Жамбылская	26,4	26,8	26,9	101,9
ВКО	10,2	10,1	10,0	98,0(-)
г. Шымкент	5,8	4,0	5,1	87,9 (-)
Другие регионы	20,9	20,5	21,3	101,9
Всего	279,3	278,7	324,9	116,3
Ягоды и другие фрукты, тыс. тонн				
ВКО	4,2	4,5	4,5	107,1
СКО	3,9	3,9	3,9	100
Алматинская	2,5	2,8	2,9	116
Актюбинская	2,2	2,1	2,1	95,5
Карагандинская	1,6	1,6	1,6	100
Другие регионы	6,8	11,9	11,9	175
Всего	21,2	22,3	22,4	105,7

В разрезе регионов по овощам выделилась Туркестанская, Жамбылская и Павлодарская области, рост отмечается за три года на 16, 26, 28 % соответственно. В секторах, включающие производство бахчевых, с 2020 года отмечается темп роста в Туркестанской, Жамбылской и Кызылординской на 10, 35, 7 % соответственно. В Средний рост по видам продукции значительно варьируется по фруктам, от 1% до 23%. По фруктам наибольший рост за три года отмечается в таких областях как Алматинская, Туркестанская и Жамбылская 23%, 19%, 1% соответственно [8].

Пищевая промышленность Казахстана в основном представлена следующими секторами: производство муки, хлебобулочных изделий, мясной продукции, молочной, рыбной, масложировой, переработкой фруктов и овощей, производством сахара, кондитерских изделий, производством полуфабрикатов, алкогольных и безалкогольных напитков, табака и сигарет (табл.3).

Таблица 3 - Количество предприятий пищевой промышленности в разрезе производителей продуктов питания и продукции переработки в 2020-2022 гг. (единиц)

Наименование	2020	2021	2022	2021	Динамика 2021/2020 %
Пищевая промышленность	1 748	1 784	1778	1 828	104
Обработка и консервирование мяса и мясных продуктов	346	395	495	448	129
Обработка и консервирование рыбы, ракообразных и моллюсков	72	74	79	81	112,5
Обработка и консервирование фруктов и овощей	53	54	49	52	98
Производство растительных и животных масел и жиров	56	66	62	63	112,5
Производство молочных продуктов	222	223	229	227	102
Производство продуктов мукомольной промышленности, крахмалов и крахмальных продуктов	309	284	282	252	81,5
Производство хлеба и хлебобулочных изделий	452	447	420	448	99
Производство прочих пищевых продуктов	173	188	187	184	106

Наименование	2020	2021	2022	2021	Динамика 2021/2020 %
Производство готовых кормов для животных	65	70	75	73	112
Производство напитков	200	204	221	226	113
Производство табачных изделий	3	2	2	2	67

Так, анализируя количество предприятий пищевой промышленности можно сделать вывод, общее количество предприятий имеет незначительный рост за 2021-2020 годы на 4%. В в 2021 году разрезе предприятий наибольшее количество отмечается в таких отраслях как производство хлебобулочных и мучных изделий 448 предприятий, на втором месте производство продуктов мукомольной промышленности, крахмалов и крахмальных продуктов 252 предприятий, на третьем месте производство молочных продуктов 227. За период 2020-2021 годов отмечается снижение предприятий на 29 %.

Шымкент производит около 10% всего объема продукции пищевой промышленности страны, Туркестанская область — около 30%. В целом, объем валовой продукции сельского хозяйства Туркестанской области за январь–декабрь 2022 года составил 729,7 млрд. тенге, что на 5,1% больше уровня прошлого года. В том числе продукция растениеводства, соответственно 422,8 млрд. тенге (106,0%), продукция животноводства – 303,3 млрд. тенге (104,0%) (за январь–декабрь 2021 г. ИФО – 104,7%). Во всех категориях хозяйств области выполнено 239,9 тыс. тонн мяса (104,3%) (в живом весе), произведено 748,3 тыс. тонн молока (103,6%), 216,4 млн. штук яиц (114,9%). В производстве продуктов питания (ИФО 98,4%) в Туркестанской области по сравнению с 2021 годом уменьшено выпуск молока на 19,0% и производство хлеба на 0,9%. В отрасли производство текстильных изделий (ИФО 116,1% раза) увеличился спрос на волокно хлопковое изделие на 18,2%, а на белье постельное уменьшился на 57,6%.

В результате производство продуктов питания в республике выросло на 4,2%, в том числе растительного масла на 51%, сахара на 46%, крупы на 18%, рыбы (свежей, охлажденной и мороженой) на 18%, муки на 11%, переработанного риса на 5,5%, колбасных изделий на 5,4%, макарон на 4,5%.[9]

Основными системными проблемами, характерными для всех отраслей сельского хозяйства, пищевой и перерабатывающей промышленности, являются:

- 1.нехватка сельскохозяйственного сырья с определенными качественными характеристиками для промышленной переработки;
- 2.сельскохозяйственный сектор характеризуется низким уровнем производительности земельных и трудовых ресурсов, низкой урожайностью, значительно отстающей от мировых показателей,
- 3.физический износ технологического оборудования;
- 4.недостаточная база знаний и компетенций для фермеров и местных торговцев;
5. отсутствие информационной системы и торговых площадок;
- 6.низкий уровень конкурентоспособности производителей продуктов питания на внутреннем и внешнем продовольственных рынках;
- 7.неразвитая инфраструктура хранения, транспортировки и логистики продуктов питания;
8. низкий уровень инвестиций как государственных, так и частных в сельское хозяйство и пищевую промышленность;
9. низкий уровень социализации, инфраструктуры в сельской местности;
- 10.некачественные дороги, высокие цены на ГСМ, дальность сельхозпроизводителей от перерабатывающих предприятий отсюда и вытекает высокое ценообразование на логистические услуги[10].

Для решения вышеназванных системных проблем необходимо проводить целенаправленные мероприятия в рамках государственной программы развития сельского хозяйства, программы Национальной безопасности и других стратегических программ.

В рамках данных мероприятий необходимо пересмотреть роль сельхозпроизводителя, фермера. Ориентированная на фермера, то есть фермер должен стать центральным звеном в экосистеме новой

модели сельского хозяйства. Модель услуг, предусматривающая смещение акцента государственной поддержки в пользу мелких и средних фермеров (в отличие от традиционной ориентированности на крупные сельскохозяйственные предприятия), являющихся главной целевой группой государственных мер по развитию.

Следующий момент улучшения сельского хозяйства. Это повышение потенциала сельского хозяйства в Казахстане. Страна занимает пятое место в мире по площади сельскохозяйственных земель (почти 25 миллионов гектар пахотных земель и более 70 миллионов гектар пастбищных угодий, из которых в настоящее время используется всего лишь 30 процентов); обладает достаточно большими водными ресурсами (подземными, речными и тальными водами), относительно чистой природной производственной базой (по сравнению с некоторыми крупными и аграрными странами), создающей возможности для производства высококачественной продукции; характеризуется близостью к крупным рынкам; и существенными растущими инвестициями в транспортные/торговые коридоры. Таким образом, имея такой потенциал, используется не в полном масштабе сельхозпроизводителями, что сказывается на качестве продукции, цене и главное на экологии Казахстана.

Одним из немаловажных показателей, которые необходимо улучшать – это показатели производительности отрасли. В настоящее время сильно отстают от ее потенциала, что объясняется множеством факторов. В целом, сельскохозяйственный сектор характеризуется низким уровнем производительности земельных и трудовых ресурсов, низкой урожайностью, значительно отступающей от мировых показателей, недостаточным использованием современных ресурсов и систем производства, неэффективными услугами государственной поддержки, низким уровнем инвестиций в инфраструктуру цепочки добавленной стоимости и недостаточным уровнем государственных инвестиций в переработку и маркетинг сельскохозяйственной продукции. Эти недостатки отражаются и на природных ресурсах, в частности в виде деградации земельных ресурсов, выбросов парниковых газов (ПГ) и истощения водных ресурсов.

Еще одна важная проблема сельского хозяйства Казахстана – это миграция населения. В последнее время наблюдается сильный отток населения из села, особенно молодежи. Это связано с тем, что на селе нет комфортных условий жизни, нет интернета, нет дорог, нет социальной обеспеченности, нет услуг, повышающих качество жизни. Эту проблему необходимо решать через субсидии государства, обеспечения сел водой, дорогами, проведения высокоскоростного интернета, доступность цифровых услуг и элементарно бытовыми условиями жизни.

Таким образом, мы выделили некоторые проблемы в развитии сельского хозяйства Казахстана, влияния мирового рынка пищевой промышленности, отечественной продовольственной безопасности, которые требуют незамедлительного решения в первую очередь со стороны государства и потом уже на местах. Решение этих вопросов снимет насущную угрозу продовольственной безопасности в Казахстане, повысит обеспеченность собственными продуктами питания и другой сельскохозяйственной продукции, выведет отечественных сельхозпроизводителей на новый более качественный уровень и наша продукция сможет конкурировать на мировых пищевых площадках.

Список литературы

1. Габуниа Н.Г., Корелин К.В. Экономическая безопасность предприятия и управление рисками // Известия Санкт-Петербургского государственного экономического университета. – 2016. – № 4 (94), С. 79-81.
2. Юрасов И. А., Бондаренко В. В., Юдина В. А., Кузнецова Т. А. Корпоративная социальная ответственность. – М.: Инфра-М, 2015. – 234 с.
3. Митина И.А., Салтанова Т.А., Чельшева Э.А. Проблемы регулирования развития агропромышленного комплекса национальной экономики в контексте экономической безопасности // Вестник Евразийской науки, 2022, no. 5. Доступно: <https://esj.today/PDF/57ECVN520.pdf> (дата обращения: 05.05.2023).

4. Официальная статистическая информация Комитета по статистике Министерства национальной экономики Республики Казахстан [Электронный ресурс]. – 2020. – URL: <https://stat.gov.kz/official/industry/151/statistic/6> (дата обращения: 18.01.2023).
5. Сельское хозяйство, Лесное хозяйство и Рыболовство в РК. Комитет статистики МНЭ РК, 2016-2022. Таблица 3.59-3.68, стр. 105-116.
6. Промышленность Казахстана и его регионов 2014-2020гг
7. Официальная статистическая информация Комитет по статистике Министерства национальной экономики Республики Казахстан [Электронный ресурс]. – 2021. – URL: Внешняя торговля Республики Казахстан // <https://stat.gov.kz/official/industry/31/publication> (дата обращения: 18.01.2023).
8. Алтухов А.И. Продовольственная безопасность в контексте реализации новой редакции ее доктрины // Вестник Курской государственной сельскохозяйственной академии, 2022, по. 9, с. 82-89.
9. Кайгородцев А. А. Продовольственная безопасность Казахстана: оценка состояния и пути обеспечения // Большая Евразия: Развитие, безопасность, сотрудничество. Экономика и бизнес. – 2021. – No 2(1). – С. 51-54.
10. Артемова Е.И., Плотникова Е.В. Государственное регулирование и поддержка развития АПК – условие продовольственного суверенитета страны // Естественно-гуманитарные исследования, 2021, по. 3(35), с. 38-43.

УДК 519.876.5

РОЛЬ ЦИФРОВОЙ ГРАМОТНОСТИ ЭКОНОМИЧЕСКОМ РАЗВИТИИ КАЗАХСТАНА (на примере Актюбинской области)
THE ROLE OF DIGITAL LITERACY IN THE ECONOMIC DEVELOPMENT OF KAZAKHSTAN (on the example of Aktobe region)

Адай.А.С., Кенесова.А.М., Тегисбаева Д.Г.
Актюбинский региональный университет имени К. Жубанова
г.Актобе., Казахстан
Научный руководитель: Кусаинов.Х.Х., Жунусов.Б.А.
Aday.A.S., Kenesova.A.M., Tegisbayeva D.G.
Aktobe Regional University named after K. Zhubanov.
Aktobe, Kazakhstan
Supervisor: Kusainov.H.H., Zhunusov.B.A.

Аннотация: В данной статье анализируется важность цифровой грамотности для экономического развития в Казахстане. Обсуждаются экономические выгоды повышения уровня грамотности населения и его влияние на различные сферы экономики. Особое внимание уделяется тому, как повышение грамотности может способствовать уменьшению социального и экономического неравенства в стране.

Ключевые слова: Цифровые технологии, экономическое развитие, интеграция, государственные программы, грамотность, цифровизация.

Abstract: This article analyses the importance of digital literacy for economic development in Kazakhstan. The economic benefits of improving the literacy level of the population and its impact on various spheres of the economy are discussed. Particular attention is paid to how improving literacy can help reduce social and economic inequality in the country.

Keywords: Digital technologies, economic development, integration, government programs, literacy, digitalization.

В современном мире грамотность играет ключевую роль в формировании инклюзивного общества и экономики. В Казахстане правительство активно содействует программам по повышению уровня грамотности населения, признавая важность этого фактора для устойчивого экономического развития. В данной статье мы проанализируем экономическую эффективность таких программ и их роль в инклюзивном экономическом развитии страны.

Программы по повышению грамотности в Казахстане имеют потенциал значительно повысить экономическую эффективность страны. Увеличение числа грамотных работников способствует улучшению производительности труда, что ведет к росту ВВП. Кроме того, грамотные граждане имеют больше возможностей для доступа к высокооплачиваемым работам и предпринимательской деятельности, что способствует увеличению доходов населения и снижению уровня бедности.

Повышение уровня грамотности также играет важную роль в инклюзивном экономическом развитии. Грамотность обеспечивает людям доступ к образованию, информации и технологиям, что помогает им активно участвовать в экономической жизни страны. Это способствует уменьшению социального и экономического неравенства, поскольку дает возможность даже самым уязвимым группам населения получить доступ к ресурсам и возможностям для саморазвития и самореализации.

Дальнейшее развитие программ по повышению грамотности в Казахстане представляет собой перспективное направление для улучшения качества жизни граждан и достижения целей устойчивого развития. Важно обеспечить доступность образования и обучения для всех слоев населения, в том числе для детей с особыми образовательными потребностями и мигрантов. Также необходимо активно привлекать частный сектор и международные партнеры для поддержки программ грамотности и обеспечения их устойчивости и эффективности.[1].

Цифровые технологии имеют огромное влияние на экономическую и продовольственную

безопасность государств. Вот некоторые из основных аспектов этого воздействия:

1. Экономическая эффективность: Цифровые технологии позволяют оптимизировать процессы производства, управления ресурсами и логистики. Это увеличивает производительность труда и позволяет экономить ресурсы, что в конечном итоге способствует экономическому росту.

2. Улучшение доступа к рынкам: Цифровизация содействует доступу к глобальным рынкам. Онлайн-платформы и электронная коммерция позволяют компаниям проникать на новые рынки за пределами своих национальных границ, что способствует диверсификации экономики и снижению зависимости от отдельных рынков.

3. Улучшенное управление цепями поставок: Цифровые технологии, такие как интернет вещей (ИТ), блокчейн и искусственный интеллект (ИИ), позволяют более эффективно отслеживать и управлять цепями поставок, что способствует сокращению времени доставки, улучшению качества продуктов и снижению издержек.

4. Повышение устойчивости к кризисам: Цифровые технологии могут улучшить способность государств и компаний реагировать на экономические и продовольственные кризисы. Аналитика данных и прогностические модели позволяют предвидеть и адаптироваться к изменениям в рыночных условиях быстрее и эффективнее.

5. Повышение продовольственной безопасности: Цифровые инновации могут улучшить производственные процессы в сельском хозяйстве, включая автоматизацию, мониторинг почвы и климата, и оптимизацию использования ресурсов, таких как вода и удобрения. Это может повысить урожайность и снизить потери урожая из-за плохих погодных условий или болезней.

Цифровизация – это повсеместное внедрение цифровых технологий в разные сферы жизни, таких как промышленность, экономика, образование, культура, обслуживание и т.п.

Цифровизация всех сфер жизни и экономики Казахстана – это возможность занять передовые позиции на мировой арене, а также улучшить качество жизни граждан и создать благоприятные условия развития предпринимательства.[2].

Одной из цели цифровизации является обеспечение прозрачности и искоренение бюрократии и коррупционных правонарушений путем оптимизации бизнес-процессов и минимизацией участия человеческих факторов при оказании государственных услуг. Внедрение цифровизации осуществляется на основе Государственной программы «Цифровой Казахстан».

Государственная программа «Цифровой Казахстан» – это важная комплексная программа, которая нацелена на повышение уровня жизни каждого жителя области за счет использования цифровых технологий.

Одним из основных направлений программы ГП РК «Цифровой Казахстан» является – переход к цифровому государству, в рамках которого реализуется ряд цифровых инициатив, в том числе «Создание ситуационного центра акимата Актюбинской области».

Ситуационный центр акимата Актюбинской области (далее – СЦ) создан с целью повышения эффективности деятельности местных исполнительных органов на основе использования современных информационно-коммуникационных технологий в деятельности.

Для оперативной и эффективной деятельности Ситуационного центра реализована Служба 109 с полноценным интеллектуальным интерфейсом, позволяющая быстро обрабатывать обращения.

Из общего количества зарегистрированных обращений 10 836 (доля 93%) на сегодня завершены 10 043 с предоставлением ответов и решений, на рассмотрении остаётся 793 обращений.

109 является одним из шагов к масштабной цифровизации региона. Центр оказывает всестороннюю работу по обеспечению бытовых условий населения, занятости, здравоохранения, чрезвычайных ситуаций, пассажирского транспорта и дорожной инфраструктуры, правонарушений и других вопросов, возникающих у граждан. Напомним, что квалифицированные специалисты не только качественно работают в сфере цифровизации, но и оперативно реагируют на социально значимые вопросы, которые активно обсуждаются среди населения. Информационная площадка, объединяющая несколько модулей, является эффективной и доступной для населения. В частности, можно связаться со Службой 109 несколькими способами:

- Бесплатный звонок по территории области на номер 109;
- Instagramopen.aqtobe;
- whatsApp номер +7 7132 90 96 05.

Жители могут в любое время обратиться в 109 (текст, фото, видео, сообщение), выбрав наиболее удобный способ обращений.

Дополнительно к ситуационному центру имеется Информационно–аналитическая система мониторинга индикаторов развития Актюбинской области, которая включает в себя 10 модулей и содержит данные по основным показателям области. Анализируя большие данные по ключевым сферам (от безопасности до бюджета региона), и на основе этого можно делать объективный вывод, насколько ситуация в той или иной сфере является стабильной и как на нее влияют мероприятия, проводимые государственными органами. Имеется частичная интеграция с ИС государственных органов.

Также, действует мобильное приложение Open Aqtobe с целью оцифровки процессов взаимодействия населения с государственными органами, легкого обращения в государственные органы с жалобами и предложениями. Платформа мобильного приложения предоставляет жителям области/района/города бесплатно пользоваться онлайн–сервисами и мгновенно получать самую актуальную и нужную информацию, не выходя из дома, благодаря смартфону.

На данный момент ведется интеграция со службой 109, для прямого взаимодействия населения области с областными государственными органами.

Вместе с этим, совместно с Управлением автомобильных дорог и пассажирского транспорта и Актюбинским областным филиалом КазАвтоЖол ведутся работы по интеграции GPS трекеров, установленных на технике зимнего содержания автодорог, с Ситуационным центром. Это позволит нам не только отслеживать маршруты передвижения техники, но и оперативно среагировать в случае непредвиденных обстоятельств и направить ближайшую технику в зону бедствия.

Для прозрачности работ в сфере ЖКХ совместно с Адалдык аланы был внедрен программно–аппаратный комплекс «Система управления, учета и мониторинга работ» с заданными функциональными возможностями.

В рамках государственной программы «Цифровой Казахстан» действует геопортал г. Актобе в целях оказания государственных услуг населению. Посредством геопортала автоматизирована

10 основных государственных услуг в сфере архитектуры и земельных отношений. Таким образом жители города Актобе, не выходя из дома, посредством личного ЭЦП могут получать следующие услуги через свой личный кабинет:

1. Выдача решения на изменение целевого назначения земельного участка;
2. Разделение земельного участка;
3. Постановка на очередь по получению земельного участка;
4. Продление аренды земельного участка;
5. Предоставление земельного участка в частную собственность;
6. Уточнение границ земельного участка;
7. Изменение конфигурации земельного участка;
8. Объединение земельных участков;
9. Снятие обременения (запрета) на земельный участок;
10. Переоформление с уточнением границы земельного участка (при наличии государственного акта с некоординированным земельным участком).

Также были проведены работы по автоматизации таких обязательных процессов как земельная комиссия и согласование решения акимата города Актобе.

Вместе с этим, для удобства жителей города в геоинформационной системе города Актобе планируется автоматизировать услуги коммунальных служб и организовать данный портал как единое окно обслуживания населения.

На данный момент в пилотном режиме реализуется обеспечение всех рабочих станций МИО и Образования антивирусным ПО компании Dr.WEB. В серверном помещении ситуационного центра развернута виртуальная машина с ПО «Центр управления Dr.Web Enterprise Security Suite», с возможностью централизованной защиты всех узлов, устройств и сервисов сети. Данное решение

позволяет «взглянуть сверху» на антивирусную сеть области с одного рабочего места (через Веб–администратор).

Минимальная трудоемкость обслуживания сети, во многом связанная с простотой администрирования, сокращают время обслуживания системы до минимума.

По сравнению с аналогичными решениями других производителей Центр Управления гарантирует минимальный сетевой трафик. Компрессию данных между клиентом и сервером обеспечивает специально разработанный протокол обмена информацией.

Работа антивирусной сети, основанной на Dr.Web, совершенно прозрачна. Журнал аудита действий администраторов позволяет отслеживать все шаги по установке и настройке системы. Все ее компоненты могут вести файлы отчетов с настраиваемым уровнем детализации. В итоге любые действия над файлами отображаются в статистике. Предусмотрена система оповещения администратора о проблемах, возникающих в антивирусной сети. Ее сообщения могут отображаться в Веб–администраторе или приходиться по электронной почте.

Дополнительные возможности ПО:

- настраивать политики безопасности для любых типов пользователей, включая «мобильных», и для любых станций – даже отсутствующих в данный момент в сети – позволяют обеспечить актуальность защиты в любой момент времени;
- защитить от самостоятельного изменения настроек пользователями;
- блокировка доступа сменным носителям, ресурсам локальной сети и сети Интернет — защита от случайных или намеренных действий пользователей;
- возможность защиты сетей, не имеющих доступа в Интернет;
- минимальное использование ресурсов компьютеров и серверов благодаря компактности антивирусного ядра и использованию в нем новейших технологий;
- контролировать установленное программное обеспечение, видеть какая версия операционной системы установлена; видеть основные данные о рабочей станции (модель центрального процессора, объем ОЗУ, жесткие диски, сетевой адаптер, подключенные принтеры), что позволит провести инвентаризацию без выезда на место расположения рабочей станции.

Наряду с вышеуказанными проектами в рамках ситуационного центра задействован проектный офис в целях повышения эффективности управления всем портфелем проектов местных исполнительных органов. Проектный офис предоставляет возможность скомпоновать все реализуемые проекты в одну платформу, планирования и контроля хода его реализации, является инструментом для выполнения задач и доступа ко всей необходимой для их выполнения информации, что обеспечивает акиму области и его заместителям единую панель мониторинга всех проектов местных исполнительных органов с возможностью оперативного анализа отклонений и принятия управленческих решений.

Также Управлением ведутся работы по созданию IT ассоциации для развития молодых талантов. В случае необходимости, в целях реализации и продвижения местных проектов могли обратиться местному IT сообществу не привлекая сторонние компании из соседних регионов. В этой связи, в целях привлечения молодых кадров планируется заключить меморандум между Управлением и Актыбинским региональным университетом имени К. Жубанова. [3].

Цифровизация многогранна и практически не имеет границ, управлением цифровизации на ежедневной основе ведутся анализы текущих бизнес–процессов взаимодействия между органами и населения для повышения уровня жизни среди населения и оказываемых услуг государством.

Список литературы

1. FINANCIAL INCLUSION AND FINANCIAL LITERACY IN KAZAKHSTAN
<https://www.adb.org/sites/default/files/publication/460061/adb-wp876.pdf>
2. Smith, J. (2021). Digital Literacy and Economic Development: A Case Study of Region. Journal of Digital Economy
3. БЮРО НАЦИОНАЛЬНОЙ СТАТИСТИКИ
<https://stat.gov.kz/ru/>

УДК 338.2

**ОРГАНИЗАЦИОННЫЕ ИЗМЕНЕНИЯ: СОПРОТИВЛЕНИЕ ПЕРСОНАЛА И МЕТОДЫ
ЕГО ПРЕОДОЛЕНИЯ**
**ORGANIZATIONAL CHANGES: STAFF RESISTANCE AND METHODS OF
OVERCOMING IT**

Ашуралиев Мурад Рабазанович

Студент 1 курса Северо-Кавказского института (филиал) ВГУЮ (РПА Минюста России)

Muradasuraliev91@gmail.com

Адрес: улица Гайдара Гаджиева 7д

Ashuraliev Murad Rabazanovich

Muradasuraliev91@gmail.com

Address: 7dGaidarHajiyevStreet

Аннотация: в статье обоснована необходимость проведения организационных изменений в современных условиях развития; представлены основные факторы сопротивления персонала в период проведения организационных изменений и методы их преодоления.

Ключевые слова: внешняя среда, организационные изменения, управление изменениями, эволюционные изменения, революционные изменения, сопротивление персонала.

Abstract: the necessity of carrying out organizational changes in the current conditions of development of organization is presented in the article; the main factors of staff resistance during the period of organizational changes and methods for overcoming them are presented in the article.

Keywords: external environment, organizational changes, change management, evolutionary changes, revolutionary changes, staff resistance.

Актуальной проблемой для большинства современных организаций является сохранение жизнеспособности в динамично меняющейся внешней среде. Формирование эффективной системы управления развитием организации становится обязательным требованием эффективности и жизнеспособности ее деятельности в период бурного развития глобализационных и интеграционных процессов, развития науки, технологий и знаний.

Важнейшей проблемой управления современными организациями становится их динамичное развитие и, соответственно, необходимость наличия эффективной системы управления изменениями, которая является одним из ключевых условий ее успешной деятельности. С точки зрения А. Занковского, «Непрерывное развитие организации все больше становится необходимым условием не только ее эффективной деятельности, но и выживания в изменяющемся мире» [5].

Управление изменениями – это структурированный процесс, задача которого – предложить и внедрить изменения в соответствии с техническими и экономическими возможностями организации [6].

Эксперты по управлению и руководители едины во мнении, что организационные изменения, проведенные в нужное время и должным образом, являются одним из основных факторов успеха и выживания организации в современных условиях. Современные организации сталкиваются с необходимостью интенсификации организационных изменений, в том числе и радикального характера, что обусловлено необходимостью поддержания конкурентоспособности, обеспечения необходимого технологического уровня развития и качественного обслуживания потребителей собственной продукции или услуг.

В настоящее время организации сталкиваются с необходимостью проведения таких мероприятий как: слияния или поглощения, изменения в организационной структуре, реструктуризация, внедрение новых элементов информационных технологий, изменения системы мотивации персонала, внедрение программ обучения и повышения квалификации персонала, а также изменения, связанные с разработкой и реализацией программ по формированию организационной культуры.

Необходимость перемен в организации диктуется высоким динамизмом и непредсказуемостью событий во внешней среде организации, что обусловлено такими факторами как: рост конкуренции в глобальных масштабах, бурное развитие информационных и прочих технологий, изменения во вкусах и предпочтениях потребителей, необходимость привлечения и удержания в организации квалифицированных сотрудников. Это могут быть изменения как в ближайшей среде организации (поставщики, конкуренты, потребители), где руководство компании способно оказывать ограниченное влияние на происходящие процессы, так и в дальнем окружении, на которое организация не может оказывать никакого влияния, и вынуждена адаптироваться под происходящие в ней изменения.

В современной управленческой литературе различают два подхода к управлению организационными изменениями:

- механистический, в соответствии с которым компания рассматривается как машина, работающая по жестким правилам, при котором планирование организационных изменений проводится руководством компании, предполагается тщательное планирование проводимых изменений и тщательная система контроля, сопротивление персонала рассчитывается, и им управляют;

- органический, согласно которому, организация – это открытая система, подвергающаяся влиянию факторов внешней среды. Работники организации должны понимать необходимость организационных изменений и способствовать их проведению [6].

Организационные изменения можно рассматривать с различных точек зрения. В первую очередь, их можно классифицировать как эволюционные и революционные. В рамках первого варианта четко прослеживаются тенденции и перспективы развития организации и изменений во внешней среде, что позволяет реализовать процесс изменений постепенно, в соответствии с заранее разработанным планом.

Революционные изменения зачастую проводятся спонтанно, поэтому процесс их проведения может стать неуправляемым, стихийным и проводиться в течение относительно короткого периода времени. Во многих организациях в силу тех или иных причин возникает необходимость проведения именно революционных изменений, что значительно усложняет их проведение. В зависимости от глубины и характера проведения изменения могут быть незначительными, то есть носить корректирующий характер, или фундаментальными, когда изменения затрагивают все сферы деятельности организаций.

Для уверенности в конечном успехе проводимых организационных преобразований организация должна быть готова к их проведению. Предпосылками достаточной подготовленности организации к изменениям являются следующие:

- убежденность сотрудников в том, что преобразования являются естественным состоянием развития организации, признаком ее нормального функционирования;

- наличие и дальнейшее совершенствование системы общих ценностей, разделяемой всеми сотрудниками организации;

- создание и поддержание морально-психологического климата, способствующего поддержке персоналом проводимых организационных изменений;

- наличие четкой системы целеполагания и планирования, направленной на поддержку динамики проводимых преобразований.

Результаты организационных изменений могут носить как положительный, так и отрицательный характер. К положительным результатам изменений можно отнести позитивное влияние на мотивирование деловой активности, возникновение ощущения обновления; стимулирование отношений сотрудничества и взаимоподдержки в организации; рост профессионализма и компетентности сотрудников организации; появление дополнительных возможностей для раскрытия творческого потенциала работников.

К основным отрицательным последствиям, как правило, относятся необходимость финансовых затрат на их проведение; ухудшение координации работы организации на первоначальном этапе проведения изменений; значительная вероятность определенного ухудшения квалификации сотрудников по причине появления новых профессиональных обязанностей;

ухудшение социально-психологического климата в организации; появление недовольства проводимыми изменениями среди сотрудников организации.

Добиться необходимых положительных результатов позволит соблюдение важнейших принципов управления изменениями. Основными принципами, которыми необходимо руководствоваться при проведении организационных изменений, являются следующие принцип направленности и целесообразности; принцип цикличности развития организации; принцип научности при разработке организационных изменений; принцип своевременности проводимых преобразований; принцип системности изменений; четкое определение целей изменений, которые должны быть доведены до всех сотрудников организации; четкое понимание существующего положения дел в организации; четкое планирование проводимых изменений; информационное обеспечение персонала о результатах проводимых изменений; принцип достаточной ресурсной обеспеченности перемен.

Однако при проведении организационных изменений руководство организации сталкивается с многочисленными проблемами, препятствующими их эффективному проведению, ключевой из которых становится сопротивление сотрудников внедрению изменений. Исследования ведущих зарубежных и российских специалистов подтверждают, что сопротивление персонала может значительно снизить эффективность организационных изменений, что подтверждается результатами проведенных исследований, согласно которым около 70% организационных изменений заканчиваются неудачей [5]. Особенно актуальной данная проблема является для российских предприятий, уровень сопротивления в которых более высок, чем в зарубежных компаниях.

Важнейшими предпосылками возникновения сопротивления изменениям в организации являются следующие:

- внесение определенного дисбаланса в действующую организационную систему. Внедрение изменений нарушает упорядоченную систему взаимоотношений, сложившихся в организации, в результате чего возникают противоречия между сложившимся порядком вещей в ущерб потребностям организации;

- возникновение определенных угроз личным интересам сотрудников в ходе проведения изменений, следствием чего является стремление работников защищать свои интересы в ущерб потребностям организации;

- неэффективная организация процесса проведения перемен.

Выявление и систематизация факторов, оказывающих влияние на процесс проведения организационных изменений, является одной из центральных проблем, так как это позволит использовать наиболее эффективные методы преодоления сопротивления.

В научной литературе выделяют несколько подходов к систематизации факторов сопротивления изменениям в организации. В соответствии с классификацией С. Розенберга и С. Моска, выделяют личностные и организационные факторы сопротивления переменам, а также факторы, тесно связанные со спецификой проводимого изменения, его сутью [5].

Страх перед неизвестностью, негативное отношение работников к изменениям, страх перед неудачей, боязнь увеличения объема работы, отсутствие понимания необходимости проведения перемен, страх потери положения и стабильности в организации, недостаток мотивации в осуществлении изменений и пр. являются основными личностными факторами сопротивления переменам.

К организационным относятся неэффективное руководство, масштабы организации и проводимых организационных изменений, недостатки организационной культуры, низкий уровень доверия между руководителями и работниками, рост уровня конфликтности в период проведения организационных изменений, неэффективное взаимодействие между уровнями управления в организации, нежелание или неумение руководства организации преодолеть сопротивление проводимым изменениям.

Для осознания сотрудниками необходимости проведения преобразований целесообразными представляются следующие шаги со стороны руководства организации:

- разработка понятного плана проведения изменений, где четко обозначены цели, задачи, перечень необходимых действий и конкретные результаты проводимых преобразований;

- формирование системы коммуникационных сетей с целью своевременного информирования сотрудников о ходе и результатах проводимых изменений;
- привлечение к проведению преобразований наиболее компетентных и профессиональных сотрудников;
- четкое и доступное обоснование необходимости проводимых перемен;
- формулирование конкретных показателей, подтверждающих обоснованность преобразований.

Необходимость проведения, обоснованность и значимость изменений, неэффективное планирование и реализация изменений относятся к факторам, связанных со спецификой проводимых организационных изменений, его содержанием. Соппротивление персонала организационным изменениям являются серьезным фактором, препятствующим их результативности, а неумение руководителей управлять ими значительно снижают скорость и эффективность их проведения.

Р.Г. Бухбиндер подразделила факторы сопротивления персонала изменениям на 5 групп [3]:

- психологические, которые включают в себя личностные качества человека, возрастное влияние, восприятие изменений как сложных и недостижимых, негативные ожидания от перемен, обусловленные предыдущим опытом участия в них, стремление работать в условиях стабильности отлаженности процессов;
- социальные, обусловленные существованием у работников неформальных связей, образовавшихся за время их работы в компании, облегчающих работникам поиск необходимой информации и уменьшающих время на выполнение своих обязанностей, опасением утери статуса и своей роли в организации, что чаще свойственно менеджерам среднего и верхнего уровня управления, наличием субкультуры и контркультуры в организациях, нормы и ценности которых отличаются от организационной культуры, но поддерживается частью работников;
- организационные, суть которых заключается в том, что руководители сами допускают серьезные просчёты при проведении организационных изменений. Заключаются они в том, что сотрудников не ставят в известность о проводимых изменениях или информируют только по факту их начала. Нередки ситуации, когда руководитель организации не проявляет особого интереса к проводимым изменениям и, соответственно, топ-менеджмент не в полной мере их поддерживает.

У работников нет чёткого видения результатов проводимых изменений, так как не выработана стратегия их проведения, что приводит к определённому демотивированию персонала.

Наличие у персонала негативного опыта проведения или участия в изменениях в прошлом, когда перемены были проведены, но эффект от их проведения значительно отличался от запланированного, следствием чего является существование определённого недоверия в успешность проводимых изменений.

Опасения работников, что возможны значительные изменения в условиях их работы, которые могут заключаться в необходимости изучения новых программ или освоения новых технологий, возможность перевода в другое подразделение или даже переезда в другой город.

- профессиональные, заключаются в том, что меняются профессиональные обязанности работников. Они комфортнее чувствовали себя на прежних, привычных условиях работы и не хотят каких-либо изменений в этом плане.

- экономические, которые выражаются в том, что происходят изменения в системе оплаты труда и работники опасаются снижения оплаты или повышения объёма работ. Недостаточное финансирование изменений может привести к борьбе подразделений за влияние на руководителя, ответственного за распределение ресурсов, перемены в системе распределения ресурсов по подразделениям вызовут сопротивление со стороны тех отделов, которые раньше имели больше доходов и, соответственно, влияние и статус. Такое положение приводит к снижению показателей деятельности подразделений.

Снижения сопротивления возможно добиться путем повышения уровня мотивированности работников. Если удастся мотивировать сотрудников на выполнение работы в соответствии с новыми правилами, изменения успешно пройдут в подразделениях и в организации в целом.

Руководители организации должны иметь четкое представление о проблемах, которые могут возникнуть в ходе проведения преобразований и разработать планы по их преодолению. Методы

сопротивления переменам должны быть достаточно разнообразными и предполагать использование процедур наиболее адекватных для ситуации, сложившейся в организации. Наиболее разумным представляется использование как демократичных, так и авторитарных методов проведения организационных изменений, преимущественной использование которых зависит от складывающейся в данной организации ситуации.

Основываясь на приведенной типологии причин сопротивления персонала возможна разработка системы мер по нейтрализации или снижению сопротивлению персонала.

Точного описания всех методов, направленных на нейтрализацию всех факторов сопротивления работников в настоящее время не разработано, однако можно выделить все существующие на сегодняшний день для возможного использования тех, которые наиболее актуальны в конкретной организации.

Одним из наиболее действенных способов является обучение и тренинг персонала, который позволяет повысить эффективность внедрения изменений за счет того, что снижает уровень стресса у работников, опасаящихся, что они не справятся с новыми дополнительными функциями.

Достаточно эффективным представляется метод, который заключается в том, что сотрудников регулярно собирают (1-2 раза в неделю) и в неформальной обстановке они рассказывают о своих успехах, что способствует поддержанию положительных эмоций в коллективе.

Ощутимый эффект может дать установление краткосрочных целей в течение всего периода проведения организационных изменений, достижение которых вселяет уверенность в сотрудников в конечном успехе изменений, поскольку они будут более мотивированы на достижение конечных результатов проводимых изменений.

Достаточно эффективным методом является привлечение сотрудников к планированию и организации внедряемых изменений. Вовлечение большего количества сотрудников в данный процесс приведет к большему эффекту от применения данного способа, так как они будут владеть всей информацией о целях и задачах изменений, и имеют возможности оказывать определенное влияние на процесс его проведения. Участие сотрудников в процессе планирования организационных изменений повысит ответственность за конечные результаты, а также окажет положительное воздействие на их мотивированность.

Значительно снизить сопротивление можно путем регулярного информирования сотрудников о результатах внедряемых изменений, поскольку работники должны знать в чем необходимость проводимых изменений и к каким результатам стремится компания. Необходимо предоставлять возможность открытого обсуждения проблем, связанных с внедряемыми изменениями, что будет способствовать предотвращению возможных конфликтов, снизит напряженность в коллективе.

Руководить внедрением изменений должен менеджер, обладающий лидерскими качествами и пользующийся авторитетом в организации, что окажет значительный положительный эффект на результаты проводимых изменений.

Успешному проведению изменений будет способствовать привлечение к их проведению известных людей, пользующихся уважением и авторитетом у сотрудников компании, что будет подчеркивать важность и значимость проводимых изменений.

Определенное воздействие оказывает также увольнение некоторых сотрудников, наиболее открыто и активно показывающих неприятие проводимых изменений. Однако такие меры могут иметь отрицательный эффект, который проявится в виде ухудшения морально-психологического климата в коллективе, в росте подавленности и агрессивности работников. Данный метод может быть эффективен, когда другие методы не дают ощутимого эффекта.

Несмотря на то, что большая часть работников настороженно относится к изменениям, определенная часть сотрудников может воспринимать изменения с большим энтузиазмом. Задачей руководства организации является увеличение части сотрудников, приветствующих проводимые организационные изменения. Факторами, способными оказать влияние на увеличение количества сторонников перемен являются: рост заработной платы, расширение прав сотрудников, снижение объема обязанностей, улучшение морально-психологического климата в коллективе, полноценное использование потенциала работников, более творческий характер после внедрения изменений, большая ответственность и самостоятельность в работе, рост престижа, соответствие изменений

традициям и нормам коллектива, менее напряженный характер работы, повышение профессионализма и компетентности работников, рост статуса сотрудников.

Эффективное управление персоналом в период проведения организационных изменений является важнейшим фактором поддержания конкурентоспособности компании в современной высококонкурентной рыночной среде. Использование предложенных методов, несомненно, окажет положительное воздействие на темпы и окончательный результат проводимых организационных изменений. Компании используют те способы, которые являются для них наиболее актуальными, в зависимости от ситуации, складывающейся в организации. Кроме того, в различных организациях могут быть выявлены и другие факторы сопротивления изменениям, на которые организация самостоятельно разрабатывает методы преодоления.

Список использованных источников

1. Андреева Е.А. Организационные изменения: сравнительный анализ основных подходов / Е Андреева // Вестник Санкт-Петербургского университета. Серия «Менеджмент». – 2004. – Выпуск 2.
2. Божко Л.М. Понятие организационных изменений и его синонимы / Л. Божко // Вестник Омского университета. Серия «Экономика». – 2014. - №1.
3. Бухбиндер Р.Г. Организационные изменения: проблема сопротивления персонала и пути ее решения / Р. Бухбиндер // Вестник Омского университета. Серия «Экономика». – 2009. - №4.
4. Кобзева Н.М. Феномен сопротивления изменениям: сущность, виды и формы проявления / Н. Кобзева // Вестник Воронежского государственного университета инженерных технологий. – 2013. - №4.
5. Мкртычян Г.А, Исаева О.М. Причины сопротивления персонала организационным изменениям: взгляд менеджеров как агентов перемен / Г. Мкртычян, О. Исаева // Организационная психология. – 2015. - №5.
6. Полевая М.В. готовность организаций к внедрению изменений / М. Полевая // Вестник Финансового университета. – 2017. - №1.
7. Сазанов Е.Г. Сопротивление организационным изменениям: диагностика и преодоление / Е. Сазанов Е. // Проблемы теории и практики управления. – 2003. – №6.
8. Силютин В.И. Понимание сущности организационных изменений и развития / В Силютин // Вестник Самарского государственного университета. – 2012. - №1.

**КОНЦЕПЦИИ КОНТРОЛЛИНГА В ОТЕЧЕСТВЕННОЙ И ЗАРУБЕЖНОЙ
ПРАКТИКЕ ЭКОНОМИЧЕСКОГО УПРАВЛЕНИЯ НА МИКРОУРОВНЕ**

**CONCEPTS OF CONTROLLING IN DOMESTIC AND FOREIGN PRACTICE OF ECONOMIC
MANAGEMENT AT THE MICRO LEVEL**

**Е.Е. Банцевич, А.П. Козлов
Y.E. Bantsevich. A.P. Kozlov**

**Учреждение образования «Белорусский государственный университет пищевых и химических
технологий»**

**Республика Беларусь, 212027, г. Могилев, пр. Шмидта, 3, email:
bantsevich_buaa@mogilev.bgut.by**

**Educational Institution «Belarusian State University of Food and Chemical Technologies»
Republic of Belarus, 212027, Mogilev, Schmidt Ave., 3, email: bantsevich_buaa@mogilev.bgut.by**

Аннотация

В рамках научной проблематики исследования механизмов повышения экономической безопасности и эффективности в системе экономического управления выполнен анализ теоретических основ контроллинга на микроуровне. Представлена эволюция научных взглядов на систему управления через контроллинг. Дана характеристика основных концепций контроллинга, определены внешние и внутренние субъекты системы корпоративного контроллинга, представлены типы организационной структуры контроллинга.

Ключевые слова: теоретические основы, система управления, риски хозяйственной деятельности, контрольная среда, внутренний контроль, предмет и объекты контроллинга, субъекты контроллинга, рекомендации

Abstract

Within the framework of the scientific problem of studying the mechanisms of increasing economic security and efficiency in the economic management system, an analysis of the theoretical foundations of micro-level controlling has been carried out. The evolution of scientific views on the management system through controlling is presented. The characteristics of the main controlling concepts are given, the external and internal subjects of the corporate controlling system are defined, and the types of the controlling organizational structure are presented.

Keywords: theoretical bases, management system, business risks, control environment, internal control, the entity and objects of controlling, the subjects of controlling, recommendations

Введение

Вопрос выбора системы показателей для оценки состояния экономической безопасности предприятия, разработка инструментов внутреннего контроля для организаций пищевой промышленности заслуживает детальной научно-исследовательской проработки. В зарубежной практике принятия управленческих решений, можно встретить концепцию управления – «контроллинг», именно она способствует осмыслению происходящих процессов и пониманию будущего. Контроллинг – это управленческий сервис, то есть поддержка руководства в области стратегического и оперативного управления организации, включающий в себя информационное обеспечение руководства финансовой и нефинансовой информацией и содействующий процессу постановки целей и достижению результатов на основе разработки планов.

Материал и методы исследования

Методология проведенного исследования основана на системном подходе с использованием таких общенаучных методов как: наблюдение, сравнение, при этом происходит накопление фактов и их описание, далее применяется обобщение и систематизация данных, их анализ, синтез, логическое исследование собранных фактов, выработка суждений и умозаключений, создаются теоретические обобщения, используются методы системного анализа и устанавливаются границы их применения.

Результаты исследования и их обсуждение

Система контроллинга призвана управлять процессами текущего анализа и регулирования плановых и фактических показателей, чтобы по возможности избежать ошибки, отклонения от плановых показателей – как в настоящем, так и будущем.

Отсюда назначение контроллинга – предупреждение возникновения кризисных ситуаций. Ошибки и проблемы, возникающие при анализе ситуации внутри организации, переплетаются, если их вовремя не исправить, с ошибками в оценке будущих условий окружающей среды. Другими словами, необходимо предусмотреть, чтобы принимаемое решение не основывалось на ошибочных предпосылках, а это особенно важно, когда принимаемое решение сопряжено с большим риском. Основными задачами контроллинга являются выявление ошибок в работе организации и координация ее деятельности с целью предотвращения кризисных ситуаций и повышения эффективности работы организации.

Решение этих задач связано с:

1. Определением фактического состояния организации и ее структурных единиц;
2. Прогнозированием состояния и поведения экономики организации на заданный будущий момент времени;
3. Заблаговременным определением места и причин отклонений значений показателей, характеризующих деятельность как организации в целом, так и его структурных единиц;
4. Обеспечением устойчивого производственно-финансового состояния организации при наступлении (достижении) предельных значений показателей;
5. Поиск слабых и узких мест в деятельности организации.

Результативность решения выявленной проблемы во многом определяется тем, как хорошо скоординированы цели различных уровней управления, средства и методы их реализации.

Поэтому следующей задачей контроллинга является задача контроля и регулирования. Суть данной задачи состоит в информационном сопровождении процесса планирования. Ее решение связано с:

1. Разработкой методик планирования;
2. Представлением информации для составления планов;
3. Установлением допустимых границ отклонений;
4. Анализом причин и разработкой предложений для уменьшения отклонений;
5. Учетом и контролем затрат и результатов;
6. Разработкой инструментария для планирования, контроля и принятия управленческих решений;
7. Стимулированием планирования.

Реализация всех названных задач контроллинга делает возможной подготовку к использованию будущих благоприятных условий, проясняет возникающие проблемы, подготавливает предприятие к внезапным изменениям во внешней среде, улучшает координацию действий в организации и тем самым способствует длительному и успешному функционированию предприятия и его структурных единиц.

В качестве ключевых целей организации можно выделить достижение высокой рентабельности, обеспечение ликвидности и повышение эффективности организации в целом. Достижение поставленных целей основывается на выполнении следующих функций контроллинга [1]:

1. Мониторинг состояния экономики организации;

2. Сервисная функция (обеспечение аналитической информацией для принятия управленческих решений);
3. Управляющая функция;
4. Контроль и анализ экономичности работы подразделений;
5. Подготовка (разработка) методологии принятия решений, их координация, а также контроль восприятия этой методологии руководством.

Мониторинг состояния экономики предприятия – это контроль равновесия показателей прибыли и затрат. Равновесие достигается тем, что через определенные промежутки времени заданные величины сравнивают с фактическим состоянием и определяют, не нужно ли вмешательство (противодействующие меры) для достижения необходимого или желаемого состояния, и в случае необходимости осуществляют его.

Таким образом, можно дать также следующее определение контроллинга – система регулирования затрат и результатов деятельности, необходимая для достижения целей организации, позволяющая предупредить появление кризисных ситуаций и своевременно принять меры, когда экономике организации угрожает опасность.

Сервисная функция заключается в своевременном представлении необходимой информации руководству для принятия решения по корректировке стратегии развития предприятия. Информационное обслуживание контроллинга обеспечивается при помощи систем планирования, нормирования, учета и контроля, ориентированных на достижение цели, конечного результата деятельности предприятия. Информация должна содержать заданные (нормативные, плановые) и фактические данные, в том числе об отклонениях, выявляемых средствами учета по подразделениям.

Управляющая функция заключается в переоценке стратегии, корректировке реализации целей и изменении целей. Осуществляется эта функция с использованием данных анализа отклонений, ставок покрытия, общих результатов деятельности для принятия решений по управлению. Такие решения принимаются на всех уровнях управления организацией, и весьма важной задачей контроллинга является координация целей различных уровней, средств и методов их реализации, с тем, чтобы в максимальной степени обеспечить достижение конечной цели предприятия.

Основная задача руководства заключается в создании потенциала успеха на рынке в будущем, что достигается, прежде всего, применением системы стратегического планирования. Чтобы разрабатываемая стратегия была верной, необходимо иметь систему «раннего обнаружения» будущих тенденций, как в окружающем мире, так и внутри, и в самой организации. Внешние индикаторы должны информировать руководство об экономических, социальных, политических и технологических тенденциях, внутренние – представляющие на практике отдельные показатели и их системы – сообщать о текущем «самочувствии» организации, а также прогнозировать кризисные ситуации в отдельных сферах деятельности или в целом на предприятии.

Задачей контролера является методическая и консультационная помощь при создании системы раннего обнаружения тенденций и факторов, способных принести при их развитии не только выгоду, но и потери. Задача контролера состоит также и в том, чтобы следить за правильностью применения методики, способствующей достижению предприятием прибыли (предотвращению убытка). Эту функцию контролер должен выполнять в качестве своего рода консультанта, сопровождающего экономиста, по достижению прибыли таким образом, чтобы каждый сотрудник сохранял с помощью соответствующих инструментов способность к самоконтролю.

Основные концепции контроллинга.

В немецком издании «Экономический словарь предприятия» контроллинг определен как концепция информации и управления. Тем не менее, до сих пор нет единого определения термина «контроллинг», а имеется множество мнений, которые порой существенно отличаются друг от друга. В рамках немецкой теории контроллинга существуют различные школы и подходы. Концепции контроллинга можно разделить на три группы по представлению А. Шмидта: концепции, ориентированные на бухгалтерский учет, ориентированные на информационную систему и координацию. Такая группировка объясняется функциональным обоснованием и институциональным представлением о контроллинге [2]. Основные концепции контроллинга представлены в таблице 1.

Таблица 1 – Основные концепции контроллинга

Ориентация концепции	Сущность и основные задачи контроллинга в рамках концепции
На систему учета (Х.Ю. Кюппер и Е Хейнен)	Переориентация системы учета из прошлого в будущее, создание на базе учетных данных информационной системы поддержки управленческих решений, связанных с планированием и контролем деятельности предприятия
На управленческую информационную систему (Т. Райхман и Е. Шеффлер)	Создание общей информационной системы управления (managementinformationsystem). Разработка концепции единой информационной системы, ее внедрение, координация функционирования информационной системы, оптимизация информационных потоков
На систему управления (Д. Хан, П. Хорват, И. Вебер и Д. Шнайдер)	Интеграция и инструментальная часть системы управления. Планирование и контроль деятельности структурных подразделений предприятия. Координирование, реагирование и адаптация к меняющимся внутренним и внешним условиям с тем, чтобы реализовать намеченные цели.

Формирование механизма контроллинга в условиях каждой отдельной страны хоть и имеет много общего, но по своей сути складывается под влиянием множества национальных факторов. Использование контроллинга должно осуществляться на основе существующих в отечественной практике инструментов планирования, контроля, комплексных систем интегрирования различных аспектов экономического управления, а также предусматривать адаптацию зарубежного опыта в сфере контроллинга к отечественным экономическим условиям.

Концепция контроллинга с ориентацией на систему учета берет за основу учетную информационную базу для принятия управленческих решений. Контроллинг создает в сфере вопросов для управления предприятием систему внутреннего управленческого (производственного) учета более сложную информационную систему по сравнению с данными бухгалтерского учета и отчетности. Управленческий учет направлен на решение конкретной управленческой задачи и представляет собой систему организации, сбора и агрегирования учетных данных. Контроллинг, базирующийся на данных бухгалтерского учета и в первую очередь управленческого учета, относится, прежде всего, к оперативному уровню управления предприятием. Стратегический уровень управления контроллинг охватывает в том случае, когда речь заходит о производственном потенциале предприятия.

Ориентированная на учет концепция применяется, если поставленные перед предприятием информационные цели могут быть реализованы в основном с помощью данных бухгалтерского учета. Показатели при использовании данной концепции представлены в натуральном и денежном выражении. Подход, использующий учетную концепцию контроллинга, может быть охарактеризован как ориентированный на прибыль. Он основывается на данных бухгалтерского учета, и поэтому ограниченно ориентирован на информацию. Контроллинг, базирующийся на учетной концепции, использует релевантную информацию в стоимостном выражении, что преимущественно отражает оперативное направление управления предприятием.

Концепция с ориентацией на управленческую информационно-аналитическую систему включает не только стоимостные показатели. Она охватывает всю целевую систему предприятия, поэтому выходит за рамки подхода, ориентированного на бухгалтерский учет. Источником количественной и качественной информации является производственно-хозяйственная деятельность предприятия, а также данные бухгалтерского учета. В рамках управленческой информационной концепции, включающей в себя постоянный сбор, обработку, систематизацию и предоставление самой различной информации, служащей основным источником для принятия управленческих решений руководством предприятия, контроллинг рассматривают как процесс информационного обеспечения. Зависимость от качества и объема информации – главная особенность при использовании этого подхода для принятия управленческих решений при других равных условиях.

Главная задача контроллинга заключается в отслеживании при получении релевантной информации, а также в ее подготовке в соответствии с потребностями внутренних пользователей.

Объективное включение больших информационных задач в хозяйственную структуру предприятия создает определенные трудности при их решении. Поставленные задачи не являются самоцелью для предприятия. Они связаны со специфическими информационными потребностями и являются производными вышестоящих целей предприятия.

Т. Райхман отмечает важность информационной поддержки управления и считает, что основная задача контроллинга заключается в обеспечении руководства компании информацией для принятия решений [3]. П. Прайсслер интерпретирует контроллинг следующим образом: «своеобразный управленческий инструмент, позволяющий принимать решения с помощью целенаправленного сбора и обработки информации для обеспечения и поддержки внутрифирменного процесса управления» [3].

Подход с ориентацией на управленческую информационную систему значительно расширяет сферу контроллинга, в отличие от концепции, ориентированной на учет.

Воздействие контроллинга как концепции управления на организационную культуру должно способствовать развитию управления предприятием на основе системного мышления. Такое воздействие осуществляется на уровне культуры предприятия – уровне осознаваемых ценностей. В случае усвоения и использования персоналом положительных результатов эти ценности обретают вид базовых предположений и оказывают положительное влияние на поведенческие аспекты сотрудников предприятия.

В качестве факторов контроллинговой деятельности, положительно воздействующих на культуру предприятия, можно обозначить:

- создание центров ответственности (оптимизация организационной структуры);
- развитие и оптимизация системы прозрачных информационных потоков в процессах управления предприятием;
- целеполагание как формирование системы общих и детализированных целей предприятия (включая индивидуализацию целей).

Исследователь проблем управления предприятием Д. Шнайдер считает, что задачи контроллинга должны быть ограничены в отношении всеобщей координации управления. По мнению Д. Шнайдера, функции и задачи контроллинга включают следующие направления: разработка и координация отдельных планов предприятия и сведение их в единый план, формирование внутреннего производственного учета, предоставляющего исходную информацию для планирования и служащего для контроля за выполнением планов. Рекомендуемое Д. Шнайдером ограничение функций контроллинга представляется чрезвычайно узким подходом: на первое место ставится комплекс задач по планированию, включающий интегрированную систему планово-контрольных расчетов, базирующуюся на информации внутреннего производственного учета, ограниченной чисто денежными показателями [3].

П. Хорват, представляющий контроллинг как подсистему управления, координирующую подсистемы информационного обеспечения, планирования, контроля и, поддерживающей системообразующую и системоувязывающую координацию. Системообразующая координация представляет собой создание системных и процессных структур, способствующих согласованию задач. Системоувязывающая координация заключается в сохранении информационных связей между подсистемами, а также в их последующей адаптации. В соответствии с интерпретацией П. Хорвата, контроллинг ориентирован на результат. Контроллинг выступает в качестве функции поддержки руководства для достижения главной цели предприятия - определенных финансовых показателей. По П. Хорвату контроллинг выполняет функции информационного обеспечения, интегрирования и координирования процесса планирования на предприятии. [3].

Немецкие ученые А. Дайле и Э. Майер помимо выше обозначенных концепций рассматривают так называемую практическую концепцию контроллинга. Практическая концепция контроллинга менее научна и систематична. Основная цель данной концепции – создание единого образа контроллинга в условиях производства, а также практическое внедрение контроллинга на предприятиях. Данная концепция рассматривает контроллинг как механизм для целенаправленного управления промышленным предприятием. Такой подход вносит значимый эмпирический вклад в развитие концепций контроллинга [4].

Роль контроллинга в вопросе повышения эффективности управления требует особого внимания. Контроллинг способствует обеспечению функционирования и развитие предприятия на этапах стратегического и тактического управления. В этом аспекте Э. Майер отмечает, что концепция контроллинга позволяет интегрировать традиционный учет, планирование и маркетинг в рамках отдельного предприятия в единую систему управления и, следовательно, она должна координировать оба вида мышления - системное и прямолинейное [4]. Распространение контроллинга тесно связывается с повышением качественного уровня системы управления предприятием и внедрением эффективных нововведений менеджмента. Координируя, интегрируя и направляя деятельность всей системы управления на достижение поставленных целей, контроллинг выполняет функцию «управления управлением». Выполнение контроллингом данной функции переводит его на качественно новый уровень. Замены управления предприятием при этом не происходит. Контроллинг не представляет собой механизм, который автоматически освобождает менеджеров от функций управления, а является системой, обеспечивающей эффективное управление финансовыми и трудовыми ресурсами. Таким образом, контроллинг – четко функционирующий механизм информационной поддержки процессов менеджмента на предприятии, интегрирующий работу различных подразделений предприятия в вопросах планирования, учета, контроля и анализа деятельности предприятия в целом и его отдельных структурных звеньев. Контроллинг имеет определяющее значение для повышения внутреннего потенциала управления, достижения определенного уровня управленческой деятельности, обеспечивающего сохранение и развитие производственного и финансового потенциала предприятия.

Х.Ю. Кюппер, стараясь прийти к согласию относительно концепции контроллинга, определяет контроллинг следующим образом. Контроллинг направлен на обеспечение целевого управления предприятием с помощью координации системы менеджмента в целом для обеспечения соответствующих действий по управлению. Таким образом, по мнению Х.Ю. Кюппера, координация всей системы управления предприятием для обеспечения целенаправленного руководства им, составляет сущность контроллинга [5]. Контроллинг при выполнении координирующей функции, способствует достижению всей системы целей предприятия, а не одной конкретной цели, поставленной перед управленческим персоналом предприятия. Особое значение при выполнении координирующей функции придается стоимостным целям. Однако Х.Ю. Кюппер замечает, что для контроллинга существует опасность определения его задач как всеохватывающих [5]. При такой широкой интерпретации задачи контроллинга не могут быть беспрепятственно отделены от задач других подсистем управления.

Таким образом, все концепции контроллинга предназначены для поддержки действий, связанных с менеджментом. Координирующая составляющая контроллинга является преобладающей во всех трех подходах. Но только в рамках последнего подхода контроллинг определяется как основная организационная функция менеджмента. Концепции, использующие подходы с ориентацией на систему учета и на информационную управленческую систему, отводят контроллингу подчиненную роль.

Субъекты контроллинга

Субъектами корпоративного контроллинга являются те должностные лица и структурные подразделения, которые реализуют задачи корпоративного контроллинга. Всех субъектов контроллинга можно разделить на четыре группы в зависимости от специфики выполняемых задач в рамках системы корпоративного контроллинга: высшие органы управления предприятием, ревизионная комиссия, внутренний финансовый контроллер и служба внутреннего аудита, персонал компании (менеджмент среднего звена).

Последняя группа субъектов корпоративного контроллинга реализует функцию самоконтроллинга, то есть такую модель организации контроллинга на предприятии, при которой отдельные менеджеры берут на себя выполнение задач контроллинга, а контроллер выступает модератором этих задач.

Также субъектов системы корпоративного контроллинга можно разделить на внешних и внутренних. К субъектам внутреннего контроллинга относят внутренние службы организации, которые входят в структуру самого предприятия – специальные (служба контроллинга или

внутренние контроллеры), полуспециальные (планово-экономический отдел, бухгалтерия), временная группа.

Выбор того или иного варианта часто зависит от необходимости и интенсивности проведения контроллинга, а также субъективного понимания, восприятия и интерпретации руководителем предприятия системы контроллинга в целом. Так, при восприятии контроллинга как концепции и философии управления предприятием часто необходима специальная служба контроллинга. Если контроллинг рассматривается как инструмент, методология или процесс управления, целесообразно использовать разрозненный или внешний контроллинг.

Служба контроллинга должна реализовывать следующие основные функции: методологическую; аналитическую; интеграционную; координационную; контрольную; консультационную.

В зависимости от вида, размеров и характера деятельности предприятия, организационная структура службы контроллинга может быть построена по-разному. Для крупных предприятий характерно образование специального подразделения (отдела, службы), руководимой финансовым директором (финансовым менеджером), на небольших и средних предприятиях обычно функции контроллинга выполняют руководители различных финансовых отделов. Важно отметить, что чем меньше предприятие, тем выше место контроллинга в иерархии управления, так как часто в таких организациях сам руководитель берет на себя функции контроллинга. Перед созданием службы контроллинга необходимо определить место службы в организационной структуре предприятия.

На практике в основном встречаются три варианта организации службы контроллинга: объединение службы контроллинга с другим отделом; служба контроллинга прямо подчиняется руководителю предприятия и занимает особое место в иерархии управления; служба контроллинга становится самостоятельным отделом, подчиненным линейной структуре управления. В большинстве случаев служба контроллинга входит в состав финансово-экономической службы предприятия, а контроллер находится в подчинении у руководителя этой службы.

Основными преимуществами создания специальной службы контроллинга являются быстрота, системность и качество системы контроллинга. Недостатком является конфликт интересов с планово-экономической службой, если таковая существует.

Внешними субъектами контроллинга являются внешние аудиторы предприятия и рейтинговые агентства. Принципиальное отличие между внутренними и внешними субъектами системы корпоративного контроллинга заключается в том, что внешние субъекты также являются пользователями результатов внутреннего корпоративного контроллинга. Например, внешний аудитор является субъектом системы корпоративного контроллинга, а аудиторское мнение в заключении – одним из наиболее распространенных механизмов корпоративного контроллинга, используемом финансовыми институтами для оценки надежности компании, привлекающей финансирование. При этом внешний аудитор фактически всегда пользуется результатами работы внутреннего контроллера или аудитора, чтобы оценить неотъемлемые бизнес-риски и, как следствие, риски существенного искажения бухгалтерской (финансовой) отчетности предприятия. Такая ситуация характерна именно для системы корпоративного контроллинга и отличает ее от других областей финансово-экономической работы на предприятии.

Объекты контроллинга.

Объектами контроллинга являются факторы производства, показатели эффективности их использования и организации, экономический потенциал предприятия (численность, основные средства, объемы производства и реализации), а также показатели финансового состояния в сравнении с прогнозируемыми.

Для контроллинга используется разнообразная информация финансового и управленческого учета, на основании которой определяется эффективность использования ресурсов, ход реализации хозяйственных процессов, формирование прибыли, показатели финансового состояния. Отбор показателей определяется менеджерами на основе специальных исследований.

К основным объектам контроллинга можно отнести следующие: развитие и исследования; снабжение; логистику; производство; сбыт; инвестиции; финансы; персонал (кадры); качество; проекты (программы).

В широком смысле под объектом контроллинга можно понимать всю систему управления в целом. В данном случае объектом контроллинга выступают цели компании, система планирования, контроля и информационного обеспечения. При этом следует различать корпоративный финансовый контроллинг и контроль качества на предприятии. В первом случае объектом контроля выступает система управления компанией, во втором – выпускаемая продукция.

В узком смысле объекты контроллинга можно разделить на классические и новые. Под классическими объектами корпоративного контроллинга понимаются отдельные области финансовой функции предприятия: система учета, финансовая отчетность, краткосрочное бюджетирование, проектный менеджмент. К «новым» объектам корпоративного контроллинга относятся: информационные системы, стратегическое планирование, порядок регламентации и оптимизации бизнес процессов, инструменты финансово-экономического анализа, методики управления по местам возникновения прибыли.

Предметом контроллинга являются микроэкономические процессы и явления на предприятии, которые характеризуются определенными показателями – индикаторами в их динамике и макроэкономические процессы в стране, которые оказывают непосредственное влияние на экономику предприятия. Для контроллинга важным является учет изменений как внутреннего, так и внешней среды, в отличие от финансового учета, который отслеживает в основном внутренние изменения в хозяйственной деятельности и управленческого, что учитывает изменения внутри системы наблюдения и лишь в определенной мере за ее пределами.

Критерием способности предприятия адаптироваться к изменяющейся среде является получение положительного финансового результата хозяйственной деятельности, а потому ориентация на прибыль показывает, что предприятие демонстрирует свою способность выстоять, преодолевая изменения, часто негативные, в окружающей среде. Поэтому предприятия должны перейти от пассивной регистрации хозяйственной деятельности (финансовый учет) к системам, которые позволяют обеспечить формирование данных для анализа и оценки своей позиции в изменяющемся рыночном окружении (контроллинг).

Выводы (заключение)

Обобщив подходы к структуре системы контроллинга, ее можно представить совокупностью следующих элементов:

- методология контроллинга, включающая в себя механизм контроллинга и концепцию контроллинга;
- структура контроллинга, состоящая из субъективной и объективной подсистем;
- процесс контроллинга, включающий коммуникации, схему процесса, разработку и реализацию управленческих решений;
- система обеспечения контроллинга, состоящая из информационно-правового, финансового, материально-технического, кадрового, информационного, программного обеспечения, сетей связи, системы документооборота и организационной культуры.

Координируя, интегрируя и направляя деятельность всей системы управления предприятием на достижение поставленных целей, контроллинг выполняет функцию «управления управлением» и является синтезом учета, контроля, экономического анализа.

Список литературы

- 1 Диаров, А. А. Контроллинг: учебн.-практ. пособие / А.А. Диаров. – М.: Издательство МГУТУ, 2008. – 47 с.
- 2 Чувашлова, М.В. Контроллинг как новое философское мышление в управлении промышленной организацией / М.В. Чувашлова // *Фундаментальные исследования*. 2012. № 9-2. С. 505–509.
- 3 Хан, Д. Планирование и контроль: концепция контроллинга / Пер. с нем.; под ред. и с предисл. А.А. Турчака, Л.Г. Головача, М.Л. Лукашевича. – М.: Финансы и статистика, 1997. – 800 с.
- 4 Майер, Э. Контроллинг как система мышления и управления / Э. Майер. – М.: Финансы и статистика, 1993. – 96 с.
- 5 Мескон, М. Х. Основы менеджмента / М.Х. Мескон, М. Альберт, Ф. Хедоури / пер. с англ. – М.: Дело, 2002. – 704 с.

**СОВРЕМЕННЫЕ КИБЕРАТАКИ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ****MODERN CYBER ATTACKS AS A THREAT TO INFORMATION SECURITY OF THE
RUSSIAN FEDERATION**

Гальцова Лилия Евгеньевна

[Galtsova Liliy Evgenievna](mailto:rf@rpa-mjust.ru)

rf@rpa-mjust.ru

Аннотация: В условиях современного мира период цифровизации характеризуется не только быстрым прогрессом в области информационных технологий, но также сопровождается возрастающей угрозой информационных конфликтов, включая кибератаки. Данное научное исследование охватывает обширный анализ актуальных угроз в области кибербезопасности, детально рассматривает разнообразные методы защиты от кибератак и предлагает подробное описание основных видов кибератак, применяемых инструментов, а также методов, подкрепленных конкретными примерами реальных инцидентов для более полного понимания серьезности данной проблемы. Далее в рамках исследования проводится анализ возможных последствий таких кибератак как для организаций, так и для частных лиц, выявляются уязвимые места и потенциальные угрозы. В заключении представлены современные методы обеспечения кибербезопасности и профилактики кибератак, стратегии по укреплению системы защиты от киберугроз, а также рекомендации по принятию мер, направленных на предотвращение подобных атак в будущем.

Ключевые слова: Кибератаки, информационная безопасность, информационные технологии, киберугроза, киберпреступность.

Annotation: In the modern world, the period of digitalization is characterized not only by rapid progress in the field of information technology, but is also accompanied by an increasing threat of information conflicts, including cyber-attacks. This research study covers an extensive analysis of current cybersecurity threats, examines in detail the various methods of protecting against cyber-attacks, and offers a detailed description of the main types of cyber-attacks, the tools used, and methods, supported by specific examples of real-life incidents to better understand the severity of this problem. Further, the study analyzes the possible consequences of such cyber-attacks for both organizations and individuals, identifying vulnerabilities and potential threats. In conclusion, modern methods for ensuring cybersecurity and preventing cyber-attacks, strategies for strengthening the system of protection against cyber threats, as well as recommendations for taking measures aimed at preventing similar attacks in the future are presented.

Key words: Cyber-attacks, information security, information technology, cyber threat, cybercrime.

В эпоху глобализации, наблюдается стремительный рост технического прогресса, который сопровождается развитием негативных явлений, включая увеличение преступности. С развитием компьютерных технологий растет количество преступных действий, связанных с электронным обменом информацией, в частности, террористическая деятельность. В настоящее время наблюдается увеличение числа террористических организаций, а также новых форм терроризма, таких как кибертерроризм. Угроза кибератак в настоящий момент представляет собой реальную опасность.

Постоянное совершенствование глобальной сети Интернет, что ведет к появлению новых перспектив, увеличению количества серверов, значительному увеличению объема информации и огромному потенциалу для развития мирового сообщества.

В современных реалиях интернет является общедоступной сетью, используемой подавляющим большинством людей в мире. Всероссийский центр изучения общественного мнения (ВЦИОМ) опубликовал исследование, согласно которому, доля интернет-пользователей в России на момент 2021 года составила 81%, а на сегодняшний день 84%, из которых 74% делают это ежедневно [1].

На сегодняшний день развитие человечества в целом и человека как личности в частности невозможно представить без использования прогрессивных информационных технологий. Однако

совершенствование данного направления порождает и новые угрозы, борьба с которыми в настоящее время является одним из основных направлений борьбы с угрозами национальной безопасности Российской Федерации.

Кибератаки стали одной из наиболее серьезных угроз в этой области. Эти атаки проводятся с использованием различных инструментов и методов и направлены на получение конфиденциальной информации, блокировку работы системы или даже ее уничтожение.

Кибератака, в узком смысле, — это покушение на компьютерную безопасность информационной системы [2]. По мнению доктора юридических наук, доцента Беровой Д.М. в широком смысле кибератака рассматривается как поиск решений, методов, конечной целью которых является получение контроля над удаленной системой в целях ее дестабилизации [3].

Преступления в киберпространстве по своей направленности можно разделить условно на три уровня:

- Гражданский уровень (почтовые вымогатели, кража платежных данных);
- Корпоративный уровень (кража клиентской базы и копирование уникальных технологий);
- Государственный уровень (кража данных, связанных с государственной тайной).

Киберпреступления классифицируются по следующим признакам:

По способу использования:

1. компьютер является объектом правонарушения;
2. компьютер используется как запоминающее устройство;
3. компьютер используется как средство, способствующее совершению

киберпреступления.

По наличию насилия:

1. насильственные и иные потенциально опасные (кибертерроризм, угроза физической расправы, киберпреследование, детская порнография);
2. ненасильственные (противоправное нарушение владения в киберпространстве, киберворовство, кибермошенничество).

По способу воздействия:

1. физические злоупотребления;
2. программные злоупотребления;
3. операционные злоупотребления;
4. электронные злоупотребления.

Существует множество различных типов кибератак, каждый из которых имеет свои уникальные характеристики и цели [4]. Некоторые из наиболее распространенных типов кибератак включают в себя:

– Вирусы — это программы, которые могут заражать компьютеры и другие устройства, распространяться через сети и наносить различные виды вреда, такие как уничтожение данных, блокировка работы системы и даже кража конфиденциальной информации;

– Черви — это программы, которые способны распространяться самостоятельно через сети и заражать множество компьютеров. Они могут наносить серьезный ущерб, блокируя работу системы и удаляя файлы;

– Троянские кони — это программы, которые могут маскироваться под обычные файлы и заражать компьютеры, предоставляя злоумышленникам удаленный доступ к устройству и конфиденциальной информации;

– Фишинг — это атака, которая предназначена для получения конфиденциальной информации, такой как пароли и номера кредитных карт, путем обмана пользователей и предоставления им ложной информации;

– DDoS-атаки — это атаки, которые направлены на блокирование работы системы путем перегрузки ее трафиком, что делает невозможным доступ к ресурсу;

– Атаки на инфраструктуру — это атаки, которые направлены на разрушение физической инфраструктуры, такой как электронные системы управления транспортом или электропитание.

Основными инструментами и методами кибератак могут быть:

1. Малварь (вредоносное ПО): Программное обеспечение, которое используется для

нарушения безопасности компьютерной системы. Это может быть вирус, червь, троянский конь или любой другой тип малвари. В 2017 году вирус WannaCry заразил более 200 000 компьютеров в 150 странах, используя уязвимость в операционной системе Windows. Этот вирус заблокировал доступ к файлам на компьютере и требовал выкуп за их восстановление.

2. Фишинг: Метод, используемый для получения личной информации, такой как логины и пароли, путем подделки ложных электронных писем или веб-сайтов. В 2016 году фишеры атаковали компанию Dropbox, отправляя ложные электронные письма с просьбой изменить пароль. Когда пользователи переходили по ссылке и вводили свой старый пароль, злоумышленники могли получить доступ к их аккаунтам.

3. Атаки на слабые места в системе: Киберпреступники могут искать уязвимости в компьютерных системах, чтобы получить несанкционированный доступ. В 2013 году компания Target была атакована киберпреступниками, которые использовали уязвимость в слабо защищенной системе точек продаж. В результате были украдены данные более 40 миллионов кредитных карт.

4. Социальная инженерия: Метод, включающий манипулирование человеческими действиями для получения конфиденциальной информации или доступа к системам. В 2018 году атаки бизнес-перехвата стали особенно популярны. Киберпреступники используют социальную инженерию, чтобы обмануть сотрудников компании и получить доступ к конфиденциальной информации, например, счетам на оплату.

5. Атаки на сеть: Метод, в котором киберпреступники направляют трафик на целевую систему, что может привести к перегрузке и отказу в обслуживании. В 2016 году киберпреступники провели одну из крупнейших атак DDoS на сайт провайдера DNS Dyn.

6. DDoS-атаки: Атака, которая направляет большой объем трафика на сервер, чтобы привести его к сбоям или перегрузке. В 2012 году атака DDoS была направлена на банк JPMorgan Chase.

7. Взлом паролей: Метод, в котором киберпреступники используют утилиты для взлома паролей и получения несанкционированного доступа к системам. В 2012 году хакеры получили доступ к базе данных LinkedIn, где хранились зашифрованные пароли пользователей.

8. Инженерия обратного проектирования: Метод, который используется для изучения кода программного обеспечения и выявления его уязвимостей. Например, в 2017 году была обнаружена кибератака на компанию Samsung, в ходе которой злоумышленники использовали инженерию обратного проектирования для изучения программного обеспечения компании и создания вредоносного кода, который был внедрен в мобильные устройства Samsung. Этот вредоносный код позволил киберпреступникам получить доступ к конфиденциальной информации, включая данные о кредитных картах и персональные данные пользователей.

9. Использование ботнетов: Ботнеты — это сети компьютеров, зараженных малварью, которые контролируются злоумышленниками для выполнения кибератак. В 2015 году была обнаружена атака на популярный сайт Ashley Madison, который предоставляет услуги знакомств для людей, ищущих внебрачные отношения. Киберпреступники внедрили вредоносный код на сайте, чтобы получить доступ к конфиденциальным данным клиентов, включая их имена, адреса электронной почты и кредитные карты.

Все эти инструменты и методы используются киберпреступниками для проведения кибератак с различными целями, включая кражу личных данных, шпионаж, получение выгоды и даже кибертерроризм.

Для организаций кибератаки могут вызвать существенные финансовые потери, вызванные утечкой конфиденциальных данных клиентов, снижением производительности и нарушением бизнес-процессов, что в свою очередь может повлечь за собой серьезное нарушение репутации и потерю доверия со стороны клиентов и партнеров.

Для частных лиц кибератаки могут привести к краже личных данных, таких как имена, адреса, номера социального страхования и кредитных карт, что повлечет за собой потенциальную угрозу кражи денег или ложное представление о личности. В случае утечки личной информации возможны проблемы с налоговыми декларациями, медицинскими записями и другими личными документами.

Последствия кибератак могут иметь серьезные последствия для потерпевших лиц, включая утечку конфиденциальной информации, нарушение функционирования систем, материальные потери

и утрату деловой репутации. Организации и частные лица должны осознавать, что предупредительные и защитные меры являются обязательными для предотвращения кибератак и обеспечения безопасности своих информационных систем и данных [6].

Современные стратегии защиты от кибератак включают в себя применение антивирусного программного обеспечения, механизмов защиты сети с помощью паролей, шифрования информации, а также использование других технологий [7].

На данный момент времени у преступников имеется большая база и выбор средств и орудий совершения преступления, это охарактеризовано в первую очередь быстрым ростом компьютерных и it технологий в мире. Не так давно в качестве орудия и средства совершения преступления злоумышленники стали использовать ИИ и его подсистемы.

Это в свою очередь позволило преступникам получить огромный доступ ко всем базам данным мира, тем самым давая больший простор для совершения преступных деяний в сфере киберпреступности.

Поскольку преступления, связанные с новыми технологиями, в частности с использованием искусственного интеллекта, являются совершенно новыми, а иногда могут требовать узко квалифицированных знаний, внесение изменений в Постановление Пленума Верховного Суда РФ сможет обеспечить правильное и единообразное толкование и применение данной нормы судами, а также раскрыть технические вопросы, связанные с пониманием и применением искусственного интеллекта в качестве средства совершения преступления понятным для судей языком. Следует определять ИИ как “способность компьютерной системы имитировать мышление человека”, данное определение дает наиболее сжатое понятие ИИ.

Стоит упомянуть тот факт, что применяя, ИИ в государственных учреждениях, ИИ может собирать всю информацию, а в дальнейшем доступ к этой информации могут, получают третьи лица, что может повлечь за собой преступления. К примеру, ИИ может создавать видеоролики с участием высокопоставленных чиновников, для этого необходимо наличие фотографий в базах данных или сети Интернет.

На данный момент времени преступления с использованием ИИ происходят ежедневно, а именно ИИ во многих браузерах и сети Интернет ведет сбор информации о каждом человеке, собирает личные данные: (пароли, логины, паспортные и личные данные, данные о геолокации лица) и эти данные хранятся в системе ИИ, при этом получить доступ к этим данным могут получить и третьи лица в следствии чего могут совершаться преступления.

Эффективное обеспечение безопасности от кибератак требует применения комплексных мер, включающих использование разнообразных технологий, обучение пользователей и содействие специализированных служб. Только такой интегрированный подход позволит достичь высокого уровня защиты и обеспечить безопасность информации от киберугроз.

Некоторые примеры современных методов защиты от кибератак включают:

– Многофакторная аутентификация — это метод, который требует от пользователя несколько форм аутентификации, например, пароля и кода, отправленного на мобильный телефон или по электронной почте. Это делает сложнее для злоумышленников получить доступ к системе;

– Криптография — шифрование данных может помочь защитить конфиденциальность информации. Криптографические алгоритмы используются для защиты данных в пути и в хранилище;

– Файрволы — это программные или аппаратные устройства, которые мониторят и фильтруют входящий и исходящий трафик в компьютерной сети. Файрволы могут быть настроены для блокировки доступа к определенным сайтам или приложениям;

– Обновления безопасности: обновления программного обеспечения, такие как патчи безопасности, могут закрывать уязвимости, которые могут быть использованы злоумышленниками. Обновления следует устанавливать как можно быстрее после их выпуска;

– Мониторинг безопасности — это процесс непрерывного мониторинга сети и систем на наличие возможных угроз. Можно использовать специализированные программы и устройства, чтобы отслеживать активность в сети и обнаруживать подозрительную деятельность.

Профилактика кибератак — это совокупность мер, направленных на предотвращение

возможности проведения кибератак и снижение рисков их возникновения. Рассмотрим основные меры профилактики [8]:

- Регулярное обновление программного обеспечения и системных утилит: обновления содержат исправления уязвимостей, которые могут быть использованы злоумышленниками для проведения кибератак;
- Использование сильных паролей и механизмов аутентификации: пароли должны быть уникальными, длинными и содержать буквы, цифры и специальные символы. Механизмы аутентификации, такие как двухфакторная аутентификация, помогают защитить учетные записи пользователей;
- Обучение пользователей: осведомленность пользователей о возможных угрозах и методах защиты поможет им более эффективно защищать свои устройства и данные;
- Использование антивирусных программ и брандмауэров: антивирусные программы помогают обнаруживать и блокировать вредоносные программы и уязвимости. Брандмауэры, в свою очередь, контролируют доступ к сети и блокируют нежелательный трафик;
- Регулярное создание резервных копий данных: резервные копии позволяют быстро восстановить данные в случае кибератаки или иных сбоев;
- Мониторинг сетевой активности: мониторинг сетевой активности позволяет выявлять аномалии в поведении сетевых устройств и оперативно реагировать на угрозы.

Важно понимать, что профилактика кибератак является непрерывным процессом, требующим постоянного обновления и усовершенствования мер защиты.

«Лаборатория Касперского» разработала интерактивную карту киберугроз[9], которая позволяет просматривать статистику по количеству кибератак на страны мира в режиме реального времени. Стабильно Россия занимает первую позицию по количеству направленных на ее структуры кибератак. Так, поданным OAS, т.е. автоматической проверки, которая показывает поток данных по вредоносным программам, обнаруженным во время открытия, копирования, запуска или сохранения файлов, ежедневно в России выявляется около 2 млнтских вредоносных программ. В США такой показатель достигает около 400тысяч.

Также следует отметить, что в Российской Федерации отсутствует документ, который содержал бы основные положения уголовной политики в сфере противодействия киберпреступлениям. В Российской Федерации действуют:

- Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646)[10];
- Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»[11];
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[12].

Однако данные нормативные акты не являются документами, в комплексе регулируемыми вопросы противодействия киберугрозам. Таким образом, обозначается необходимость разработать проект национальной концепции Стратегии кибербезопасности государства, которая должна быть базирована на принципах и законах других государственных документов, которые бы рассматривали ее реализацию на различных национальных уровнях и сферах [13]. Документ на уровне стратегии/концепции позволил бы не только сориентировать российского законодателя и правоприменительную практику в данной сфере, но и способствовал бы развитию международного сотрудничества, которое также чрезвычайно необходимо в области противодействия киберпреступлениям.

В заключении, следует отметить, что кибератаки превращаются во все более распространенное и опасное явление в современном информационном обществе. Их негативные последствия могут быть серьезными как для организаций, так и для отдельных граждан, включая укрывание личных данных, финансовые убытки, нарушение конфиденциальности, нарушение бизнес-процессов и даже угрозу национальной безопасности. Для защиты от кибератак необходимо использовать современные методы защиты и профилактические меры, такие как регулярное обновление программного обеспечения и антивирусных программ, обучение сотрудников организации в области информационной безопасности, использование многофакторной

аутентификации и шифрования данных. Также важнейшим способом противодействия данной угрозе является расширение познания государств в области киберпреступности и кибертерроризма, создание отдельных учреждений силовых структур и органов, направленных исключительно на борьбу против данного вида преступности. Выделение и разработка схем, тактики методов криминалистического познания, проведение более тщательного отбора на занимаемые места в инфраструктурах особой важности, создание и улучшение системы уровня допусков, к тем или иным объектам информации и технологий, привлечение более компетентных специалистов и иных лиц, сособыми знаниями, с целью противодействия киберпреступности [14]. Обеспечение безопасности информации представляется ключевым аспектом в современном информационном мире, и поэтому важно принимать все необходимые меры для защиты себя и своей организации от киберугроз.

Список использованных источников:

1. Всероссийский центр изучения общественного мнения (ВЦИОМ)[Электронный ресурс] // URL: <http://wciom.ru>. (дата обращения: 23.04.2024).
2. Кибератака - URL: <http://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%E0%F2%E0%EA%E0/> (Дата обращения 24.04.24).
3. Борова Д. М. Кибератаки как угроза информационной безопасности // Пробелы в российском законодательстве. Юридический журнал. – 2018. – №. 2. – С. 186-188.
4. Карханин Б. А. Анализ современных угроз кибератак и их негативного влияния // ББК 1 Н 34. – С. 2321.
5. Быков А. О. ББК 67.52 Б 95 П 82. – 2023.
6. Галкин Д. А. Кибератаки на работе: как обезопасить свой бизнес от утечек данных и вредоносных программ // Современные информационные технологии и информационная безопас. – 2024. – С. 37.
7. Пономарева С. В., Мустафаев Т. А. Кибербезопасность и защита сетевой инфраструктуры основных бизнес-процессов предприятий оборонно-промышленного комплекса России // Инновационная экономика: информация, аналитика, прогнозы. – 2023. – №. 3. – С. 154-161.
8. Ниёзов М. А. Современные проблемы защиты Информационных систем от кибератак и профилактика киберпреступлений. – 2022.
9. Интерактивная карта киберугроз [электронный ресурс]. – Режим доступа.— URL: <https://cybermap.kaspersky.com/ru> (дата обращения: 27.04.2024).
10. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
11. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».
12. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
13. Крайнова, Н. А. Юридическая конвергенция права и технологий в сфере противодействия киберугрозам / Н. А. Крайнова // Право и цифровая экономика. – 2021. – № 2(12). – С. 23-31. – DOI 10.17803/2618-8198.2021.12.2.023-031. – EDN AQKSLJ.
14. Фахриев И. Д. КИБЕР ТЕРРОРИЗМ КАК АКТУАЛЬНАЯ УГРОЗА ДЛЯ ГОСУДАРСТВА // Аллея науки. – 2020. – Т. 1. – №. 8. – С. 301-304.

**УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ФАКТОР СОЦИАЛЬНЫХ
КОНФЛИКТОВ В ПОСТИНДУСТРИАЛЬНОМ ОБЩЕСТВЕ
THREATS TO INFORMATION SECURITY AS A FACTOR OF SOCIAL CONFLICTS IN POST-
INDUSTRIAL SOCIETY**

Гасангусенова Айшат Магомедовна
студентка 1 курса, Северо-Кавказский институт
(филиал) ВГУЮ (РПА Минюста России)
г. Махачкала, Россия
Email: aishatgasang@gmail.com
Gasangusenova Aishat Magomedovna
1st year student, North Caucasus Institute
(branch) VGUY (RPA of the Ministry of Justice of Russia)
Makhachkala, Russia
Email: aishatgasang@gmail.com

Аннотация. Постиндустриальное общество характеризуется глубокими трансформациями социальной структуры, вследствие чего формируется бесклассовая система стратификации. Именно поэтому в постиндустриальном обществе значительную опасность представляют социальные конфликты, которые могут возникать, вследствие нарушений информационной безопасности на макро- и микроуровнях социума.

Ключевые слова: информация, информационная безопасность, глобальный миропорядок, социальный конфликт, постиндустриальное общество.

Annotation. Post-industrial society is characterized by deep transformations of the social structure, as a result of which a classless stratification system is formed. That is why in a post-industrial society, social conflicts that can arise due to violations of information security at the macro and micro levels of society pose a significant danger.

Keywords: information, information security, global world order, social conflict, post-industrial society.

Постиндустриальное общество прошло активный период генезиса и развития во второй половине XX в. Достаточно быстро социологическая наука пришла к выводу о том, что информация и информационные технологии являются основой нового общества. В этом многим ученым виделась инновационная технологическая составляющая нового социума. Отличительной особенностью такого социума выступает не только и не столько информация и информационно-компьютерные технологии. Речь идет о продуцировании сетевых структур, в основном связанных с интернет-средой. Горизонтальные связи индивидов и групп, интегрированные в пространство коммуникаций, создают принципиально новую социальную архитектуру, носящую уникальный характер. Таким образом, классическое социологическое позиционирование постиндустриального общества акцентирует внимание на его бесклассовом характере, во многом исключая традиционные антагонистические конфликты, описанные в свое время классиками марксизма. Так, в обществе XXI в. информация и информационные технологии выходят на первый план, все сильнее влияют на политическую, экономическую, социальную и культурную подсистемы общества.

Угрозами для безопасности России выделяют в основном международный криминал, незаконный оборот наркотиков, распространение оружия и боеприпасов. На сегодняшний день активно развит информационный экстремизм. Социальные сети стали неотъемлемой частью жизни для большинства граждан. Из социальных сетей мы узнаем актуальные новости, знакомимся с различными пропагандами, сталкиваемся и с информационным экстремизмом. Субъекты экстремизма воздействуют на массы людей сценами насилия и открытостью своих суждений, тем самым пытаются манипулировать сознанием людей. Большинство граждан доверяет подобной информации, что негативно сказывается на их психике. Мы считаем, что необходимо создать новые ценности,

преподнести новые позитивные общественные взгляды.

Постепенное усиление социального воздействия информации предполагает ее априорную ценность, а с другой стороны, показывает опасность дезинформации, нарушения целостности информации, снижения ее качества. Именно поэтому дисфункции в информационной среде справедливо относятся многими современными исследователями именно к категории угроз информационной безопасности. Подобные проблемы, в свою очередь, создают благодатную почву и для развития социальных конфликтов в постиндустриальном обществе. Именно обладание информацией предоставляет доминирующие позиции в обществе XXI в.; соответственно, дисфункции обращения информации, информационного взаимодействия потенциально провоцируют конфликты.

По мнению исследователей, «любой конфликт, связанный с деятельностью людей в рамках всего общества, коллектива или группы, может быть охарактеризован как социальный конфликт. При этом различные теории конфликта могут различаться в определении причин конфликта, его форм, видов, особенностей проявления и т.п.» [1].

И. Л. Бачило отмечает, что нынешний этап развития информационных отношений характеризуется возможностью информационного воздействия на индивидуальное и общественное сознание, вплоть до угрозы информационных войн, в результате чего неизбежным противовесом свободы информации становится проблема информационной безопасности.

Сегодня большое влияние уделяется иноагентам. Иноагенты – это организация, объединения людей, СМИ, которые, по мнению государства, делают что-то в интересах другой страны или иностранных структур. Иноагенты пропагандируют свою «политику», дезинформируют граждан, отравляют им разум, вследствие чего часть граждан может поддержать идеи и мысли иноагентов и распространять их информацию другим людям. В дальнейшем за такие действия граждане могут понести уголовное наказание. В основном иноагентами признают журналистов, которые пользуются большой популярностью у молодежи. Глобальная сеть Интернет является благодатной средой для информационного экстремизма. Если говорить про предупреждение экстремизма и терроризма, то это большая проблема, которую невозможно решить исключительно при помощи правоприменительной деятельности одного органа государственной власти.

Чем сложнее социальная структура, чем более дифференцировано общество, чем больше в нем свободы, плюрализма, тем больше несовпадающих, а порой и взаимоисключающих интересов, целей, ценностей, и, соответственно, больше источников для потенциальных конфликтов» [2].

В свою очередь, Т.Н. Жуйкова указывает, что в связи с неизбежностью конфликтов «следует научиться распознавать и, по возможности, управлять ими, чтобы они протекали безболезненно как для участников конфликта, так и общества в целом. Опасные последствия несут негативные проявления социального конфликта: физическое и психологическое насилие; формирование негативного «образа врага»; инкриминирование группе отклоняющегося поведения по одному частному случаю; упрощение и схематизация реальности» [3].

В информационном обществе важную роль играют электронные масс-медиа и Интернет. Управление такой сложной системой требует консолидации усилий различных факторов внешней и внутренней среды: индивидов, групп, общностей, организаций, институтов. Следует обратить внимание на то, что информационная безопасность связана с эффективным действием механизмов социального контроля и управления системой средств массовой коммуникации, вследствие чего возникает состояние защищенности информационно-коммуникационного пространства на макро- и микроуровнях, обеспечивающее гармоничное развитие личности, общества и государства [4].

Научно-технический прогресс приводит к появлению новых технологий, которые используются не только в позитивных целях для развития общественных отношений, но и для негативных. Обеспечение информационной безопасности связано с различными аспектами современного общества. Существенным фактором риска макросреды общественной жизни выступает глобализация, связанная с формированием единого мирового пространства, стиранием пространственно-временных границ, всемирной интеграцией национальных государств в единую микросистему. Одним из инструментов глобализационного воздействия выступает массовая культура потребления. На первый взгляд, продвижение подобной наднациональной формы культуры должно способствовать

интеграции стран, культур, менталитетов народов и т.п. Система обеспечения информационной безопасности связана с тем, что общество XXI в. считается открытым. Это означает не только открытость информационных каналов, легкость коммуникации и т.п. Многие барьеры в настоящее время оказались сняты, в том числе и духовные, связанные с моралью, нравственностью. Зачастую в Интернете и на телевизионных каналах демонстрируются сцены насилия, агрессии, криминального поведения. Это воздействие формирует особое агрессивное социальное настроение, весьма благоприятное для развития конфликтов. Сложность современной проблемной ситуации в том, что она не имеет очевидных вариантов решения, так как цензура и запреты в целом - явление архаическое, свойственное более ранним формам общественной организации и не соответствует прогрессивному развитию общества, а поиск какого-то устраивающего все стороны консенсуса может существенно затянуться. С пространственной точки зрения их целесообразно системно анализировать на взаимосвязанных уровнях: глобальном, международном, национальном, региональном и местном.

Для решения этой задачи, в том числе в молодежной среде, необходимо создать самовоспроизводящуюся систему идей, субъектов-носителей и каналов их распространения, которая сможет автономно от государства способствовать формированию позитивного общественного сознания, исключающего, саму возможность использования насилия для достижения каких-либо целей. Такой системой могут и должны стать институты гражданского общества, научного и бизнес-сообщества, образовательные структуры и средства массовой информации.

Подводя некоторые итоги, целесообразно отметить, что состояние информационной безопасности играет важную роль в обеспечении стабильного развития социума. В свою очередь, подобное равновесное положение социальной системы выступает фактором в целом бесконфликтного существования групп, общностей, организаций, корпораций и т.п. Уровень конфликтности при таком развитии событий остается незначительным и не превышает средних значений, что свидетельствует лишь о том, что мы имеем дело с живой, а не мертвой социальной системой. Однако нарушение информационной гармонии, стабильности, целостности, общего качества информации - показатель не только дисбаланса информационной безопасности, но и, одновременно, фактор развития социальных конфликтов. В процессе управления информационной подсистемой современного общества важное значение имеет способность научного, объективного анализа сложившейся обстановки и поиска эффективных управленческих решений. Только так в обществе XXI в. представляется возможным вовремя предотвращать социальные конфликты, берущие свое начало в информационной среде общественной жизни. Утрата управляющих функций приводит к росту отклонений в информационно-коммуникационной сфере и, как следствие, к социальным конфликтам. В данном аспекте неоспоримым преимуществом обладают эмпирические социологические исследования, обладающие способностью осуществлять как статический, так и динамический анализ общества в целом, его отдельных подсистем и структурных элементов, в том числе и информационной сферы. Это направление сотрудничества науки и практики социального управления представляется наиболее перспективным в современных условиях.

Список литературы:

1. Маклюэн. М. Понимание медиа: внешние расширения человека. М.
3. Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе / пер. с англ. А. Матвеева; под ред. В. Харитонова. Екатеринбург.
4. Каспаров А.Р. Конфликтологический потенциал в российской полиции: соционормативное измерение: канд. социол. наук. Краснодар.
5. Иванихин А.А. Социальные конфликты в современном мире: дис. канд. филос. наук. Москва.
6. Жуйкова Т.Н. Социальный конфликт как предмет научного изучения // Вестник Воронежского института МВД России. № 4.
7. Жуйков А.А. Информационная безопасность в условиях генезиса виртуального пространства трансформирующегося российского общества: дис. . канд. социол. наук. Краснодар.

8. Жуйков А.А. Современные проблемы информационной безопасности // Вестник Краснодарского университета МВД России. № 4.

**УЧЕТНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ
ACCOUNTINGASPECTSOFFENSURINGECONOMICSECURITY**

**Джамалутдинова Наида Хайбулаевна
367009, г. Махачкала, ул. Акушинского, д.7
Jamalutdinova Naida Khaibulaevna
367009, Makhachkala, Akushinskystr., d. 7**

Аннотация: Отмечена актуальность направлений развития естественных наук в целях обеспечения экономической безопасности организации, включающих психологические аспекты в бухгалтерском учете. Указана необходимость изменений, включающих автоматизацию бухгалтерского учета с использованием систем искусственного интеллекта и биткойна как цифровой валюты.

Ключевые слова: учетная политика, анализ, экономическая безопасность, организация, контракты, договорная политика, финансовые результаты.

Abstract: The relevance of the directions of the development of natural sciences in order to ensure the economic security of the organization, including psychological aspects in accounting, is noted. The need for changes is indicated, including automation of accounting using artificial intelligence systems and bitcoin as a digital currency.

Keywords: accounting policy, analysis, economic security, organization, contracts, contractual policy, financial results.

Одним из важных условий устойчивого развития хозяйствующего субъекта и обеспечения его экономической безопасности является совершенствование учетно-аналитической системы. Поэтому данная система развивается в целях обеспечения пользователей достоверной информацией для принятия эффективных управленческих решений и повышения конкурентоспособности в рыночных условиях хозяйствования. Ученые-экономисты в своих исследованиях предлагают разные определения данного понятия. Учетно-аналитическую систему в широком смысле они характеризуют как сбор, обработку, регистрацию и оценку всех видов информации, необходимой для принятия управленческих решений. А в более узком смысле – как четыре вида информации: нормативная, бухгалтерская (учетная), аналитическая, не учетная [1, с. 178]. Характерной особенностью рыночного хозяйства в целом, а для российских предприятий в частности, являются сравнительно новые проблемы, связанные с управлением экономической безопасностью. При неудовлетворительной организации экономической безопасности предприятия теряют контрагентов, сокращаются объемы производства и реализация продукции, увеличиваются затраты и, соответственно, уменьшаются доходы и прибыль. В конечном итоге убыточная деятельность ведет к главной опасности – банкротству. Поэтому для хозяйствующих субъектов проблема обеспечения экономической безопасности приобрела в настоящее время первостепенное значение.

Общепризнанным фактом в мировой экономике является непосредственная зависимость экономической безопасности от достоверности учета и финансовой отчетности. Подтверждением этого является банкротство крупных западных компаний, причиной которых стали нарушения и мошенничества в бухгалтерском учете и финансовой отчетности. В учетно-экономическую систему могут быть включены разные виды отчетности: финансовая, налоговая, управленческая, нефинансовая [2, с. 939]. При этом учетно-аналитическая система должна отвечать интересам как внешних, так и внутренних пользователей. От качества организации бухгалтерского учета находится в прямой зависимости экономическая безопасность не только отдельных организаций и учреждений, но и всей социально-экономической сферы государства, а также и мировой экономики.

Анализ законодательно-нормативного регулирования бухгалтерского учета показывает, что основным требованием формирования учетной политики организации является принцип

рациональности. Требование рациональности – это периодическое проведение сравнительного анализа доходов, которые должны превышать затраты, связанные с функционированием учетно-аналитической системы организации. Это означает, что учетно-аналитическая система способна принести прибыль и тем самым обеспечить экономическую безопасность хозяйственной деятельности организации.

Важным аспектом развития учетно-аналитической системы является обеспечение стабильности функционирования и экономической безопасности бизнеса в кризисных условиях хозяйствования. В связи с распространением за последнее десятилетие институциональной теории бухгалтерского учета появилась необходимость разработки дизайна учетно-аналитической системы. Такая необходимость предопределена увеличением объема учетной информации и необходимостью ее экономического анализа.

Среди основных принципов создания учетных систем важнейшим, на наш взгляд, является его разработка как нового направления развития информационной системы для организации. Актуальность направления заключается в том, что в современном корпоративном мире появился новый тип институционального субъекта – экспоненциальная организация. Экспоненциальная организация оказывает несоизмеримо большее воздействие по сравнению с другими аналогичными организациями благодаря использованию новой организационной модели и быстроразвивающихся технологий [3, с. 228]. Такие организации отличаются от других с точки зрения стратегии, структуры, культуры, процессов, систем, показателей деятельности. Экспоненциальные организации опираются на информационные технологии, которые переводят материальное в цифровую форму и делают их доступными для всех людей. Естественно, учетно-аналитическая система также должна соответствовать данной организационной форме, которая исторически отличалась осторожностью и консервативностью.

В области бухгалтерского учета и аудита также предстоят революционные изменения, включающие автоматизацию бухгалтерского учета с использованием систем искусственного интеллекта и блокчейна как цифровой валюты и цифровых платежных систем. Данное направление включает в себя: автоматическое напоминание о реальной задолженности; автоматическое управление налогообложением; систему выявления отклонений на стадии исполнения договорных обязательств и др. В результате усилится налоговый контроль государства, что приведет к «бегству» капитала в офшорные зоны.

Современный мир – это мир трансакций, осуществляемых на основе заключения коммерческих, социальных, коммуникационных договоров и смарт-контрактов. Так, учетно-аналитическая система, построенная на инфраструктуре блокчейна, по мнению многих специалистов, способна обходиться без проведения обязательных аудиторских проверок. Организационные формы учетно-аналитических систем оказывают непосредственное влияние на обеспечение экономической безопасности не только отдельных организаций и учреждений, но и всей социально-экономической сферы государства, а также и мировой экономики. Поэтому важное значение приобретает анализ влияния учетной политики на финансовые результаты деятельности организации с тем, чтобы ее откорректировать в случае необходимости.

Важнейшим условием развития учетно-аналитической системы является обеспечение стабильности функционирования и экономической безопасности бизнеса в кризисных условиях хозяйствования.

Список использованных источников:

1. Андреева Л.В., Бодрова Т.В., Зубарева Е.В. Учетно-аналитическая система: теория и практика. / монография. – Москва: Изд-торговая корпорация «Дашков и Ко», 2022. – 311 с.
2. Цакаев А. Х. Пропорциональное регулирование финансового рынка в обеспечении экономической безопасности России // Экономическая безопасность. – 2021. – № 4. – с. 927–942.
3. Салим Исмаил, Майкл Мэлоун, Юри ван Геест Взрывной рост. Почему экспоненциальные организации в десятки раз продуктивнее вашей (и что с этим делать). – М.: Альпина Пэблишер, 2020. – 435 с.

**ФАКТОРЫ РИСКА ПРИ ПРИНЯТИИ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ В ПЕРИОД
ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЭКОНОМИКИ РФ
RISK FACTORS WHEN MAKING MANAGEMENT DECISIONS DURING THE DIGITAL
TRANSFORMATION OF THE RF ECONOMY**

Н.П. Докторова

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНЕЦКАЯ АКАДЕМИЯ УПРАВЛЕНИЯ И
ГОСУДАРСТВЕННОЙ СЛУЖБЫ», Россия, 283015, ДНР, г. Донецк, ул. Челюскинцев, 163-а,
email: doktorovanp@gmail.com**

**FEDERAL STATE BUDGETARY EDUCATIONAL INSTITUTION OF HIGHER EDUCATION
“DONETSK ACADEMY OF MANAGEMENT AND PUBLIC SERVICE”, Russia, 283015, DPR,
Donetsk, st. Chelyuskintsev, 163-a, email: doktorovanp@gmail.com**

Аннотация: В статье рассматривается влияние цифровой трансформации на управленческие решения и риски, с которыми сталкиваются лица, отвечающие за эти решения. Приведена классификация рискованных факторов, возникающие при принятии управленческих решений в условиях цифровой трансформации экономики РФ. Особое внимание уделяется информационной безопасности и цифровой защите данных. В статье анализируется как внешние, так и внутренние рискованные факторы. Внешние факторы включают в себя изменения законодательства, геополитическую обстановку, экономическую нестабильность и т.д. Внутренние риски могут включать в себя недостаточную квалификацию персонала, неэффективное использование ресурсов, недостаточную цифровую защиту данных и т.д.

Ключевые слова: управленческие решения, цифровая трансформация, риски, неопределенность.

Abstract: The article examines the impact of digital transformation on management decisions and the risks faced by those responsible for these decisions. A classification of risk factors that arise when making management decisions in the context of the digital transformation of the Russian economy is given. Particular attention is paid to information security and digital data protection. The article analyzes both external and internal risk factors. External factors include changes in legislation, geopolitical situation, economic instability, etc. Internal risks may include insufficient personnel qualifications, inefficient use of resources, insufficient digital data protection, etc.

Keywords: management decisions, digital transformation, risks, uncertainty.

Введение

Результативность управленческой деятельности на любом предприятии и любой сферы зависит в первую очередь от правильности заранее принятых управленческих решений лиц ответственных за их реализацию. Степень сложности при принятии управленческого решения зависит непосредственно от степени осведомленности ответственного лица о факторах, оказывающих воздействия на принимаемое решение. Наиболее оптимальные условия – это условия полной определенности и информированности о всех возможных факторах и вариантах развития событий. Однако, в реальной жизни такие условия при принятии управленческих решений встречаются чрезвычайно редко. Зачастую ответственные лица сталкиваются с условиями информационной неопределенности или внешнего воздействия на принимаемое решение, что обуславливает возникновение риска принятия некорректного или неправильного управленческого решения.

На сегодняшний день экономика РФ претерпевает значительные качественные изменения, вызванные запущенным процессом цифровой трансформации [1]. Данная трансформация нацелена на развитие существующей экономической системы, а также на значительное упрощение ведения экономической деятельности всем субъектам. Однако, как и любая трансформация в непосредственном процессе преобразования на первых этапах несет помимо большой пользы, так же

и множество возникающих рисков и неопределенностей, особенно для лиц ответственных за принятие управленческих решений.

Цель исследования заключается в изучении и классификации факторов риска и иных неопределенностей, возникающих у ответственных лиц, при принятии управленческих решений в период цифровой трансформации экономики РФ.

Материал и методы исследования. Понимание неизбежности появления рисков при принятии управленческих решений стимулирует разработку методов прогнозирования и предотвращения негативных последствий, а также оперативного реагирования на события с целью уменьшения убытков. Для выработки механизмов оперативного выявления таких рисков и применения эффективных мер по их снижению необходимо выявить факторы, способствующие возникновению таких неблагоприятных ситуаций.

В начале исследования необходимо определиться с вводными данными. Одним из таких вводных является определение степени цифровой трансформации бизнес-среды на текущем этапе развития, т.к. недостаточная цифровизация субъектов экономики может стать отдельным рисковым фактором для лиц ответственных за принятие управленческих решений [4].

В 2022 году банком «Открытие» совместно с аналитическим центром НАФИ был проведен всесторонний анализ уровня цифровизации бизнеса [2]. На основе опросов была проанализирована динамика изменения индексов цифровизации бизнеса. К данным индексам относятся следующие направления, а именно исследование степени использования цифровых каналов передачи данных, что подразумевает оценку степени применения различных облачных технологий, систем автоматизации и электронных систем общения, таких как электронная почта и мессенджеры.

Следующим индексом является внедрение современных информационных технологий в непосредственное рабочее пространство. Сюда относятся системы автоматизации документооборота, использование нейросетей и трехмерной печати.

Следующим индексом является внедрение и использование сети интернет для развития компаний и маркетинговых продвижений.

И самым главным индексом, от которого непосредственно зависит возникновение рисков факторов, является обеспечение информационной безопасности и цифровой защиты данных, благодаря использованию специализированных антивирусных программ. Отдельного упоминания стоит индекс вовлеченности как руководящего, так и рядового персонала компаний к развитию и обучению новым внедряемым цифровым технологиям. Динамика данных показателей в процентных пунктах представлена на рис. 1.

Данная динамика показывает стабильный рост общего показателя цифровизации бизнеса, что безусловно является положительным показателем происходящей цифровой трансформации экономики РФ. Однако, по ключевым показателям степени использования цифровых каналов передачи данных и внедрения современных информационных технологий в непосредственное рабочее пространство наблюдается некоторая стагнация по сравнению с предыдущим 2021 годом.

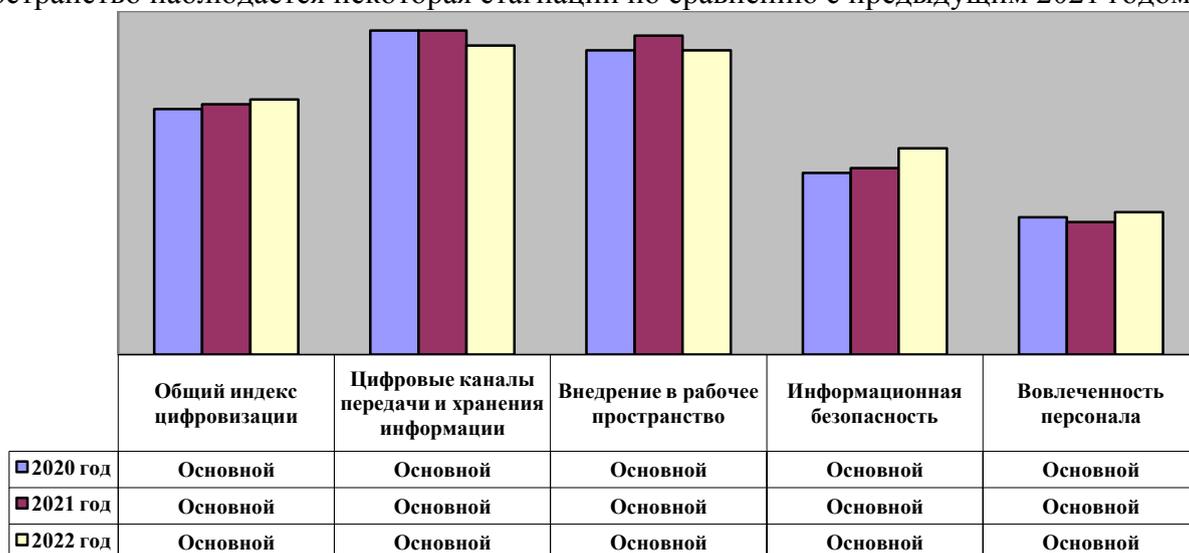


Рисунок 1 – Динамика показателей уровня цифровизации бизнеса [2].

Важным фактором является индекс информационной безопасности и цифровой защиты данных. Несмотря на рост до 42 процентных пунктов в 2022 году по сравнению с предыдущими годами данный процентный показатель является недостаточным для исключения данной угрозы из списка рисков факторов, которым подвержены лица ответственные за принятие управленческих решений. Сохраняется достаточная угроза утечки конфиденциальных корпоративных и личных данных.

В сравнении с аналогичным периодом в 2021 году, наблюдается заметный прирост заинтересованности юридических лиц в использовании антивирусных программ — на 40%, а также специализированных инструментов для защиты бизнеса — на 22%. При этом доля компаний, не обеспечивающих защиту своих данных, сократилась на 12 процентных пунктов. При исследовании столичных компаний отмечается больше пунктов мониторинга для обнаружения сетевых атак по сравнению с регионами — 11% против 4%. А вот в региональных компаниях значительно чаще применяются антивирусные продукты для защиты физических лиц — до 46%. Кроме того, индивидуальные предприниматели, отлично от юридических лиц, более активно применяют специализированные программные решения для обеспечения безопасности бизнеса — 30% по сравнению с 11%. И они более склонны к использованию центров мониторинга сетевых атак — 7% против 1% [2].

Однако, несмотря на положительную динамику, опрос, проведенный в данном исследовании, показывает, что по состоянию на осень 2022 года 18% компании вообще не используют какие-либо программы для защиты данных, что является большой проблемой для обеспечения глобальной цифровой и информационной безопасности.

При этом присутствует и положительная динамика в желании компаний обучать свой персонал использованию новых цифровых технологий и информационных систем, что в будущем окажет и положительную динамику на информационную безопасность за счет возросшей цифровой грамотности участников бизнес-процессов.

Исследование показывает, что обязательные курсы для персонала предоставляют лишь 8% всех компаний, что выше на 5 процентных пунктов, чем год назад. Другие 7% оплачивают обучение по желанию работников, оставаясь на том же уровне, что и в ноябре 2021 года. Также с ноября 2021 года доля компаний, организующих обучение самостоятельно, увеличилась на 7 процентных пунктов, достигнув 22% [2].

Изменения окружающей бизнес-среды, вызванные цифровой трансформацией экономики РФ, бросают вызов управленцам всех уровней в борьбе с возникающими разнообразными рисковыми факторами.

Условно рисковые факторы, оказывающие влияние на лиц, принимающих управленческие решения, можно разделить по направлению своего воздействия на внешние и внутренние.

Внешние факторы влияют на всю экономическую среду в целом, внутренние же воздействуют на конкретную ее часть или предприятие. Систематизация и классификация всех рисковых факторов представлена в таблице 1.

Таблица 1 - Классификация рисковых факторов, влияющих на принятие управленческих решений.

Критерии классификации	Факторы
Внешние факторы	Естественные бедствия и природно-климатические изменения (вероятность возникновения форс-мажорных ситуаций из-за метеорологических явлений, таких как засухи и природные пожары, морозы, град, сильные ветры, наводнения); Экологические угрозы (вспышки заболеваний);

	<p>Социально-экономическая обстановка в регионе и мировой арене (закрытие предприятий в связи с пандемией, изменения в мировой политике и экономике, колебания цен на сырье, спад спроса на местные товары и услуги и т.д.);</p> <p>Геополитические и военные факторы (военные действия, политическая изоляция);</p> <p>Нормативные и законодательные ограничения (недостатки или противоречия в законодательстве, а также непредвиденные действия государственных органов);</p> <p>Коррупция;</p> <p>Технологические риски, вызванные скачками в научно-техническом прогрессе.</p>
Внутренние факторы	<p>Производственные проблемы (низкое качество поставляемого сырья, износ оборудования и производственных ресурсов);</p> <p>Социальные вызовы (нехватка квалифицированных кадров, человеческий фактор (ошибки в расчетах и прогнозах), снижение деловой активности на рынке и т.д.);</p> <p>Финансовые и экономические трудности (рост цен на сырье и энергоносители, неплатежеспособность партнеров, увеличение налогов);</p> <p>Утечки информации, вызванные недостаточной защитой данных.</p>

При принятии любого управленческого решения необходимо придерживаться широкого и разностороннего подхода к учету и анализу рисков факторов как внешних, так и внутренних, а также их взаимосвязи в контексте целей решаемой задачи.

Данные критерии классификации рисков факторов носят в значительной степени условный характер. Зачастую провести строгую границу между некоторыми типами рисков факторов не представляется возможным. Это обусловлено тем, что на практике наблюдается многочисленными проявления рисков факторов, которые могут попадать под разные категории, однако все они оказывают воздействие на результаты бизнеса и требуют учета при принятии управленческих решений. Например, риск финансовых потерь из-за неплатежеспособности партнеров и риск утраты доверия клиентов из-за некачественной продукции могут представляться разными по своей сути, но оба они могут существенно повлиять на успех компании. Ответственные лица, принимающие управленческие решения, должны учитывать эту сложность при анализе рисков факторов и разработке стратегий их управления.

В контексте управления рисками необходимо учитывать не только конкретные проявления рисков, но и их потенциальное воздействие на бизнес и возможные стратегии реагирования.

Одним из способов нивелирования ситуации с учетом внутренних рисков факторов может быть вовлечение персонала в процесс принятия управленческих решений. Привлекая персонал к принятию управленческих решений лица ответственные за это, могут рассчитывать на более полное понимание возможных последствий и на более гибкое реагирование на них [3].

Еще одним методом принятия управленческих решений в условиях значительного числа рисков факторов является использование метода дерева решений. Данный метод представляет собой графическую модель, которая позволяет провести систематизацию различных вариантов решений и анализ их последствий в условиях неопределенности и риска.

Процесс построения дерева решений начинается с определения основной проблемы или задачи. Затем идет идентификация всех возможных альтернативных вариантов решения, а также оценка вероятности возникновения различных сценариев и их возможных результатов.

Наряду с основным преимуществом данного метода, которое заключается в учете значительного числа рисков факторов и возможных решений по их учету, а также визуализация данного процесса принятия решений, что в комплексе с современными цифровыми технологиями делает его очень наглядным и действенным, существует и ряд недостатков. Для успешного

применения данного метода необходимо точное определение возможных исходов и оценку вероятностей, что может потребовать значительных ресурсов.

Результаты исследования и их обсуждение. Для успешной работы и принятия правильных и взвешенных управленческих решений в современном мире цифровой трансформации необходимо уделять значительное время и ресурсы на освоивание новых технологий. На сегодняшний день исследования, проводимые аналитическими агентствами, показывают значительный рост цифровой грамотности в корпоративной среде, однако он все равно далек от всеобщего, что делает работу лиц ответственных за принятие управленческих решений сопряженную с наличием и учетом рисков факторов.

Одним из них, как показало исследование, является низкий уровень корпоративной информационно безопасности. Вообще не заботятся 18% опрошенных компаний о наличии даже простого антивируса, что открывает огромные возможности по краже конфиденциальной информации от конкурентов или других злоумышленников.

Особое внимание должно быть уделено развитию как управленческого, так и рядового персонала для работы в новых цифровых условиях, а также для понимания тех рисков и угроз, которые сопряжены с ними.

Выводы

Цифровая трансформация экономики РФ создала дополнительную нагрузку на лиц ответственных за принятие управленческих решений за счет необходимости учета дополнительных рисков факторов. Однако, наряду с дополнительными рисками появляется, и дополнительная возможность принимать решения более выверенно с учётом обработки гораздо большего числа данных и анализом гораздо больше числа возможных рисков факторов.

А внедрение современных информационных систем при использовании метода дерева решений и принятии управленческого решения, сопряженного с рисковыми факторами, позволит сделать его наглядным и действенным.

Список литературы

1. Программа "Цифровая экономика Российской Федерации" // Официальный сайт Правительства РФ. [Электронный ресурс]. URL: <http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf> (дата обращения: 09.03.2024).
2. Банк «Открытие»: интерес малого бизнеса к цифровизации и удаленной работе резко вырос в 2022 году // Аналитический центр НАФИ – исследовательские решения для вашего бизнеса [Электронный ресурс]. URL: <https://nafi.ru/analytics/bank-otkrytie-interes-malogo-biznesa-k-tsifrovizatsii-udalennoy-rabote-rezko-vyros-v-2022-godu> (дата обращения: 09.03.2024).
3. Ромодан Ю. О., Кинаш А. О. Участие работников в управлении организацией // Управление стратегическим развитием основных сфер и отраслей народного хозяйства в условиях современных вызовов: Материалы международной научно-практической конференции (Донецк, 02–03 ноября 2022 г.). Донецк: Донецкая академия управления и государственной службы при Главе Донецкой Народной Республики. 2022. С.149-153.
4. Докторова Н. П. Использование информационных технологий в принятии управленческих решений в здравоохранении ДНР // Сборник научных работ серии "Государственное управление". 2023. №31. С.124-135.

**ОБЕСПЕЧЕНИЕ УСТОЙЧИВОГО ЭКОНОМИЧЕСКОГО РАЗВИТИЯ
СЕЛЬСКОХОЗЯЙСТВЕННЫХ ОРГАНИЗАЦИЙ НА ОСНОВЕ
СОВЕРШЕНСТВОВАНИЯ ИНФРАСТРУКТУРЫ
ENSURING SUSTAINABLE ECONOMIC DEVELOPMENT OF
AGRICULTURAL ORGANIZATIONS BASED ON INFRASTRUCTURE
IMPROVEMENT**

И.В. Журова

**Белорусская государственная сельскохозяйственная академия,
г. Горки, Беларусь, e-mail: 010219871@mail.ru**

I.V. Zhurova

**Belarusian State Agricultural Academy,
Gorki, Belarus, e-mail: 010219871@mail.ru**

Аннотация: В статье рассмотрены особенности обеспечения устойчивого экономического развития сельскохозяйственных организаций на основе расширения региональной сбытовой кооперации. Обоснованы организационно-экономические аспекты создания и развития регионального информационно-консультационного центра по сбыту овощной продукции, его месторасположение в Могилевской области, выполнен прогноз основных направлений развития.

Ключевые слова: регион, устойчивое экономическое развитие, овощная продукция, сбыт

Abstract: The article considers the features of ensuring sustainable economic development of agricultural organizations based on the expansion of regional sales cooperation. The organizational and economic aspects of the creation and development of a regional information and consulting center for the sale of vegetable products, its location in the Mogilev region, and the forecast of the main directions of development are substantiated.

Keywords: region, sustainable economic development, vegetable products, sales

Введение.

В настоящее время деятельность сельскохозяйственных организаций по производству овощной продукции открытого грунта характеризуется невысоким уровнем слаженности процессов на всех этапах движения продукции (от момента сбора урожая до поставки конечному потребителю), в связи с чем функция управления сбытом приобрела ведущую роль. Сбыт обеспечивает связь производственного процесса с процессом реализации полученной продукции, обеспечивая стабильность и непрерывность поставок продукции на рынок.

Для обеспечения устойчивого экономического развития сельскохозяйственным организациям недостаточно только производить продукцию в объемах, предусмотренных производственными планами и программами, важно ее реализовать. Это предполагает переход сельскохозяйственных организаций от производственно-сбытовой ориентации к маркетинговой.

Цель исследования заключается в исследовании условий формирования, углублении теоретико-методологических основ обеспечения устойчивого экономического развития сельскохозяйственных организаций на основе расширения региональной сбытовой кооперации. Объект исследования – функционирование рынка сбыта овощной продукции. Предмет исследования – развитие теоретико-методологических основ обеспечения расширения региональной сбытовой кооперации сельскохозяйственных организаций.

Материал и методы исследования. Информационный материал для написания статьи получен на основе изучения научных публикаций, бухгалтерской (финансовой) отчетности организаций и других официальных периодических изданий аналитического характера [1–4].

При проведении исследования использовались общенаучные методы анализа и синтеза, обобщения, сравнения, абстрактно-логический и др.

Результаты и их обсуждение. Проведенные исследования деятельности сельскохозяйственных организаций Могилевской области позволили сделать вывод о том, что в настоящее время имеются существенные проблемы с организацией сбыта полученной овощной продукции открытого грунта. В таблице 1 приведены данные о фактическом уровне товарности продукции овощеводческих организаций Могилевской области.

Таблица 1 – Уровень товарности овощной продукции, произведенной овощеводческими организациями Могилевской области

Наименование организации	Вид овощей	Валовой сбор продукции с учетом скидки на естественную убыль, т	Объем реализации, т	Уровень товарности продукции, %
ОАО «Рассвет имени К. П. Орловского»	Капуста	1409,3	650,8	46,18
	Свекла	652,4	446,8	68,49
	Морковь	588,1	310,2	52,75
	Лук репчатый	1658,9	1394,4	84,06
ОАО «Фирма «Кадино»	Капуста	1981,0	916,2	46,25
	Свекла	736,7	463,4	62,90
	Морковь	609,4	319,6	52,45
	Лук репчатый	685,2	466,8	68,13
	Прочие	20,8	5,4	25,96
ОАО «Горецкое»	Капуста	150,8	34,6	22,94
	Свекла	256,7	116,4	45,34
	Морковь	349,6	41,0	11,73

Проблемы, связанные с возможностью реализовать произведенную сельскохозяйственными организациями овощную продукцию, как правило, обусловлены невысоким уровнем развития маркетинговой, логистической деятельности в данных организациях, а также отсутствием бренд-менеджмента.

Кроме того, сельскохозяйственные организации отличаются низким уровнем технико-технологической оснащенности складов, недостатком холодильных установок, погрузо-разгрузочных и фасовочных машин.

Существующий в настоящее время на рынке овощей открытого грунта механизм характеризуется разобщенностью межхозяйственных связей по цепочке «производство – хранение – переработка – реализация», в связи с чем, товаропроизводители вынуждены искать покупателей продукции в условиях отсутствия прозрачной информационной базы о состоянии рынка овощной продукции.

Проблема выхода на рынок для сельскохозяйственных организаций также связана с тем, что отдельные производители, как правило, не могут обеспечить такой объем производства, который позволил бы обеспечить долгосрочные взаимодействия с торговыми сетями, в связи с чем процесс реализации протекает неравномерно (более половины продукции реализуется в сезон уборки урожая), а часть продукции реализуется через посредников или перерабатывающим организациям по невысоким ценам.

Как следствие нерешенности существующих проблем с организацией сбыта количество сельскохозяйственных организаций, осуществляющих выращивание овощной продукции снижается, ввиду невысокой доходности данного вида деятельности.

Все вышеуказанное вызывает необходимость наращивать усилия сельскохозяйственных организаций по развитию и совершенствованию сбытовой деятельности, направленной на консолидацию усилий в отношении повышения конкурентоспособности и привлекательности производимой продукции, а также трансформацию системы логистики и создание новых структур,

занимающихся задачами складирования, хранения, транспортировки, информационным сопровождением движения продукции.

В решении проблемы сбыта овощной продукции открытого грунта сельскохозяйственными организациями Могилевской области важное значение принадлежит созданию регионального информационно-консультационного центра по сбыту овощной продукции.

Деятельность центра будет способствовать росту экономической устойчивости деятельности сельскохозяйственных организаций, а также эффективности распределительной сети овощной продукции за счет: рационального использования складских помещений; оптимизации товарных, финансовых и информационных потоков; сокращения издержек обращения; рационального использования имеющихся ресурсов, в том числе на основе концентрации и совместного использования элементов рыночной инфраструктуры.

Создание регионального информационно-консультационного центра по сбыту овощной продукции позволяет решить следующие задачи:

- обеспечить более тесное взаимодействие сферы производства и потребления по цепочке «производство – хранение – переработка – реализация»;
- устойчивое и круглогодичное снабжение населения овощной продукцией;
- предоставить производителям овощной продукции стабильную возможность выхода на рынок;
- ускорить процесс реализации продукции и минимизировать издержки в сфере обращения; повысить конкурентоспособность продукции на основе постоянного контроля качества и безопасности;
- увеличить объем реализации и ассортимент овощной продукции на основе координации спроса и предложения с учетом потребительских предпочтений;
- исключить многочисленных посредников из цепи продвижения продукции; сформировать рынок овощной продукции с активной конкурентной средой.

Положительный экономический эффект от создания регионального информационно-консультационного центра по сбыту овощной продукции будет достигаться за счет того, что на рынке будут конкурировать не отдельные сельскохозяйственные организации–производители, а региональное объединение, которое благодаря научно-производственной, технологической и логистической кооперации обеспечит наращивание объемов производства качественной, конкурентоспособной продукции по доступным ценам за счет сокращения производственных и коммерческих издержек.

Оценка потенциальной емкости основных региональных рынков овощной продукции Могилевской области (без учета доли потребности в овощной продукции, которая удовлетворяется за счет индивидуального сектора) показала, что концентрация спроса на овощную продукцию в Могилевской области находится в Могилевском, Бобруйском и Горецком районах (удельный вес которых составляет примерно 75 % в общей структуре данного рынка). Данное обстоятельство позволяет сделать вывод о целесообразности размещения регионального информационно-консультационного центра по сбыту овощной продукции в городе Могилев.

Предложенное расположение центра позволяет увязать процессы производства, хранения, переработки и реализации продукции в единую цепь поставки овощной продукции на региональный рынок путем взаимодействия с сельскохозяйственными организациями Могилевской области, расположенными в районах концентрации спроса на овощную продукцию (аглогородках Кадино (Могилевского района), Мышковичи (Кировского района), Ректа (Горецкого района)) и обладающими необходимыми производственными и складскими мощностями.

Особенностью предложенной модели является то, что помимо управления и организации грузопотоков, центр будет осуществлять маркетинговое, юридическое и информационно-аналитическое обеспечение, а также оказывать соответствующие комплексные услуги по оформлению (фитосанитарному, таможенному, сертификации) овощной продукции (рисунок 1).



Рисунок 1 – Функции информационно-консультационного центра по сбыту овощной продукции Могилевской области

Предлагаемая структура регионального информационно-сбытового центра по сбыту овощной продукции Могилевской области предполагает в качестве главного органа управления Совет, который будет выступать в роли координатора действий центра, определять стратегические направления его развития, решать вопросы, касающиеся его функционирования, а также осуществлять контроль и оценку функционирования центра. Совет формируется путем включения в его состав представителей от каждой сельскохозяйственной организации-участника.

Единоличным исполнительным органом, подчиненным Совету и осуществляющим руководство текущей деятельностью центра, является директор. Сельскохозяйственные организации, входящие в состав регионального информационно-консультационного центра по сбыту овощной продукции, сохраняют статус самостоятельных юридических лиц.

Для эффективного взаимодействия сельскохозяйственных организаций и регионального информационно-консультационного центра по сбыту овощной продукции важное значение имеет соблюдение принципа справедливого распределения расходов по реализации продукции, а также прибыли от совместной деятельности.

В этих целях усовершенствована методика распределения прибыли между участниками регионального информационно-консультационного центра по сбыту овощной продукции, обеспечивающая возможность максимального учета их вклада. Особенность методики заключается в применении трехуровневой модели:

1-й уровень – производится определение размера прибыли от реализации овощной продукции на каждом этапе продвижения продукции по цепочке «производство – хранение – переработка –

реализация» (1-й этап – производство – информационно-консультационный центр; 2-й этап – информационно-консультационный центр – потребитель);

2-й уровень – распределяются расходы по содержанию регионального информационно-консультационного центра по сбыту овощной продукции и определяется размер членских выплат исходя из размера доли каждого участника в общем объеме реализации;

3-й. уровень – рассчитывается прибыль от реализации овощной продукции через региональный информационно-консультационный центр по сбыту овощной продукции каждого участника.

Обеспечение эквивалентности распределения денежного потока на каждом этапе продвижения продукции требует установления единых для всех участников центра трансфертных цен на овощную продукцию. В качестве трансфертных цен (C_i) следует использовать средние цены производителей сельскохозяйственной продукции.

Предложенный порядок определения величины прибыли на различных этапах продвижения продукции позволяет максимально обеспечить соблюдение интересов сельскохозяйственных организаций–производителей, в производственном процессе которых аккумулируется большая часть затрат на производство готовой продукции. Такое распределение позволяет, в свою очередь, обеспечить максимальную заинтересованность сельскохозяйственных организаций в наращивании объемов производства, ассортимента овощной продукции и улучшения ее качества.

Заключение

Таким образом, предложенный подход к формированию регионального информационно-консультационного центра по сбыту овощной продукции способствует стабилизации конъюнктуры рынка овощей, увеличению доходов сельскохозяйственных организаций по производству овощной продукции открытого грунта и повышению их экономической устойчивости, а также росту экспортного потенциала экономики Могилевской области.

Список литературы

1. Гнатюк С.Н. Комплексная оценка влияния уровня согласованности экономических интересов перерабатывающих организаций АПК на повышение эффективности производства / С.Н. Гнатюк, О.П. Громыко // Вестник БГУТ. – 2022. – №2(33). – С.105–113.
2. Ефименко А. Г. Формирование и развитие эффективного механизма согласованности экономических интересов организаций АПК: моногр. / А.Г. Ефименко, О.П. Громыко.– Могилев: БГУТ, 2023. – 204с.
3. Журова, И. В. Совершенствование сбыта овощной продукции на основе логистического подхода / И. В. Журова // Проблемы экономики : сб. науч. тр. / Белорус.гос. с.-х. акад. – Горки, 2021. – № 2. – С. 61–69.
4. Киреенко, Н. В. Механизм совершенствования логистической системы в АПК Беларуси в условиях региональной торгово-экономической интеграции / Н. В. Киреенко, А. Л. Косова // Весці НАН Беларусі. Серыя аграрных навук. – 2019. – Т. 57. – № 2. – С. 162–178.

СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ ОРГАНИЗАЦИЙ КАК ФАКТОР СНИЖЕНИЯ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ НАПРЯЖЕННОСТИ В ОБЩЕСТВЕ

Зиралова Д., студентка 1 курса юридического ф-та
Северо-Кавказского института (филиал)
ВГУЮ (РПА Минюста России)
Научный руководитель: Магомедов М.Ш. к.э.н.,
Северо-Кавказский институт (филиал)
ВГУЮ (РПА Минюста России)

Аннотация: статья посвящена проблемам развития социальной ответственности бизнеса в России и зарубежных странах. В статье раскрыто понятие социальной ответственности организаций в современных условиях, представлены точки зрения известных экономистов и социологов на роль и значение социально ответственного поведения современных компаний; изложены основные этапы развития теории и практики социальной ответственности бизнеса; представлены основные аргументы сторонников и противников социально ответственного поведения бизнеса.

Значительное внимание уделено развитию социальной ответственности российских компаний на современном этапе развития страны: подробно раскрыты характерные черты российской модели социальной ответственности бизнеса; приведены основные причины, препятствующие социально ответственному поведению российского бизнеса, заключающиеся в нестабильной экономической ситуации, политической нестабильности, социальной пассивности населения страны, концентрации капитала в некоторых регионах страны и пр., обоснована необходимость проявления солидарной социальной ответственности власти и бизнеса с целью недопущения роста социальной напряженности в российском обществе.

Ключевые слова: социальная ответственность, рыночная конкуренция, социально-экономическое развитие, имидж компании

Социализация бизнеса стала одной из основных тенденций социально-экономического развития современного мирового сообщества, и в процессе своего становления и развития прошла более чем полувековую историю. Анализ современных тенденций позволяет сделать вывод, что масштабы и степень социально ответственного поведения бизнеса стабильно возрастают.

Несмотря на актуальность феномена социальной ответственности, в научном мире до сих пор не сложилось однозначной трактовки данного явления. В современном понимании социальная ответственность бизнеса воспринимается как прагматичная деятельность бизнеса, которая может выступать одним из инструментов, ведущих к формированию положительного имиджа компании и дальнейшего укрепления ее репутации; совершенствованию качества управления организацией; росту инвестиционной привлекательности компании в глазах потенциальных инвесторов.

Одно из первых определений социальной ответственности бизнеса было дано Г. Боуэном в 1953 г.: «Социальная ответственность бизнесмена состоит в реализации такой политики, принятии таких решений, либо следования такой линии поведения, которые стали бы желательны для целей и ценностей общества».

Огромный вклад в развитие концепции социальной ответственности бизнеса внес профессор Университета Аризоны К. Дэвис [5]. В своих работах он обосновал ряд важнейших положений, которые сыграли определяющую роль в становлении современной концепции социальной ответственности бизнеса и вывели ее на новый уровень понимания и развития.

Дэвис считал, что помимо экономических, компании ответственны за удовлетворение социальных, политических, психологических и других ожиданий общества. Он также считал, что социально ответственное поведение компании может в будущем стать основой для долгосрочного экономического эффекта. Таким образом, Дэвис стал одним из первых, кто не противопоставлял социальную ответственность компаний и экономическую эффективность их развития. Теория получила название теории разумного эгоизма и стала доминирующей концепцией социальной ответственности бизнеса в настоящее время

Существование различных точек зрения о роли предпринимательства в современном обществе привели к появлению многочисленных аргументов «за» и «против» социальной ответственности бизнеса.

Аргументы сторонников социальной ответственности бизнеса заключаются в том, что компаниям выгодно заниматься социальной деятельностью в интересах дела, так как в долгосрочной перспективе эта деятельность принесет компании прибыль; социальная политика компаний желательна с точки зрения этики, так как компания имеет определенные нравственные обязательства перед обществом; социально ответственные компании относятся к законам с большим уважением; формируется положительный имидж компаний, участвующих в социальных программах.

Противники социальной ответственности бизнеса считают, что решение социальных проблем общества является прерогативой государства, а компании, уплачивая налоги, уже выполняют свои социальные обязательства перед обществом. Также противники социально ответственного поведения компаний исходят из положения, что эффект участия компаний в социальных программах невозможно измерить и сложно оценить ценность социально направленного мероприятия для общества. И важнейшим аргументом является то, что нарушается принцип максимизации прибыли акционеров, так как на социальные проекты отвлекаются трудовые, материальные и финансовые ресурсы.

В современной России интерес к социальной ответственности бизнеса стал проявляться с середины 90-х гг., однако это был интерес на чисто теоретическом уровне, так как первоочередной задачей российских компаний того периода было элементарное выживание.

В советский период развития страны социальную ответственность взяло на себя государство. Будучи государственными по форме собственности, советские предприятия также несли ответственность перед обществом и государством, например, за состояние окружающей среды, качество выпускаемой продукции, развитие социальной сферы. Однако на практике все это носило формальный характер.

Впервые интерес к социальной ответственности бизнеса в постсоветской России стал проявляться с конца 90-х гг., когда в СМИ стали регулярно появляться публикации на данную тему и в обсуждении этого феномена принимали участие широкие круги общественности, ученые, предпринимательское сообщество. Дополнительный импульс развитию социальной ответственности бизнеса придал тот факт, что данные проблемы довольно часто затрагивались в выступлениях Президента страны В.В. Путина.

В современном российском обществе процесс становления национальной модели социальной ответственности бизнеса продолжается. Характерной чертой реализации программ социальной ответственности является участие в них в основном компаний крупного бизнеса. Государственное регулирование и стимулирование социальной ответственности бизнеса в России практически отсутствует, и, поэтому, для эффективного развития российской модели социально ответственного поведения бизнеса необходимо формирование условий для активного взаимодействия государства и бизнес-структур. Социально ответственное поведение предпринимательского сообщества в России заключается, в основном, в социальных инвестициях городов и регионов, в которых российские предприятия ведут свою деятельность.

В публикациях российских специалистов выделяется ряд причин, препятствующих развитию социальной ответственности бизнеса в современной России:

- длительная нестабильная экономическая ситуация;
- политическая нестабильность;
- концентрация капитала в определенных регионах страны;
- социальная пассивность населения и др.

Необходимо отметить, что в современной российской науке понятие социальной ответственности бизнеса трактуется довольно широко, что, вероятно, обусловлено огромным количеством социальных проблем в российском обществе, с которыми государство не справляется и зачастую пытается переложить на предпринимательское сообщество, однако ожидать от бизнеса социально ответственного поведения во всех сферах общественной жизни было бы неразумно.

Обеспечение обороноспособности страны, внешняя политика, борьба с преступностью, защита

прав и свобод человека, определение приоритетов социально-экономического развития страны, принятие правовых норм, обеспечивающих благоприятную среду для развития бизнеса, являются теми сферами общественной жизни, за развитие которых основную ответственность несет государство.

Стабильно устойчивое социально-экономическое развитие страны, охрана окружающей среды, реализация планов по модернизации экономики являются совместными задачами ответственности и государства, и бизнеса.

В то же время, рациональное использование всех видов имеющихся ресурсов, повышение качества и конкурентоспособности выпускаемой продукции и оказываемых услуг, обеспечение эффективного управления компаниями, совершенствование качества их человеческих ресурсов являются в большей степени теми областями, в которых ответственность несет бизнес.

Соответственно, основным условием эффективного, гармоничного развития современного российского общества является социально ответственное поведение перед обществом как государства, так и российского бизнеса.

В современной России уровень социальной ответственности государства должен быть более высоким, так как государство играет доминирующую роль в экономике страны и контролирует большую часть российского бизнеса в лице крупнейших финансовых институтов страны и крупных государственных корпораций.

Предполагается, что социально ответственное поведение должно осуществляться на трех уровнях:

- на федеральном – власть и бизнес несут социальную ответственность за устойчивое развитие страны;

- на региональном – власть и бизнес ответственны за социально-экономическое развитие региона, развитие региональной инфраструктуры, уровень жизни населения региона, повышение уровня квалификации человеческих ресурсов, создание рабочих мест;

- корпоративном – основную ответственность российского бизнеса, заключающуюся в обеспечении устойчивого развития предприятия, уровня квалификации работников, качества выпускаемой продукции и оказываемых услуг.

В большинстве трактовок социальной ответственности бизнеса акцент делается на добровольности социально ответственного поведения. Очевидно, что в развитых странах с высоким уровнем развития демократических основ и правосознательности представителей бизнеса, где соблюдение законов, своевременная уплата налогов, соблюдение прав работников, выпуск качественной продукции является само собой разумеющимся, упор делается на добровольности социально ответственного поведения.

Российское общество столкнулось с рядом существенных проблем в социально-экономическом, политическом, социальном развитии, которые могут привести к серьезному росту социальной напряженности в обществе. Сохранение социальной стабильности, недопущение социальных конфликтов, предпосылки которых уже начинают проглядываться, является важнейшей задачей российских властей и предпринимательского сообщества.

Отличие социальной ответственности российского бизнеса заключается также в том, что российский бизнес ответственен в первую очередь перед властью, так как степень зависимости бизнеса от власти в таких вопросах, как получение государственных заказов, льготное кредитование, содействие в выходе на внешние рынки и прочих вопросах в России несоизмеримо высока по сравнению с западными странами.

Основное отличие моделей социальной ответственности организаций определяется степенью их государственного регулирования. В настоящее время сложились две точки зрения в отношении социально ответственной ответственности бизнеса. В соответствии с первой предприниматели сами определяют степень социально ответственного поведения своих компаний. С позиций второй точки зрения общество и государство вырабатывают обязательные к исполнению или декларативные требования социально ответственного поведения бизнеса. Соответственно, в зависимости от сложившихся страновых моделей формы социальной ответственности бизнеса можно разделить на «открытые» или «скрытые».

Практически во всех странах вне зависимости от формы социальной ответственности бизнеса функционируют правовые нормы, направленные на стимулирование социально ответственного поведения компаний.

Наивысшего уровня развития концепция социальной ответственности организаций получила в США. Отличительными особенностями американской модели социальной ответственности бизнеса является ее высокая степень открытости, основывающаяся на принципе максимальной свободы деятельности предприятий и минимального вмешательства государства в предпринимательскую деятельность.

Государственное регулирование социальной ответственности является одной из важнейших особенностей социальной ответственности компаний из европейских стран. Так, правоотношения работников и работодателей в Европе более регламентированы, чем в США, свидетельством чему является законодательное закрепление во многих европейских странах обязательного социального страхования работников, вопросов пенсионного обеспечения, охраны здоровья работников. Таким образом, концепция социальной ответственности европейских компаний носит скрытый характер, обусловленный выработкой государством стандартов и норм социально ответственного поведения компаний.

На азиатском континенте распространение концепции социальной ответственности получили развитие не так уж давно, и наибольшее развитие получило в Японии. Сложно выделить какую-либо азиатскую модель социальной ответственности бизнеса, что обусловлено различными уровнем социально-экономического развития стран региона, а также их культурным многообразием.

Японская модель социально ответственного поведения бизнеса можно рассматривать как получившую наибольшее развитие в азиатском регионе. Она основывается на тесных партнерских взаимоотношениях между работниками и руководителями японских компаний, составляющими частями которых являются система пожизненного найма, благоприятный социально-психологический климат в коллективе, серьезное внимание уровню квалификации работников и возможность ее постоянного совершенствования, высокая заинтересованность работников в качестве производимой продукции. Также существенное внимание японские компании уделяют экологической составляющей социально ответственного поведения бизнеса, а также взаимодействию с местными сообществами. Необходимо отметить также, что следование принципам социальной ответственности носят в Японии исключительно добровольный характер.

Отдельного внимания заслуживает исламская модель социально ответственного поведения компаний. В исламском мире взаимоотношения основываются на Коране и носят характер партнерских, то есть совместного участия в прибылях и убытках. Исламская модель социально ответственного поведения основывается на моральных и религиозных принципах, в основе которых лежит постулат праведности поведения, признания социальной и моральной ответственности за сотрудников, работающих в компаниях, а также общества в целом. В целом, уровень социальной ответственности компаний из исламских стран можно рассматривать как достаточно высокий.

Подводя итог, можно сказать, что разнообразие моделей социально ответственного поведения компаний различных стран определяется уровнем государственного регулирования самого феномена социально-экономического развития компаний.

Список использованных источников

1. Виттенберг Е.Я. Социальная ответственность бизнеса на постсоветском пространстве. М.: РГГУ. 2011. – С. 477.
2. Градович М.С. Развитие корпоративной социальной ответственности как ключевого инструмента и конкурентного преимущества в стратегии организации // Вестник Томского государственного университета. Экономика. 2014. №3 (27). – С. 33-44.
3. Завьялова Е.Б. Вестник РУДН. Серия: Экономика. 2017. Т. 25 (2). – С. 209-218.
4. Кузнецова Н.В., Маслова Е.В. Модели корпоративной социальной ответственности // Вестник Томского государственного университета. Экономика. 2013. №3 (24). – С. 22-37.

5. Окорочкова А.А. Корпоративная социальная ответственность в эпоху «сознательного капитализма» // Российское предпринимательство. 2017. Т. 18 (7). – С. 1253-1272.
6. Перекрестов Д.Г., Поварич И.П., Шабашев В.А. Корпоративная социальная ответственность: вопросы теории и практики. – М.: Академия Естествознания, 2011.
7. Цуциева О.Т., Гобозова А.З. Сравнительный анализ моделей корпоративной социальной ответственности // Международный научно-исследовательский журнал. Экономические науки. – 2013, июнь.
8. Шлихтер А.А. Направления и механизмы взаимодействия социально-ответственного бизнеса с некоммерческим сектором США. – М.: ИМЭМО РАН, 2010. – 104 с.
9. Bowen H.R. Social responsibilities of the Businessman. – New York: Harper and Row, 1953. – 276 p.

ЗАЩИТА ПРАВ ЧЕЛОВЕКА В ЭПОХУ ГЛОБАЛИЗАЦИИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
PROTECTION OF HUMAN RIGHTS IN THE ERA OF GLOBALIZATION AND INFORMATION TECHNOLOGY

**В.А. Киселева, Ростовский институт (филиал) ВГУЮ (РПА Минюста России),
344000, г. Ростов-на-Дону, ул. 9-я линия/Советская, д. 2/32, e-mail: vika.kiselyova.04@bk.ru**
**V.A. Kiseleva, Rostov Institute (branch) VSU (RPA of the Ministry of Justice of Russia),
9th line street/Sovetskaya, 2/32, Rostov-on-Don, 344000, e-mail: vika.kiselyova.04@bk.ru**

Аннотация: В современных реалиях, где цифровизация занимает одно из центральных мест в развитии общества и государства, особенно важным ставится вопрос о необходимости уделять внимание соблюдению, обеспечению и защите прав человека. Цифровизация в области политики, либо в сфере социально-экономических процессов в государстве приводит к тому, что появляются такие феномены, как - цифровая личность, цифровая реальность, информационно-правовое пространство правоотношений, на которые механизмы защиты прав человека не распространяются в полной мере. Глобализация приводит к тому, что человек сталкивается с новыми вызовами и угрозами для своих прав, такими как нарушение приватности, цензура, дискриминация и другие формы нарушения прав.

Целью данной научной работы является исследование влияния глобализации на человека, в частности вопрос реализации прав человека в современных условиях цифровизации общества, а также разработка рекомендаций на основе полученной информации.

Ключевые слова: глобализация, информационные технологии, информация, защита прав, цифровизация.

Abstract: In modern realities, where digitalization occupies one of the central places in the development of society and the state, the question of the need to pay attention to the observance, provision and protection of human rights is particularly important. Digitalization in the field of politics or in the field of socio-economic processes in the state leads to the emergence of such phenomena as digital personality, digital reality, information and legal space of legal relations, to which the mechanisms of human rights protection do not fully apply. Globalization leads to the fact that people face new challenges and threats to their rights, such as violation of privacy, censorship, discrimination and other forms of violation of rights.

The purpose of this scientific work is to study the impact of globalization on humans, in particular the issue of the realization of human rights in modern conditions of digitalization of society, as well as to develop recommendations based on the information received.

Keywords: globalization, information technology, information, protection of rights, digitalization.

Введение

Появление и развитие информационных технологий способствует ослаблению уровня неприкосновенности частной жизни людей. В то время как технологический прогресс привнес множество полезных инноваций и усовершенствований в нашу повседневную жизнь, он также неизбежно имеет свои негативные последствия. В современном мире тема защиты прав персональных данных получает все большую огласку и становится неотъемлемой частью нашей повседневности. Все больше людей осознают важность защиты своей личной информации от нежелательного доступа и злоупотреблений. Каждый день мы оставляем огромное количество цифровых следов, которые могут быть использованы в корыстных целях. Множество людей беззаботно проводят время в интернете, не задумываясь о возможных последствиях своей активности. Они не осознают, насколько важно обеспечить свою безопасность в сети, не принимая во внимание меры предосторожности, такие как: проверять безопасность посещаемого сайта,

использовать надёжные пароли, не переходить по подозрительным ссылкам. Часто бесконтрольная публикация личной или некорректной, неточной информации в значительной степени увеличивает вероятность столкновения с неожиданными трудностями.

Сейчас меры наказания за нарушения в интернете становятся серьёзнее, как и за нарушения в реальной жизни, так как воздействие на людей в виртуальности производить легче и быстрее и внушить что-либо человеку не составляет особого труда, ведь в интернете ее можно предоставить в любом виде. Прогресс не стоит на месте, появляется необходимость учиться соблюдать меры предосторожности в интернете. Не каждому человеку известно, как необходимо это делать, но каждому пользователю необходимо ознакомиться с соответствующими правилами.

Несомненно, интернет-пространство предоставляет человеку огромные возможности для реализации идей и желаний, выражения мнения и свободного обмена информацией, что закреплено в 29 статье Конституции Российской Федерации [1], которая выражает лицам право на свободу мнения. Однако, несмотря на все преимущества, в интернете существует множество отрицательных аспектов, так как не все пользователи соблюдают закон в должной мере. Они считают, что могут свободно выражать свое мнение, не ограничиваясь нормами и правилами, предусмотренными законом, что может привести к возникновению конфликтов или даже информационной травли.

Для пресечения безнаказанного поведения лиц в интернете, законодательством РФ предусмотрены нормативные акты, такие как статья 5.61 Кодекса Российской Федерации "Об административных правонарушениях" [2]. Согласно данной статье, нарушение гражданскими лицами может повлечь штраф в размере от 1 000 до 3 000 рублей, на должностных лиц — от 10 до 30 тысяч рублей, а на юридических лиц — от 50 тысяч до 100 тысяч рублей. Кроме того, имеются статья 128.1 Уголовного кодекса Российской Федерации [3] и статья 152 Гражданского кодекса Российской Федерации [4], которые также регулируют данную сферу.

Основными задачами научной статьи являются: изучение влияния роста технологий на жизни людей, а также проблемы, возникающие в связи с воздействием интернета на человека. Немало важным является выяснение перспектив их решения, которые присутствуют на ближайшее время и рекомендации о том, каким образом человек самостоятельно может себя обезопасить, либо как он может решить свою существующую проблему.

Теоретические основы исследования

Глобализация — это процесс, который вызывает противоречивые мнения у большинства исследователей. Несомненно, одной из положительных сторон глобализации является доступность для пользователей информационных ресурсов. Однако, несмотря на это, существует одна из самых обсуждаемых тем - вопрос о защите прав человека в сфере интернет-ресурсов. В работах Э.В. Талапиной «Право и цифровизация: новые вызовы и перспективы» [5], «Права человека в Интернете» [6], есть подробный анализ прав человека в условиях цифровизации и её влияния на сферу правоотношений, подробно рассматриваются последствия, вызовы и риски внедрения информационных технологий в государстве и обществе. В исследовании зарубежных учёных Андерсона, Баскервиля, Ричарда и Кауля «Теория управления информационной безопасностью: Достижение устойчивого согласования между совместным использованием и защитой конфиденциальности информации» [7], рассматриваются современные организации, работающие в сильно взаимосвязанных средах, где они часто сталкиваются с проблемой обеспечения баланса между защитой информационных ресурсов и необходимостью обмена информацией. Присутствует противоречие между выгодой данного взаимодействия и потенциальными рисками нарушения безопасности, присущими процессу обмена информацией. Теория контроля информационной безопасности объясняет это противоречие и предлагает варианты для предотвращения рисков. Данная теория предлагает основу для понимания процесса разработки политики информационной безопасности и способ устранения противоречий между обменом и защитой информации. Исследователи данной теории в основном сосредоточились на том, как же извлечь максимальную выгоду при использовании цифровых технологий. Рассмотрение темы цифровой глобализации учёными, ясно даёт понять, что её развитие имеет огромный потенциал для дальнейшего роста и процветания.

Права человека в условиях развития цифровых технологий

С начала прошлого столетия и до настоящего времени в научной литературе разрабатываются новые категории и концепции цифровых прав человека, а в политике государств и международных организаций - новые национальные, региональные и международные программы, связанные с расширением доступа к Интернету, защитой цифровой личности, цифровой безопасностью, цифровым неравенством и т.п.

Председатель Конституционного Суда РФ В. Д. Зорькин стал одним из первых, кто заявил о цифровых правах как новой категории, а также о формировании механизмов их защиты в государстве и обществе на современном этапе. В мае 2018 г., выступая на Петербургском международном юридическом форуме, он отметил тенденции и положения, ставшие предметом дискуссий и обсуждений:

1) сейчас формируется новое право - «право второго модерна», регулирующие политические, экономические и социальные отношения «в контексте мира цифр, Больших данных, роботов, искусственного интеллекта»;

2) «мы живём во времена цифровой революции». Мир вступает в эпоху «активного использования искусственного интеллекта (ИИ) и Больших данных (Big Data) для управления в экономике, обществе и государстве»;

3) большой интерес представляют дискуссии юристов по поводу использования роботов в своей профессии, как помощников юристов, способных эффективно выполнять ряд «типовых юридически значимых процедур», в частности подготовки различных документов. И «первые попытки функционирования роботов-юристов уже есть в России»;

4) «цифровые права человека – это, по сути, конкретизация (посредством закона и правоприменительных, в том числе судебных, актов) универсальных прав человека, гарантированных международным правом и конституциями государств, – применительно к потребностям человека и гражданина в обществе, основанном на информации». И задача государства – «признавать и защищать цифровые права граждан от всевозможных нарушений, обеспечивая при этом конституционно-правовую безопасность личности, общества и государства» [8].

Существует множество подходов к вопросу о развитии прав человека в условиях новых информационных технологий. Среди таких подходов российских учёных можно выделить такие, как, например,:

1) Ю. А. Чернышова считает, что «эпоха информационных технологий диктует необходимость ревизии универсальных прав человека и их расширения», и относит к цифровым правам такие, как «право на публикацию цифровых произведений, право на использование компьютеров и других электронных устройств». Она также отмечает развитие – в качестве новых подотраслей цифрового права – права цифровых денег и цифровых споров, авторского и программного права, др. [9];

2) Э. В. Талапина, анализируя развитие прав человека в цифровую эпоху, отмечает, что «система прав человека будет меняться в зависимости от условий их реализации». Она полагает, что «с приходом цифровых технологий возникают цифровые права», и относит к ним такие права, как: «право на доступ к Интернету, право на забвение, право на защиту от нежелательной информации, уже получившие законодательное признание в разных странах» [10].

3) Е. В. Алферова полагает, что можно говорить о правах традиционных и новых, и относит к новым правам следующие: права «на информационное самоопределение, информационную безопасность, защиту персональных данных, конфиденциальность, свободу самовыражения в Сети и др.». Основным дискуссионным вопросом, обсуждаемым в настоящее время, она считает - глобальную и трудно решаемую проблему достижения баланса интересов и прав человека в интернете, в киберпространстве [11];

4) Н. В. Кравчук полагает, что можно говорить о процессе перемещения прав человека в цифровую сферу, которая «подвергает права человека беспрецедентным рискам». Он считает, что «право на свободу выражения мнений в наши дни ограничивается фильтрацией контента или блокированием доступа к нему», и подытоживает, что адаптация национальных и международных правил, «применимых к науке и технологиям, происходит медленно, а действующее право не способно адекватно регулировать ситуации, порождённые технологическими инновациями»;

Цифровые права в российской теории и практике

Цифровые инновации активно проникают в сферы российской политики, экономики и права, меняя традиционные процессы и стимулируя развитие страны. В 2018 г. в Российской Федерации стартовала программа «Цифровой экономики» [12], в 2019-м вступил в силу закон о «цифровых правах» [13], в 2020-м Минкомсвязи России было переименовано в Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации; формируется новая отрасль – цифровое право; мощными темпами развивается цифровизация политики и политика цифровизации.

Сегодня тема цифровых прав является крайне новой и неопределённой. Так, в Федеральном законе «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» от 18.03.2019 г. № 34-ФЗ российский законодатель цифровые права определил как некие имущественные и обязательственные права, содержание которых конкретно не прописано [14]. Не смотря на это, данный подход не является исчерпывающим, так как данное определение рассматривается только в сфере «имущественных прав», но не основных прав и свобод человека и гражданина.

В качестве основных цифровых прав можно отнести:

1) право на доступ к Интернету: осуществление данного права подразумевает не только отсутствие ограничений на доступ к Интернету у любого человека, но и возможность его качественного использования;

2) право на создание, использование и публикацию цифровых произведений, при реализации которого необходима защита не только правообладателей произведения, но и его пользователей (потребителей);

3) право на поиск, получение и передачу информации, что уже несомненно закреплено в Конституции РФ (ст. 29, ч. 4). Одной из важных проблем, связанных с этим и другими правами, является баланс прав в киберпространстве;

4) право на приватность в Интернете, что закреплено законодателем в Федеральном законе «О персональных данных» от 27.07.2006 г. № 152-ФЗ. Предусматривает обязанность лиц, имеющих доступ к персональным данным людей, сохранения этих данных от третьих лиц для минимизации количества преступлений;

5) право на анонимность. На сегодняшний момент в отечественном правовом пространстве на законодательном уровне данное право не закреплено. Примером этого служит «Закон Яровой», который обязывает операторов сотовой связи сохранять весь интернет-трафик пользователей в течение 30 суток. Формально закон рассматривается как антитеррористический, но цели его довольно многозначны, так как интернет-трафик содержит в себе также и персональные данные, использование которых третьими лицами может привести к негативным последствиям как для пользователей, так и для всего общества в целом. В этом случае также необходимо отметить Федеральный закон «О внесении изменений в статьи 10.1 и 15.4 Федерального закона “Об информации, информационных технологиях и о защите информации”» от 29.07.2017 г. № 241-ФЗ [13], который «запрещает» анонимность пользователей мессенджеров, тем самым ограничивая права человека;

Заключение

Информационные технологии проникли практически в каждую сферу жизни человека. Несмотря на достоинства, технологии с лёгкостью могут способствовать развитию конфликтов в обществе, зарождению противоречий, появлению угроз, затрагивающих безопасность человека. И для сохранения своей конфиденциальности и обеспечения безопасного пользования интернетом, необходимо соблюдать некоторые условия:

1. Убедиться в надёжности сайта. При переходе на неизвестный сайт необходимо проверить защищён ли он SSL-сертификатом. Адреса таких сайтов начинаются с HPS вместо HP (буква S означает «безопасный»), а в адресной строке отображается значок замка;

2. Подобрать надёжные и индивидуальные для каждой социальной сети пароли;

3. Не переходить по неизвестным ссылкам;

4. Не разглашать персональные данные;

5. Не скачивать непроверенные приложения;
6. Использовать надёжный антивирус.

Соблюдение вышеперечисленных условий позволит пользователям быть уверенными в сохранении своей конфиденциальности. Они смогут спокойно использовать различные сервисы и приложения, зная, что их персональные данные и личная информация будут храниться и использоваться с соблюдением строгих норм безопасности.

Немало важным является рассмотрение различных подходов среди учёных и практиков к развитию правового регулирования Интернета, а также соблюдению, обеспечению и защите прав человека в сети Интернет. Несомненно можно согласиться с авторами коллективной монографии «Права человека в сети Интернет» С. Э. Несмеяновой, Н. Е. Колобаевой, М. С. Саликовым, А. Н. Мочаловым, К. А. Ивановой, которые выдвигают следующие актуальные и важные положения:

1) в сфере соблюдения, обеспечения и защиты прав граждан важной ролью Интернета является информирование о деятельности органов публичной власти, предоставляемых услугах (как государственных, так и муниципальных);

2) «новое законодательство в сфере управления Интернетом должно учитывать нормы международного права, лучшие практики зарубежных стран и российские национальные достижения в данной сфере, закреплять право каждого на равный и беспрепятственный доступ к Интернету, устанавливать четкий и исчерпывающий перечень обстоятельств, при которых доступ может быть ограничен»;

3) ресурсы Интернета позволяют реализовать социальные, отчасти политические (имеются в виду избирательные технологии), культурные, экономические и другие права;

4) «нужно создать механизмы, обеспечивающие защиту персональных данных (неприкосновенность личной жизни, конфиденциальность передаваемых данных, их хранение), предотвращающие правонарушения в Интернете, гарантирующие информационную безопасность, прежде всего граждан» [15].

Стоит отметить, что глобализация привносит новые вызовы в области экономики, культуры, политики и социальных отношений. Она меняет взаимодействия между странами, людьми, создавая новые как возможности, так и угрозы. Важно помнить, что глобализация несёт как положительные, так и негативные стороны, и важно уметь балансировать между ними.

Одним из ключевых аспектов глобализации является обмен информацией и идеями. Интернет и социальные сети значительно упрощают коммуникацию и доступ к информации, что с одной стороны способствует образованию и развитию, но с другой – создаёт уязвимость для различного рода манипуляций и угроз. Модернизация механизмов и технологий реализации и защиты прав человека в виртуальной, цифровой сфере требует поиска наиболее адекватных правовых решений, признания и закрепления их законодателем на государственном уровне.

В целом, глобализация – это неизбежный процесс, который требует внимательного изучения и управления. Пользователям необходима гарантия, что их права защищены государством, но также важно и самостоятельно следить за законностью своих действий. Такой подход позволит избежать выработки излишних механизмов правового регулирования и конфликтов в правовой и политической системах.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). // Конституционное собрание РФ. 2020;
2. Кодекс Российской Федерации об административных правонарушениях (ред. от 25.12.2023) (с изм. и доп., вступ. в силу с 05.01.2024) // Государственная Дума. 2023. № 420-ФЗ;
3. Уголовный кодекс Российской Федерации (ред. от 25.12.2023) (с изм. и доп., вступ. в силу с 30.12.2023) // Государственная Дума. 2023. № 141-ФЗ;
4. Гражданский кодекс Российской Федерации (часть четвертая) (ред. от 13.06.2023, с изм. от 14.12.2023) (с изм. и доп., вступ. в силу с 29.06.2023) // Государственная Дума. 2023. № 152-ФЗ;

5. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 5–17;
6. Талапина Э.В. Права человека в Интернете // Журнал российского права. 2019. № 2. С.41-54;
7. Андерсон С., Баскервиль Р.Л., Ричард Л., Каул М. Теория управления информационной безопасностью: достижение устойчивого согласования между совместным использованием и защитой конфиденциальности информации // Журнал управленческих информационных систем. 2017. № 34 (4) С. 1082–1112.
8. Зорькин В. Д. Право в цифровом мире. Размышления на полях Петербургского международного юридического форума // Российская газета. Столичный выпуск. – 2018. – 29 мая (№ 115 (7578)).
9. Чернышова Ю. А. Права человека в условиях цифровизации общества // Психология и право. – 2019. – Т. 9, № 4. – С. 90–102.
10. Талапина Э. В. Эволюция прав человека в цифровую эпоху // Труды Института государства и права РАН. – 2019. – Т. 14, № 3. – С. 108–133.
11. Алферова Е. В. Защита прав человека в Интернете // Государство и право в новой информационной реальности. – М. : ИНИОН РАН, 2018. – С. 143–157.
12. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года : Указ Президента РФ от 07.09.2018 г. № 204 // КонсультантПлюс : справ.-правовая система. – URL: http://www.consultant.ru/document/cons_doc_LAW_297432/ (дата обращения: 02.03.2024).
13. О внесении изменений в статьи 10.1 и 15.4 Федерального закона «Об информации, информационных технологиях и о защите информации» : Федеральный закон от 29.07.2017 г. № 241-ФЗ // КонсультантПлюс : справ.-правовая система. – URL: http://www.consultant.ru/document/cons_doc_LAW_221183/ (дата обращения: 02.03.2024).
14. О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации : Федеральный закон от 18.03.2019 г. № 34-ФЗ // КонсультантПлюс : справ.-правовая система. – URL: http://www.consultant.ru/document/cons_doc_LAW_320398/ (дата обращения: 04.03.2024).
15. Саликов М. С., Несмеянова С. Э., Мочалов А. Н., Колобаева Н. Е., Иванова К. А. Права человека в сети Интернет : колл. монография. – Екатеринбург : Изд-во УМЦ УПИ, 2019. – 148 с.

**ВЛИЯНИЕ ЭЛЕМЕНТОВ СИСТЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА
ДЕЯТЕЛЬНОСТЬ ОРГАНИЗАЦИИ**
**INFLUENCE OF ELEMENTS OF THE ECONOMIC SECURITY SYSTEM ON THE ACTIVITIES
OF THE ORGANIZATION**

Е.А. Козлова, Д.А. Старовойтова

Белорусский государственный университет пищевых и химических технологий, Республика
Беларусь, 212027, г. Могилев, пр. Шмидта, 3, email: kozlova@bgut.by

E.A. Kozlova, D.A. Starovoitova

Belarusian State University of Food and Chemical Technologies, Republic of Belarus, 212027, Mogilev,
Shmidt, 3, email: kozlova@bgut.by

Аннотация: В работе рассмотрено понятие экономической безопасности организации, проанализированы элементы системы экономической безопасности, определено их влияние на деятельность организации, предложены подходы к внедрению элементов системы экономической безопасности. Исследование проблем обеспечения экономической безопасности сохраняет свою актуальность. Это связано с ростом нестабильности и расширением угроз функционирования организаций. Усиление конкуренции повышает уровень неопределенности в принятии управленческих решений. Каждый элемент системы экономической безопасности оказывает влияние на деятельность организации, обеспечивая повышение эффективности ее функционирования.

Ключевые слова: экономическая безопасность организации, система экономической безопасности организации, элементы системы экономической безопасности организации, риски и угрозы безопасности, методы и средства обеспечения экономической безопасности.

Abstract: The work examines the concept of economic security of an organization, analyzes the elements of the economic security system, determines their impact on the organization's activities, and proposes approaches to the implementation of elements of the economic security system. The study of problems of ensuring economic security remains relevant. This is due to the growth of instability and the expansion of threats to the functioning of organizations. Increased competition increases the level of uncertainty in management decision-making. Each element of the economic security system influences the activities of the organization, ensuring an increase in the efficiency of its functioning.

Keywords: economic security of the organization, economic security system of the organization, elements of the economic security system of the organization, risks and threats to security, methods and means of ensuring economic security.

Введение

Отличительной особенностью современной мировой экономики является состояние нестабильности, когда организации вынуждены искать пути минимизации угроз своей деятельности и постоянно адаптироваться к новым социально-экономическим условиям. Такая ситуация приводит к необходимости поиска устойчивых состояний защищенности, нивелирования негативного влияния внешних и внутренних угроз. Экономическая безопасность организации – это состояние, которое обеспечивает наиболее эффективное использование ресурсов организации для его стабильного функционирования и развития. Под системой экономической безопасности организации необходимо понимать совокупность средств, методов и мероприятий, обеспечивающих защиту интересов организации от внутренних и внешних угроз. Система экономической безопасности включает мониторинг и прогнозирование угроз экономической безопасности организации; оценку рисков и угроз и выработку механизма их минимизации.

В этой связи, данная тема исследования является актуальной и практически значимой.

Цель исследования

Целью исследования является изучение элементов системы экономической безопасности организации, определение их влияния на деятельность организации и выработка подходов к внедрению элементов системы экономической безопасности в деятельность организации.

Материал и методы исследования

Материалами для исследования выступили научные работы отечественных и зарубежных экономистов.

В процессе написания работы автором использованы методы теоретического исследования: системный, обобщения, сравнения и другие.

Результаты исследования и их обсуждение

С проблемой экономической безопасности сталкиваются все организации на современном этапе развития экономики. Экономическая безопасность организации – многофакторное понятие, включающее как внутренние, так и внешние факторы.

К внешним факторам можно отнести:

- экономическую нестабильность,
- изменение предпочтений потребителей,
- условий привлечения кредитных ресурсов и др.

К внутренним факторам можно отнести:

- рост себестоимости продукции,
- разбалансировку системы внутреннего управления и др.

Эффективность деятельности любой организации зависит от скорости реагирования на внешние и внутренние угрозы. Именно поэтому возникает необходимость создания системы экономической безопасности организации.

Система экономической безопасности – понятие комплексное, включающее:

- защиту интересов организации и его сотрудников;
- увеличение конкурентоспособности технологической базы организации;
- обеспечение сохранности материальных ценностей;
- выбор наиболее оптимальных управленческих решений по вопросам экономической деятельности организации;
- контроль за эффективностью функционирования системы безопасности;
- контроль за выполнением экологических стандартов и др.

Функционирование системы экономической безопасности организации реализуется через следующие объекты:

- высшее руководство организации;
- персонал, владеющий информацией, которая является коммерческой тайной;
- финансовые ресурсы организации;
- материальные активы организации;
- информационные ресурсы организации, доступ к которым ограничен;
- средства и системы информатизации деятельности организации;
- технические средства и системы охраны и защиты материальных и информационных ресурсов.

Такой комплексный подход к созданию системы экономической безопасности обосновывается необходимостью защиты своих интересов от конкурентов. Причем необходимо учитывать, что методы конкурентной борьбы могут находиться в правовом поле, а могут и выходить за его пределы. Кроме того, необходимо осуществлять тщательную проверку деловых партнеров. И здесь возникает не только проблема неплатежей, но и проблема недобросовестного выполнения договоров, что может привести к значительным финансовым рискам.

Проблема обеспечения экономической безопасности тесно взаимосвязана с проблемой информационной безопасности, что требует проверки сотрудников, ранее уволенных за различные проступки, в целях предотвращения утечки информации.

Отдельного внимания заслуживает проблема предотвращения производственного травматизма как фактора обеспечения экономической безопасности.

Таким образом, существует достаточно широкий круг вопросов, который лежит в рамках системы экономической безопасности. Ее внедрение в организации позволит обеспечить эффективное функционирование всех структурных подразделений и направлений.

Организационная структура системы экономической безопасности зависит от различных факторов, в том числе и от размеров и возможностей организации. В общем виде система экономической безопасности может в себя включать следующие элементы:

1 предварительный анализ:

- изучение договоров,
- оценка подходов к работе с поставщиками,
- мониторинг компьютерных систем организации.

2 работа с угрозами безопасности:

- мониторинг угроз безопасности,
- анализ угроз безопасности,
- оценка угроз безопасности,
- устранение угроз безопасности.

Эффективное использование перечисленных элементов возможно при соблюдении определенных принципов: законность, своевременность, непрерывность, всесторонность и др.

Система экономической безопасности должна строиться на действующем законодательстве и быть направлена на предотвращение угроз. Методы и средства обеспечения экономической безопасности должны постоянно совершенствоваться, что обеспечит эффективность их применения.

При внедрении системы экономической безопасности необходимо обеспечить финансовую, кадровую, технико-технологическую, правовую, информационную и другие виды безопасности, как элементы системы экономической безопасности организации.

В современных условиях нестабильной экономики, высокого уровня конкуренции, финансовая безопасность является фундаментом развития организации, позволяет ей стабильно функционировать на рынке. Финансовая безопасность организации – это такое состояние организации, при котором она способна противостоять финансово как внутренним, так и внешним угрозам. Для поддержания стабильного состояния организации необходимо проводить постоянный мониторинг уровня безопасности, осуществлять анализ финансовых показателей, формировать системы контрольных мероприятий для предотвращения угроз. Если налажен постоянный контроль за обеспечением финансовой безопасности, то это обеспечивает конкурентоспособность, стабильность положения на рынке, стабильный приток инвестиционного капитала и возможность расширения бизнеса в будущем. Финансовая безопасность организации может быть достигнута в случае внедрения следующих мероприятий:

- обеспечение финансовой независимости организации;
- обеспечение эффективности функционирования организации;
- обеспечение технологической независимости организации;
- обеспечение эффективности менеджмента;
- обеспечение высокой квалификации сотрудников и повышение их квалификации;
- обеспечение правовой защиты деятельности организации;
- обеспечение информационной защиты и коммерческой тайны.

Финансовая безопасность позволяет обеспечить платежеспособность организации, организовать эффективное использование основного и оборотного капитала, повысить рентабельность и максимизировать получение прибыли. Финансовая безопасность основана на целевом и эффективном использовании экономических ресурсов.

Для обеспечения финансовой безопасности в организациях необходимо оценивать угрозы, которые могут иметь негативные последствия для предприятия, анализировать текущий уровень обеспечения финансовой безопасности и выработать комплекс мероприятий по ее укреплению.

Финансовый элемент системы экономической безопасности организаций имеет определяющее значение для выявления причин финансовой нестабильности организаций, для повышения эффективности деятельности организации, а также увеличения ее прибыли. В связи с нестабильностью рыночной экономики в современном мире финансовая безопасность организаций

требует особого внимания.

Кадровая безопасность занимает важное место в системе экономической безопасности. Кадровая безопасность обеспечивает эффективность работы с трудовыми ресурсами организации, предупреждение умышленных и случайных ошибок, различных противоправных действий сотрудников. Следует обратить особое внимание на недостаточную квалификацию работников, их нежелание или неспособность приносить максимальную пользу организации. Это может быть вызвано низким уровнем управления персоналом, отсутствием средств на оплату труда отдельных категорий работников организации или необоснованными затратами.

Кадровая безопасность должна включать в себя требования к уровню знаний и опыту сотрудников, повышению квалификации. Чтобы избежать ухода кадров к конкурентам необходимо вырабатывать меры мотивирующего характера.

Необходимость обеспечения кадровой безопасности объясняется высокими рисками имущественных и финансовых потерь, которые могут быть вызваны неэффективной работой с персоналом. Кроме того, кадровая безопасность является фактором обеспечения конкурентоспособности организации, так как способствует реализации стратегических целей организации через эффективное использование имеющихся человеческих ресурсов. Основной целью кадровой безопасности можно назвать анализ кадровых рисков и угроз со стороны персонала и поиск путей их минимизации. Реализация заявленной цели возможна через определение реальных потребностей организации в трудовых ресурсах необходимой профессии и квалификации, ликвидацию вакантных мест и непрерывное развитие персонала через повышение квалификации и обучающие семинары, применение различных эффективных мотивационных подходов, в том числе и через повышение оплаты труда. Немаловажным является создание атмосферы лояльности персонала, минимизация текучести кадров и достижение высокого уровня компетентности руководителей.

Обеспечение технико-технологического элемента экономической безопасности достигается высоким уровнем технико-технологических факторов, гибкостью производственных процессов, способностью реагировать на изменения окружающей среды и противостоять дестабилизирующим факторам. Эффективность деятельности предприятия напрямую зависит от того, насколько развито производство, используются ли передовые технологии и современное оборудование. Поэтому технико-технологические факторы играют особую роль в системе экономической безопасности. В качестве основных направлений повышения технико-технологической безопасности могут выступать: автоматизация технологических процессов и производств, внедрение нанотехнологий, современных форм организации производства. Для реализации этих направлений необходимо обеспечить: современную производственно-технологическую базу, наличие ресурсов и инвестиций. Технико-технологический элемент экономической безопасности является важным аспектом в обеспечении выполнения стратегических целей организации. Для этого необходимо проводить анализ рынка технологий по производству продукции аналогичной профилю деятельности предприятия: необходимо изучить особенности технологического процесса производства тех предприятий, которые производят аналогичную продукцию, провести анализ конкретных технологических процессов и выявить внутренние резервы с целью повышения эффективности используемых технологий.

Правовая безопасность организации – это юридическая защита организации и ее экономических интересов, включающая анализ действующего законодательства, создание организационно-правовых механизмов обеспечения экономической безопасности. Обеспечение правовой безопасности организации строится на детальном мониторинге правовой системы и выработке предельно-допустимых юридических границ деятельности организации.

Информационная безопасность является еще одним важным элементом в системе экономической безопасности организации. Она состоит во внедрении информационных технологий и защите информационных ресурсов. Информационная безопасность призвана обеспечить устойчивое функционирование организации, предотвращать угрозы его безопасности, защиту законных интересов клиентов. При обеспечении информационной безопасности необходимо ранжировать доступ к информационным ресурсам в зависимости от круга должностных полномочий. Тот объем информации, который может быть доступен определенному кругу пользователей, должен

предоставляться своевременно, оперативно и беспрепятственно, что позволит создать надежную информационную базу для принятия оперативных управленческих решений.

Важным аспектом при обеспечении информационной безопасности является предотвращение угроз информационной системе. Важно провести детальный анализ всех рисков с помощью различных методик и выстроить систему защиты от угроз в информационном пространстве.

Таким образом, перечисленные выше элементы системы экономической безопасности в своей совокупности обеспечивают стабильную работу организации и ее защиту от внутренних и внешних угроз.

Выводы (заключение)

Экономическая безопасность организации характеризуется состоянием наиболее эффективного использования ресурсов для обеспечения стабильного функционирования организации.

Система экономической безопасности каждой организации индивидуальна и зависит как от размеров самой организации, так и от ее организационной структуры. Внедрение системы экономической безопасности напрямую зависит от действующего законодательства, от объемов финансовых ресурсов, которые могут быть израсходованы на эти цели и от понимания всеми сотрудниками необходимости этих действий. Эффективность системы экономической безопасности организации определяется наличием или отсутствием материального ущерба.

Система экономической безопасности, в общем виде, представляет собой совокупность элементов, обеспечивающих защиту организации от внутренних и внешних угроз. Система экономической безопасности обеспечивает защиту коммерческой тайны и конфиденциальность информации, компьютерную и физическую безопасность, безопасность хозяйственной деятельности и информационно-аналитической работы, др. аспекты деятельности организации.

Человеческий фактор является определяющим в функционировании системы экономической безопасности. Поэтому в организации необходима разработка нормативных документов четко регулирующих вопросы обеспечения безопасности бизнеса. Система экономической безопасности организации только тогда будет эффективно функционировать, когда весь персонал организации будет понимать важность обеспечения экономической безопасности организации для повышения эффективности деятельности.

Список литературы

1 Касперович С. А. Экономическая безопасность предприятия: сущность, цели и направления обеспечения / С. А. Касперович, Е. А. Дербинская // Труды БГТУ. – Минск: БГТУ, 2016. – № 7 (189). – С. 278 – 282.

2 Концепция национальной безопасности Республики Беларусь: утв. Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575: в ред. Указа Президента Республики Беларусь от 30 декабря 2011г. № 621 // Нац. правовой интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: <http://www.pravo.by/main.aspx?guid=3871&p2=1/12080>. – Дата доступа: 17.04.2024.

3 Краснощек, А. А. Современные аспекты анализа и оценки экономической безопасности организаций / А. А. Краснощек, И. А. Динец // Корпоративные финансы. – 2010. – № 4 (16). – С. 73–83.

4 Муратова Н.К. Экономическая безопасность предприятия как успешная составляющая современного бизнеса / Н.К. Муратова // Государственное управление. Электронный вестник, 2012. – №32. – [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/ekonomicheskaya-bezopasnost-predpriyatiya-kak-uspeshnaya-sostavlyayuschaya-sovremennogo-biznesa>. – Дата доступа: 13.02.2024.

5 Некрасова Н. А. Сущность понятия «Экономическая безопасность» / Н.А. Некрасова // Экономика и управление: анализ тенденций и перспектив развития, 2013. – №6. – [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/suschnost-ponyatiya-ekonomicheskaya-bezopasnost>

bezopasnost. – Дата доступа: 13.02.2024.

6 Об организации мониторинга важнейших показателей экономической безопасности Республики Беларусь: постановление Совета Министров Республики Беларусь от 22 февраля 2007 г. № 226 (в ред. постановления Совета Министров от 16 декабря 2008 г. № 194-3) // Нац. правовой интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: <http://www.pravo.by/main.aspx?guid=3871&p2=1/12080>. – Дата доступа: 17.04.2024.

7 Пузиков В.В. Методология обеспечения экономической безопасности и ее трансформация в условиях информационного развития / В.В. Пузиков // Бизнес, инновации, экономика, 2021. – Вып. 5. – С. 54–61.

8 Серебрякова Н.А. Формирование системы обеспечения экономической безопасности предприятия / Н.А. Серебрякова, С.А. Волкова, Т.А. Волкова // Вестник ВГУИТ. 2016. №4 (70). – [Электронный ресурс]. – Режим доступа: URL: <https://cyberleninka.ru/article/n/formirovanie-sistemy-obespecheniya-ekonomicheskoy-bezopasnosti-predpriyatiya>. Дата доступа: 17.04.2024).

ВНЕДРЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РОССИЙСКУЮ ЭКОНОМИКУ И ИХ ВЛИЯНИЕ НА НАЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ

А.А. Кукулян, Л.В. Шаронина

Ростовский институт (филиал) ФБГО ВО «Всероссийский государственный университет юстиции (РПА Минюста России) в г. Ростове-на-Дону, 344002, г. Ростов-на-Дону, пер.

Соборный, 26, e-mail: sharoninal@mail.ru

A.A. Kuklyan, L.V. Sharonina

Rostov Institute (branch) of the All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) in Rostov-on-Don, 344002, 26 lane. Cathedral, Rostov-on-Don, 344002, Russia, email: sharoninal@mail.ru

Аннотация: Предметом исследования являются наиболее перспективные технологические решения с использованием искусственного интеллекта. Выделяются основные направления реализации Стратегии по разработке моделей искусственного интеллекта и их применения в современной России. Цель работы изучение внедрения технологий искусственного интеллекта в различные экономические сферы страны, а также их влияние на уровень национальной безопасности.

Ключевые слова: искусственный интеллект, отрасли экономики, цифровая экономика, внутренний рынок, технологии, национальная безопасность

Abstract: The subject of the study is the most promising technological solutions using artificial intelligence. The main directions of the Strategy for the development of artificial intelligence models and their application in modern Russia are highlighted. The purpose of the work is to study the introduction of artificial intelligence technologies into various economic spheres of the country, as well as their impact on the level of national security.

Keywords: artificial intelligence, economic sectors, digital economy, domestic market, artificial intelligence technologies, national security.

В современном экономическом мировом пространстве наблюдается скачок внедрения технологий искусственного интеллекта во все сферы жизнедеятельности общества. Впервые термин «искусственный интеллект» введен в 1956 году американским ученым Джоном Маккарти. За последние несколько лет особенно широко стали использоваться модели генеративного искусственного интеллекта (ИИ), с помощью которых возможно решение задач иного порядка как на уровне бизнеса, так и при государственном управлении. Россия является одна из немногих стран мира, где происходит разработка, развитие и применение технологий ИИ в экономике [1, 2].

Для понимания роли ИИ необходимо понимать его смысловую нагрузку. До сих пор среди ученых нет общепринятого определения ИИ. Искусственный интеллект — это способность компьютера исследовать, обучаться, принимать решения и выполнять различные действия, свойственные и схожие с интеллектом человека.

Искусственный интеллект — это технология, которая имитирует человеческое поведение, чтобы выполнять задачи и постепенно обучаться, используя собираемую информацию. Искусственный интеллект — компьютерная программа, которая принимает и анализирует данные, а затем делает выводы на их основе[3].

Генеративный искусственный интеллект является типом ИИ, который может анализировать данные, находить закономерности, обучаться, затем создавать новый контент: текст, картинки, аудио и прочее. Согласно исследованиям института глобальных исследований компании McKinsey (2023 год) 22% профессионалов используют его модели постоянно на в своей работе. Данные технологии, например, смогут определить тренды потребительского спроса на различные товары (услуги) на рынках; пообщаться с клиентом в реализации услуг техподдержки и сервисе[4].

Руководители компаний отмечают, что самыми популярными бизнес-кейсами применения генеративного ИИ являются маркетинг и продажи (создание креативных материалов), клиентский

сервис (подсказки операторам поддержки и диалоговые ассистенты), ИТ (ассистент написания кода для разработчиков) и внутрикорпоративные функции (генерация тренингов, проверка документов, автоматический скоринг интервью в массовом найме сотрудников)[1].

Скорость развития моделей ИИ существенно выросла за последние 10–15 лет благодаря активизации ключевых драйверов:

- рост скорости работы компьютеров выросла (в 10 млн раз с 1993 по 2022 гг.): со 124 млрд операций в секунду до 1,1 квинтиллиона операций в секунду;
- объем вычислений для обучения моделей ИИ удваивается каждые полгода, начиная с 2010 года и по настоящее время (ранее – 1 раз в 20 месяцев);
- увеличение объема доступной информации. По данным InternationalDataCorporation, размер глобальной дата сферы к 2025 г. достигнет 175 ЗБ против всего 33 ЗБ в 2018 году.

Одним из выдающихся примеров развития искусственного интеллекта в мире на данное время является компания “Amazon”, где разработана система FraudDetector, помогающая бороться с онлайн-мошенниками (в банках, онлайн-магазинах и крупных компаниях). Алгоритм данной программы следит за действиями пользователей в реальном времени, находит подозрительные заказы, блокирует платежи.

Согласно Указу президента РФ федеральный проект «[Искусственный интеллект](#)» включен в национальный проект «[Экономика данных](#)» (опубликован 15.02.2024года) [5].

Для разработки данной концепции в области развития технологий искусственного интеллекта собрано заседание при АНО «Цифровая экономика». Кроме этого, в России в 2022 году запущена программа реализации дорожной карты по развитию ИИ в контексте построения цифровой экономики.

Федеральный проект «Искусственный интеллект» предусматривает пакет мер, направленных на поддержку компаний-разработчиков ИИ, апробацию таких решений на российских предприятиях, повышение кадрового обеспечения, развитие системы науки и образования, формирование инфраструктуры для благоприятного развития отечественного искусственного интеллекта. Главными направлениями реализации стратегии являются[5]:

- повышение уровня обеспечения российского рынка технологий ИИ квалифицированными кадрами и уровня информированности населения о возможных сферах использования ИИ;
- поддержка научных исследований и разработок;
- разработка и развитие ПО, в том числе за счет поддержки стартапов и пилотных внедрений технологий ИИ;
- повышение доступности оборудования для работы с ИИ;
- создание комплексной системы правового регулирования в сфере ИИ;
- повышение доступности и качества данных для ИИ-задач.

Однако в реальности современная российская экономика указывает на неготовность активно применять технологии ИИ. Основная задача, которую необходимо решить в ближайшее время, – сформировать внутренний рынок технологий искусственного интеллекта. Стратегической задачей России на ближайшую перспективу является переход к шестому технологическому укладу, освоение и внедрение новых технологий, включая технологии ИИ. Именно они будут оказывать системное влияние на структуру и объемы производства и определять 60–80% прогнозируемого экономического роста в ближайшие 20–25 лет[6].

Положительными новостями, способствующими достижению быстрых планов Российской Федерации в области искусственного интеллекта, следует считать готовность к внедрению искусственного интеллекта в бизнесе. Согласно исследованиям Microsoft «Бизнес-лидеры в эпоху искусственного интеллекта», в Российской Федерации 30% руководителей активно и быстро внедряют новые технологии против 22,3% в мире. Это способствует положительной динамике качественных и скоростных изменений бизнес-среды.

В направлении развития искусственного интеллекта в России лидируют финансовый, ИТ-сектор и коммуникационный секторы. Уровень внедрения технологий ИИ достигает 53% компаний. Дальше по уровню использования искусственного интеллекта идут организации топливно-энергетического комплекса, промышленности, транспортные компании и медицинская сфера.

Малые предприятия за последние 5 лет также активно используют элементы искусственного интеллекта: интернет-сервисы, интернет-магазины, некрупное промышленное производство, транспортные организации, туристические фирмы. Большинство внедряемых решений на базе искусственного интеллекта – это виртуальные помощники. Таких «помощников» в управленческой сфере применяют 38%. Второе место занимают решения по прогнозированию, аналитике, машинному обучению – 35%.

Еще один важный фактор – это собственные разработки России в области искусственного элемента. В настоящем времени с помощью системы Botkin.AI в сфере медицины проводят диагностику онкологических заболеваний. Яндекс общается и передает информацию через голосового ассистента Алису, совсем скоро на наших дорогах появятся беспилотные авто Яндекса. Компания «КамАЗ» запускает тестирование автоматизированных грузовых автомобилей.

Согласно статистике за 2021-2024 гг. применение искусственного интеллекта организациями разных сфер экономики в РФ следующее:

✓ *транспортные перевозки*: применяют ИИ - 18%, планируют применять - 30%, не планируют использовать - 53%;

✓ *здравоохранение*: применяют искусственный интеллект - 16%, планируют применять - 34%, не планируют использовать - 51%;

✓ *промышленность*: применяют искусственный интеллект - 16%, планируют применять - 33%, не планируют использовать - 51%;

✓ *сельское хозяйство*: применяют искусственный интеллект - 12%, планируют применять - 37%, не планируют использовать - 51%;

✓ *строительство*: применяют искусственный интеллект - 3%, планируют применять - 32%, не планируют использовать - 65%.

Благодаря накопленной технологической базе и сильной инженерно-математической школе Россия активно участвует в развитии области генеративного ИИ и базовых моделей. Известные крупные технологические компании (Яндекс, Сбербанк) вкладывают денежные средства и разрабатывают собственные модели генеративного ИИ (YandexGPT, YandexART, GigaChat, Kandinsky) и решения на их основе. В ближайшие четыре года Сбербанк планирует вложить в ИИ около 2 млрд долларов и заработать порядка 6 млрд.

Так же, стремительное развитие искусственного интеллекта как внутри Российской Федерации, так и в контексте взаимодействия с другими странами, оказывает влияние на национальную безопасность. Инновационные военные приложения на основе ИИ используются для обороны страны многими странами, в том числе и РФ, например в области сбора и анализа разведанных, логистики, киберопераций, информационных операций, командования и управления, а также различных полуавтономных и автономных транспортных средствах. В этой связи технологии ИИ представляют собой вызовы для военной интеграции[7]. В России прорывные технологии ИИ представлены в оборонной промышленности, особенно в робототехнике. По данным Минобороны РФ в настоящее время российские военные имеют на вооружении более 2100 беспилотных летательных аппаратов, что делает российский беспилотный воздушный флот одним из крупнейших в мире. Что касается российских беспилотных наземных систем, то здесь разработана целая линейка для удовлетворения различных боевых потребностей (малые системы, и большие танковые транспортные средства, загруженные дальнобойным, противотанковым и зенитным вооружением). Таким образом, для усиления своей обороноспособности в РФ продолжается работа по внедрению элементов искусственного интеллекта в различные системы вооружения.

Одной из важных проблем массового применения технологий ИИ являются возможные враждебные кибероперации и «глубокие фейки», поскольку ИИ обеспечивает все более реалистичные фото, аудио и видео подделки, которые противники могли бы использовать в рамках своих информационных операций.

Кроме положительных сторон использования моделей ИИ при обеспечении национальной безопасности, учеными выделяются и возможные негативные последствия.

В итоге можно констатировать о быстротечном распространении технологий искусственного интеллекта во многих сферах экономической жизнедеятельности. Происходит неизбежное

взаимодействие человека с искусственным интеллектом, что несет в себе как положительные стороны, так и угрозы в обеспечении национальной безопасности государства. Россия делает все возможное, чтобы идти в ногу с мировым сообществом.

Список литературы:

1. Искусственный интеллект в России – 2023: тренды и перспективы //Яков и партнёры x Яндекс. 2023.
2. Искусственный интеллект (рынок России) URL:<https://www.tadviser.ru/index.php>(дата обращения: 29.04.2024)
3. Искусственный интеллект // Выбор экспертов. URL: <https://www.kp.ru/expert/elektronika/iskusstvennyj-intellekt/>(дата обращения: 15.04.2024)
4. 10 терминов искусственного интеллекта, которые нужно знать в 2024 году //РБК и трендыURL:<https://trends.rbc.ru/trends/industry/>(дата обращения: 29.04.2024)
5. О развитии искусственного интеллекта в Российской Федерации: Указ Президента Российской Федерации от 10.10.2019 № 490 // Официальный интернет-портал правовой информации.URL:<http://pravo.gov.ru/?oprd=1>
6. Ивановский Б.Г.Экономические эффекты от внедрения технологий «искусственного интеллекта» // социальные новации и социальные науки. - М: ИНИОН РАН, 2021. №2. С.8-25.
7. Горохова С.С. Искусственный интеллект в контексте обеспечения национальной безопасности // Национальная безопасность. 2020. № 3. С.15-31.

**ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ТРАКТОВКЕ
ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ ПРОМЫШЛЕННОСТИ КАК
ЭКОНОМИЧЕСКОЙ КАТЕГОРИИ
THEORETICAL AND METHODOLOGICAL APPROACHES TO THE INTERPRETATION
OF THE INDUSTRIAL ORGANIZATIONS ECONOMIC SECURITY AS AN ECONOMIC
CATEGORY**

С.А. Картель

**Белорусский государственный университет пищевых и химических технологий,
г. Могилев, Беларусь, e-mail: n_kartel@mail.ru**

S.A. Kartsel

**Belarusian State University of Food and Chemical Technologies,
Mogilev, Belarus**

e-mail: n_kartel@mail.ru

Аннотация: В современных условиях значимость проблемы обеспечения экономической безопасности неоспорима. Вместе с тем, не существует единого подхода к определению сущности понятия «экономическая безопасность». В статье сделана попытка обобщения, анализа и развития теоретико-методологических подходов к трактовке понятия «экономическая безопасность организаций промышленности» как комплексной экономической категории. Выделены шесть основных подходов к трактовке данной экономической категории: как состояние защищенности от внутренних и внешних угроз; как состояние эффективного использования ресурсов и потенциала; как способность к стабильному функционированию и развитию; как обеспечение конкурентных преимуществ; как реализация экономических интересов и целей; интегрированный подход. Определены преимущества и недостатки существующих подходов к трактовке экономической безопасности организации промышленности. Установлено, что под экономической безопасностью организации промышленности следует понимать такое состояние развития организации, при котором эффективное использование ее ресурсов и потенциала обеспечивает предотвращение значимых внешних и внутренних угроз, реализацию социально-экономических интересов и достижение стратегических целей бизнеса.

Ключевые слова: организация промышленности, экономическая безопасность, угрозы, ресурсы, конкурентные преимущества, устойчивость, развитие, экономическая независимость

Annotation: In modern conditions, the importance of the ensuring economic security problem is undeniable. At the same time, there is no single approach to the "economic security" concept essence defining. The article attempts to generalize, analyze and develop theoretical and methodological approaches to the interpretation of the "economic security of industrial organizations" concept as a complex economic category. Six main approaches to the economic category interpretation have been highlighted: as the state of protection from internal and external threats; as the state of resources and potential effective use; as the ability to stable functioning and development; as ensuring competitive advantages; as the economic interests and goals realization; as an integrated approach. The advantages and disadvantages of existing approaches to the industrial organization economic security interpretation have been determined. It has been established that an industrial organization economic security should be understood as the state of organization development in which the effective use of its resources and potential ensures the significant external and internal threats prevention, the socio-economic interests realization and the strategic business goals achievement.

Keywords: industrial organization, economic security, threats, resources, competitive advantages, sustainability, development, economic independence

Введение

25 апреля 2024 года делегаты VII Всебелорусского народного собрания утвердили Концепцию

национальной безопасности Республики Беларусь. В новой Концепции национальной безопасности указано, что экономическая безопасность – состояние защищенности отраслей и сфер экономики от воздействия угроз, препятствующих устойчивому социально-экономическому развитию Республики Беларусь. Устойчивое социально-экономическое развитие и высокая конкурентоспособность экономики страны определены в качестве одного из стратегических национальных интересов, а развитие цифровых технологий и регулируемой цифровой трансформации экономики – в качестве одного из основных национальных интересов в экономической сфере.

Экономическая безопасность государства не может существовать вне контекста экономической безопасности организаций промышленности; ее достижение возможно только на основе инновационной модернизации отечественных предприятий, их превращения в конкурентоспособные, устойчиво развивающиеся субъекты хозяйствования.

Проблемы экономической безопасности организаций промышленности в условиях развития цифрового общества становятся особо актуальными. Однако, несмотря на значимость проблемы обеспечения экономической безопасности, в настоящее время не существует единого общепризнанного подхода не только к методологии анализа экономической безопасности организаций промышленности, но и к определению сущности данной экономической категории. В результате недостаточной теоретической проработки данной проблемы снижается эффективность управления, и как следствие, эффективность функционирования субъектов хозяйствования.

Цель исследования заключается в анализе и развитии подходов к определению экономической безопасности организаций промышленности как этапа совершенствования механизма управления экономической безопасностью в современных условиях. Объект исследования – функционирование организаций промышленности. Предмет исследования – развитие теоретико-методологических подходов к трактовке понятия «экономическая безопасность организаций промышленности».

Материал и методы исследования. Основой исследования является системный подход к анализу трактовки экономической безопасности организаций промышленности. В процессе исследования применялись общенаучные методы теоретического познания: логического анализа, синтеза, сравнения и обобщения.

Развитие теоретико-методологических подходов к трактовке экономической безопасности создаст основу для разработки инструментов диагностики и совершенствования механизма управления экономической безопасностью организаций промышленности.

Результаты и их обсуждение. В современных условиях значимость проблемы обеспечения экономической безопасности неоспорима. Вместе с тем, не существует единого подхода к определению сущности понятия «экономическая безопасность».

В научной литературе понятие «экономическая безопасность» рассматривается применительно к нескольким уровням хозяйствования [18]: страна, регион, отрасль национальной экономики, организация.

Подавляющее большинство авторов выделяют и рассматривают два основных уровня вышеуказанного понятия: макроуровень (экономическая безопасность государства) и микроуровень (экономическая безопасность организации промышленности).

Однако, по обоснованному мнению ряда исследователей [3, 10, 12, 15 и др.], экономическая безопасность государства и экономическая безопасность организаций промышленности не существуют вне контекста друг друга, являются взаимосвязанными и взаимообусловленными.

Теоретико-методологические подходы к определению экономической безопасности организаций промышленности как многогранной и комплексной экономической категории изложены в многочисленных научных работах.

Исследователи выделяют разные значимые смысловые части в трактовке понятия «экономическая безопасность организации промышленности». Проведенный анализ позволяет выделить основополагающие подходы к трактовке вышеуказанной экономической категории, которые приведены в многочисленных научных работах.

Экономическая безопасность организации промышленности может быть определена как:
состояние защищенности от угроз;
состояние эффективного использования ресурсов;

способность к стабильному функционированию, развитию;
наличие конкурентных преимуществ;
возможность достижения целей.

Первый подход превалировал в 2000-2020 гг., представлен в работах В.И.Барахова, М.А.Бендикова, А.Ж.Есембековой, М.В.Зибарева, В.Ю.Савина, В.Н.Самочкина, А.И.Соловьева, В.Л.Шульца и др. [17 и др.] и определяет экономическую безопасность организации как состояние защищенности ее интересов или потенциала от угроз различного характера. Некоторые авторы называют данный подход стратегическим, антитеррористическим, защитным.

При этом, под угрозами подразумеваются факторы, дестабилизирующие функционирование субъекта хозяйствования (угрозы, ущерб, непредвиденные обстоятельства, опасность, нежелательные изменения).

Источники возникновения угроз трактуются двояко.

В первой трактовке (В.Н.Самочкин, В.И.Барахов, М.А.Бендикова) предполагается, что основные угрозы экономической безопасности организации возникают во внешней среде. Следовательно, акцент делается на обеспечение способности предприятия к воспроизводству и гибкому развитию путем адаптации к быстро изменяющимся условиям внешней среды.

Во второй трактовке (В.Ю.Савин, А.Ж.Есембекова, Г.В.Сушко) учтены как внешние, так и внутренние угрозы экономической безопасности, отражены элементы структуры предприятия, подверженные воздействию данных угроз.

По мнению ряда исследователей, подход на основе угроз является ограниченным и односторонним.

А.К.Моденов [9], А.С.Микаева [7] отмечают, что согласно данному подходу угрозы имеют первичный характер, а экономическая безопасность - следствие угроз и должна обеспечиваться только при их появлении. Однако, защита от угроз не является целью экономической деятельности, более того, наиболее эффективными мерами по обеспечению экономической безопасности являются превентивные, которые разрабатываются независимо от существования тех или иных угроз.

Е.А.Бидзюра также считает, что в рамках указанного подхода теряется видение перспектив развития организации, не учитываются ее жизненные интересы [2].

В рамках второго подхода А.А.Быков, А.М.Воротынская, Д.Г.Гончаренко, Д.М.Дрягунова, В.К.Сенчагов, Е.О.Усова, М.В.Фомина, А.Д.Шерemet, А.В.Шохнех, А.Яниогло и др. [5, 16] предполагают, что экономическая безопасность организации достигается за счет эффективного использования ее ресурсов. Подход получил название ресурсно-функциональный, ресурсно-ориентированный.

В трактовках некоторых авторов (Д.М.Дрягунова, А.В.Шохнех) экономическая безопасность рассматривается без ссылок на какие-либо угрозы, предприятие позиционируется как независимый субъект хозяйствования, способный к стабильному функционированию и развитию путем эффективного использования ресурсов.

Другие авторы (В.К.Сенчагов, А.А.Быков, М.В.Фомина, А.Д.Шерemet, Е.О.Усова, А.М.Воротынская, А.Яниогло, Д.Г.Гончаренко) указывают в качестве целей эффективного использования ресурсов не только обеспечение стабильного функционирования, но и предотвращение (минимизацию, нейтрализацию, ликвидацию) угроз, однако детально угрозы не рассматриваются. В данном контексте наиболее целесообразным представляется термин «предотвращение», поскольку он подразумевает как выявление потенциальных угроз, так и устранение их негативных последствий [2].

Детализируя виды используемых ресурсов, авторы выделяют внутренние ресурсы предприятия в различной трактовке:

все ресурсы (А.Д.Шерemet, Е.О.Усова, М.В.Фомина, А.В.Шохнех, А.Яниогло);
корпоративные ресурсы (В.К.Сенчагов);
сырьевые, финансовые и трудовые ресурсы (А.А.Быков);
финансовые, материальные и другие ресурсы (Д.М.Дрягунова);
основные и оборотные средства, человеческий потенциал (А.М.Воротынская).

Наиболее значимым достоинством ресурсно-функционального подхода является его комплексный характер, позволяющий применительно к обеспечению экономической безопасности выделять ее функциональные составляющие и влияющие на них факторы, индикаторы уровня безопасности, разрабатывать меры по повышению уровня функциональных составляющих экономической безопасности на основе анализа использования ресурсов организации [5].

Наиболее удачные подходы к выделению функциональных составляющих экономической безопасности субъекта хозяйствования предложены М.В.Самошкиной [13] и Т.В.Погодиной [11].

М.В.Самошкина выделила следующие составляющие экономической безопасности организаций промышленности: финансовую, экологическую, технико-технологическую, интеллектуальную и кадровую, силовую, информационную и политико-правовую. А.В.Минаев [8] дополнил данную классификацию рыночной составляющей.

В работе Т.В.Погодиной основные составляющие экономической безопасности – оборонно-промышленная, социальная, экологическая, финансовая, технологическая, энергетическая, продовольственная дополнены цифровой составляющей.

Неоспоримым достоинством ресурсно-функционального подхода является его перспективная ориентация, направленность на обеспечение стабильного текущего и перспективного функционирования организации.

Некоторые авторы указывают на недостатки данного подхода. Так, А.С.Микаева [7] указывает на то, что в рамках подхода не уделяется должного внимания состоянию внешней среды предприятия, как основного источника различных угроз. Кроме этого, не учитывается неравномерность развития и различный уровень защищенности функциональных подсистем организации.

А.Е.Суглобов в качестве недостатка подхода отмечает широту рассмотрения данной категории, при которой экономическая безопасность отождествляется с деятельностью субъекта хозяйствования и ее эффективностью.

Е.А.Бидзюра [2] считает, что акцентирование внимания только на внутренних ресурсах организации, не в полной мере соответствует действительности, поскольку не учитывает ситуацию возникновения внешних системных рисков и помощь государства восстановления уровня экономической безопасности.

Защитный и ресурсно-функциональный подходы являются наиболее распространенными при рассмотрении трактовки экономической безопасности организации. Имеют место и иные подходы, однако их целесообразно отнести к комбинированным, содержащим помимо основной смысловой направленности элементы ресурсно-функционального подхода или подхода на основе угроз.

А.В.Агибалов, Л.А.Запорожцева, В.К.Захаров, Н.А.Максимова и др. [6] связывают экономическую безопасность организации с ее способностью к устойчивому, стабильному развитию. При этом, стабильность функционирования организации определяется как возможность или способность противостоять дестабилизирующим воздействиям.

В работах Л.К.Ивановой, О.Б.Кузнецовой, Н.В.Манохиной, А.Е.Суглобова, С.А.Хмелева и др. экономическая безопасность трактуется как наличие конкурентных преимуществ организации. Однако, конкурентные преимущества организации связывают с эффективным использованием ресурсов, с соответствием потенциала и организационной структуры стратегическим целям и задачам, либо с эффективным использованием ресурсов и нивелированием угроз.

Данный подход не лишен недостатков, поскольку повышение конкурентоспособности может происходить за счет снижения уровня экономической безопасности. Такая ситуация наблюдается, когда субъект хозяйствования осознанно идет на коммерческие риски, например риск модернизации, при этом повышается его уязвимость в отношении внешних угроз [2].

Более того, только факт наличия конкурентных преимуществ не может гарантировать организации высокий уровень экономической безопасности, требуется их эффективная реализация [7].

Экономическая безопасность организации согласно работам С.В.Кавуна, В.Б.Зубика, Е.Н.Ланцман, М.В.Мясниковича, В.В.Пузикова, Р.С.Седегова, В.Л.Гамбовцева, В.В.Шлыкова и др. связывается с возможностью или способностью организации достигать поставленных целей и реализовать (защитить) свои экономические интересы, что, в свою очередь, связывается с совокупностью свойств состояния производственной подсистемы организации. Е.А.Бидзюра [2] называет данный подход интересодетерминированным.

При этом, ряд авторов в рамках указанного подхода не только акцентируют внимание на защищенности жизненно важных интересов организации, но и выделяют значимость внутренних и внешних угроз для обеспечения экономической безопасности.

По мнению А.И.Селиванова [14], существует объективная необходимость разработки интегрального подхода к определению понятия экономической безопасности организации, отражающего ее жизнеспособность и поступательное развитие; суверенитет как независимость от внутренних и внешних факторов; внутренний потенциал, достаточный для сохранения устойчивости в нестабильной внешней среде.

Многие авторы, в том числе Е.А.Бидзюра, В.Ф.Гапоненко, О.А.Грунин, И.В.Старченко, Г.В.Сушко, Н.В.Шашло и др. [2] в своих определениях экономической безопасности организации придерживаются интегрированного подхода, выделяя три основных момента:

критерий обеспечения экономической безопасности – реализация социально-экономических интересов и достижение стратегических целей организации;

условие достижения критерия – эффективность использования ресурсов и потенциала организации;

влияющие факторы – внутренние и внешние угрозы.

В рамках интегрированного подхода следует отметить работу Ю.А.Волковой [4], которая предложила универсальную трактовку экономической безопасности промышленной организации как комплекса экономических отношений, характеризующих состояние финансово-хозяйственной деятельности организации, включающего взаимосвязанные функциональную (достижение запланированных экономических результатов и финансово-коммерческих целей, устойчивое функционирование и развитие) и обеспечивающую (эффективность использования ресурсов, защищенность от угроз, наличие конкурентных преимуществ, способность к адаптации) составляющие, которые формируются, соответственно, текущим приоритетным вектором целей и совокупностью условий функционирования промышленной организации.

Помимо описанных основных подходов к определению понятия «экономическая безопасность организации» существует и иные, получившие меньшее распространение: рыночный; гармонизированный; дедуктивный; системный; уголовный.

К.Б.Беловицкий [1] дополнительно выделил подход, основанный на управленческих и экономических понятиях, где экономическая безопасность понимается как непрерывный процесс обеспечения стабильности функционирования организации.

На основе вышеизложенного, приведем классификацию подходов к определению экономической безопасности организации промышленности (рисунок 1).

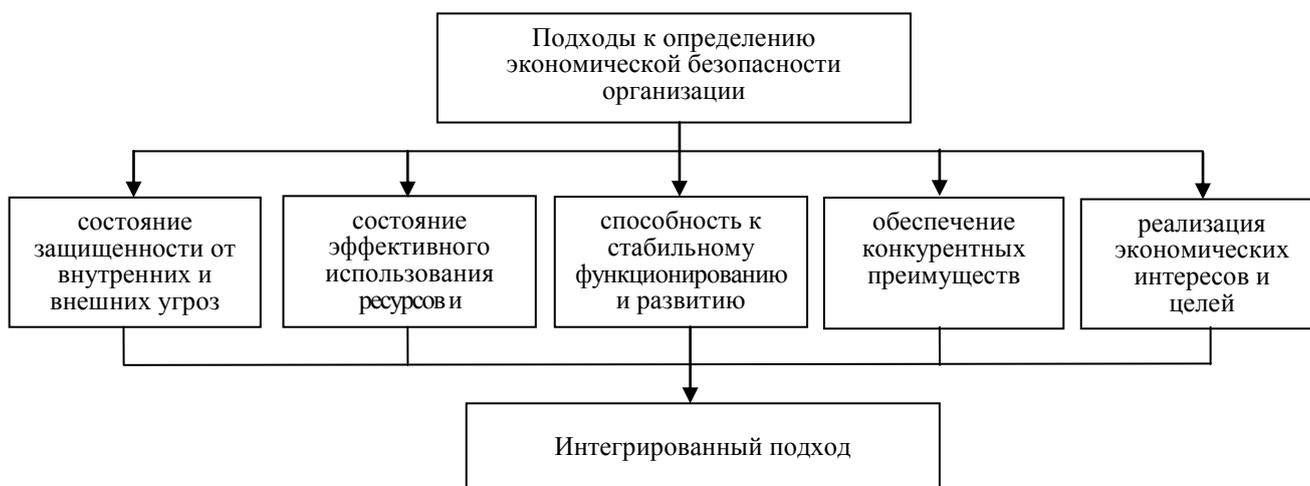


Рисунок 1 – Классификация подходов к определению экономической безопасности организации

Заключение

Несмотря на разные трактовки, можно выделить три важных элемента экономической категории «экономическая безопасность организации промышленности»: устойчивость, развитие и экономическую независимость.

Таким образом, экономическая безопасность организации промышленности – это такое состояние развития организации, при котором эффективное использование ее ресурсов и потенциала обеспечивает предотвращение значимых внешних и внутренних угроз, реализацию социально-экономических интересов и достижение стратегических целей бизнеса.

Список литературы

1. Беловицкий К.Б. Экономическая безопасность организации: моногр. / К.Б.Беловицкий. – Москва: Издательско-торговая корпорация «Дашков и К», 2023. – 183 с.
2. Бидзюра Е.А. Теоретические аспекты определения экономической безопасности как экономической категории / Е.А. Бидзюра // Экономическая наука сегодня: сб. науч. ст. БНТУ. – Минск, 2021. – Вып. 14. – С. 123–132.
3. Бидзюра Е.А. Теоретико-методологические подходы к определению экономической безопасности промышленных предприятий / Е.А.Бидзюра // Экономическая наука сегодня: сб. науч. ст. БНТУ. – Минск, 2022. – Вып. 15. – С. 100–108.
4. Волкова Ю.А. Исследование подходов к трактовке сущности экономической безопасности промышленной организации / Ю.А.Волкова // Вестник БГЭУ. – 2023. – № 2 (157). – с.19–26.
5. Гончаренок Д.Г. Подходы к определению экономической безопасности организации /Д.Г.Гончаренок // Бизнес. Образование. Экономика: Междунар. науч.-практ. конф., Минск, 2 апреля 2020 г. –Институт бизнеса БГУ, 2020. – Ч. 2. – С. 18–21.
6. Максимова Н.А. Развитие механизма диагностики и прогнозирования экономической безопасности промышленного предприятия: дисс. На соискание ученой степени канд. экон. наук. – Киров, 2023. – 231 с.
7. Микаева А.С. Подходы к понятию «экономическая безопасность хозяйствующего субъекта» / А.С. Микаева, Д.А. Течкин // Право, экономика и управление: состояние, проблемы и перспективы : материалы Всеросс. науч.-практ. конф. – Чебоксары: ИД «Среда», 2023. – С. 59–62.
8. Минаев А.В. Экономическая безопасность предприятия: понятие и сущность / А.В.Минаев, К.О.Аришонкова // Молодой учёный. – 2022. – № 46 (441). – С. 423–425.
9. Моденов А. К. Экономическая безопасность предприятия : моногр. / А. К. Моденов, Е. И. Белякова, М. П. Власов, Т. А. Лелявина. – СПб., 2019. – 550 с.
10. Невмывако В.П. Институциональные механизмы обеспечения экономической безопасности функционирования и развития малого / среднего предпринимательства /дисс.на соискание ученой степени канд.экон.наук. – Москва. – 2022. – 149 с.
11. Погодина Т.В. Экономическая безопасность и ее роль в обеспечении устойчивого развития России // Инновационное развитие экономики. – 2020. – № 1. – С.190–195.
12. Рыков И.Ю. Синтетический подход к определению категории «экономическая безопасность» / И.Ю.Рыков // Аудиторские ведомости. – 2021. – № 4. – С. 140–144.
13. Самошкина М.В. Роль информационных технологий в обеспечении экономической безопасности предприятия / М.В. Самошкина, Н.В. Бабина, П.А. Самошкин // Управленческий учет. – 2023. – № 7. – с. 113–119.
14. Селиванов А.И. Экономическая безопасность России: теоретический и практический ренессанс системного подхода / А.И.Селиванов // Вестник финансового университета. – 2017. – Том 21. – № 2. – С.12–22.
15. Солодовников С.Ю. Парадигмальный кризис белорусской экономической науки, цифровизация и проблемы подготовки кадров в сфере обеспечения национальной безопасности/С.Ю. Солодовников // Экономическая наука сегодня: сб. науч. ст. / БНТУ. – Минск, 2019. – Вып. 10. – С. 182–194.

16. Усова Е.О. Понятие и сущность экономической безопасности предприятия/Е.О.Усова, З.С.Булугин // X международная научно-практическая конференция «Современные тенденции и инновации в науке и производстве», – 2021. – С.271-1 – 271-5.

17. Шульц В. Л. Безопасность предпринимательской деятельности: учебник для вузов/ В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко. – М. : Юрайт, 2020. – 585 с.

18. Ячменева Е.Д. Практические аспекты формирования стратегии экономической безопасности компаний нефтегазовой отрасли / Е.Д.Ячменева, Ю.А.Дуболазова, Е.С.Замбрицкая // Экономические науки. – 2021. – № 2 (195). – С. 149–158.

**ВЛИЯНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ОБЕСПЕЧЕНИЕ
ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ**
**INFLUENCE OF MODERN INFORMATION TECHNOLOGY ON ENSURING ECONOMIC
SECURITY**

Е.А. Козлова, К.В. Васильченко

**Белорусский государственный университет пищевых и химических технологий, Республика
Беларусь, 212027, г. Могилев, пр. Шмидта, 3, email: kozlova@bgut.by**

Е.А. Kozlova, K.V. Vasilchenco

**Belarusian State University of Food and Chemical Technologies, Republic of Belarus, 212027,
Mogilev, Shmidt, 3, email: kozlova@bgut.by**

Аннотация: В работе рассмотрено понятие информационных технологий и их роль в обеспечении экономической безопасности организации, проанализированы направления обеспечения экономической безопасности и их реализация с использованием современных информационных технологий. Исследование проблем обеспечения экономической безопасности сохраняет свою актуальность. Это объясняется усилением влияния информационных технологий на все сферы деятельности.

Ключевые слова: экономическая безопасность организации, современные информационные технологии, риски и угрозы безопасности, методы и средства обеспечения экономической безопасности.

Abstract: The work examines the concept of information technologies and their role in ensuring the economic security of an organization, analyzes the directions for ensuring economic security and their implementation using modern information technologies. The study of problems of ensuring economic security remains relevant. This is due to the increasing influence of information technology on all areas of activity.

Keywords: economic security of the organization, modern information technologies, risks and security threats, methods and means of ensuring economic security.

Введение

Особую роль в развитии общества играет система обеспечения экономической безопасности государства. Современное общество находится в состоянии мирового финансового кризиса. Субъекты хозяйствования осуществляют свою деятельность в условиях цифровизации, используют инновационные технологии: большие массивы данных, облачные платформы, применение искусственного интеллекта, Интернет вещей, роботизация бизнес-процессов и др. Все это повышает прибыльность за счет экономии затрат и времени. Изучение трудов отечественных и зарубежных ученых показывает, что экономическая безопасность чаще отождествляется с финансовыми категориями. Однако в современной действительности важным является способ защиты экономических интересов предприятия. Возникает проблема обеспечения информационной составляющей экономической безопасности предприятия. Поэтому на первый план выходит вопрос применения современных информационных технологий в обеспечении экономической безопасности организаций. В этой связи, данная тема исследования является актуальной и практически значимой.

Цель исследования: Целью исследования является изучение влияния информационных технологий на обеспечение экономической безопасности.

Материал и методы исследования: Материалами для исследования выступили научные работы отечественных и зарубежных экономистов.

В процессе написания работы автором использованы методы теоретического исследования: системный, обобщения, сравнения и другие.

Результаты исследования и их обсуждение:

В условиях развития цифровой экономики значительно возрастает роль информации и информационных систем в обеспечении экономической безопасности, как отдельных организаций, так и государства в целом. Внедрение информационных технологий осуществляется на различных уровнях: на уровне предприятия, отраслей экономики, государства, что позволяет решать целый спектр проблем от безработицы на уровне государства до повышения эффективности деятельности конкретных организаций. Современные информационные технологии являются инструментом повышения производительности труда, роста эффективности производства.

Объемы информации, которые необходимо ежедневно обрабатывать для принятия управленческих решений, постоянно растут. Поэтому особенно востребованными становятся технологии по сбору, обработке, передаче, созданию и хранению баз данных. В процессе обычной хозяйственной деятельности организации постоянно сталкиваются с последствиями цифровизации, все глубже погружаются в информационную среду. В электронном виде хранятся отчеты, исходные данные, передача информации осуществляется посредством локальных и глобальных сетей. Именно поэтому возникает необходимость обеспечения безопасности информации и информационных систем.

В реалиях современного информационного общества обеспечение экономической безопасности может отождествляться с обеспечением информационной безопасности организации. Такая важность информационной безопасности в системе экономической безопасности приводит к формированию ряда угроз:

1) распространение ложной информации, которая может нанести ущерб организации. В современных реалиях возможно размещение на сайтах материалов, которые порочат компанию или ее руководителей, что приводит к формированию отрицательного мнения о компании. Бывают ситуации, когда конкуренты создают сайты-копии для организации недобросовестной конкуренции. Кроме того, возможно размещение негативных отзывов в социальных сетях и в средствах массовой информации. Борьба с перечисленными угрозами может производиться в двух направлениях: во-первых, это профилактика отзывов через собеседования с сотрудниками, мониторинг мнения об организации, контроль микроклимата в коллективе. Руководство должно быть максимально открытым к сотрудникам, быть готовым к диалогу, урегулированию конфликтов и поиску компромисса. Необходимо предупреждать работников об ответственности за публикацию негативной информации об организации. Чтобы минимизировать возможные негативные отзывы от клиентов необходимо проводить мониторинг удовлетворенности качеством сотрудничества с организацией, изучать проблемы, с которыми столкнулись клиенты, чтобы минимизировать их. Во-вторых, это работа с уже имеющимися негативными отзывами. Лучше всего такие отзывы не игнорировать, а принимать меры, в зависимости от содержания отзыва. Если отзыв негативный и носит абстрактный характер, человек писал его в особом эмоциональном состоянии, то необходимо сделать опровержение и описать реальное положение дел.

2) умышленные или случайные ошибки при работе с информационными системами. Данные ошибки могут представлять угрозу информационной безопасности. Под угрозами информационной безопасности можно понимать действия, которые могут привести к нарушению системы защиты информации. Угрозы информационной безопасности могут быть как естественными, так и искусственными, как преднамеренными, так и непреднамеренными.

3) нарушение правил работы с информационными потоками, так как в современных условиях важной задачей безопасности является обеспечение безопасного доступа к информационным потокам в компьютерных системах. Для решения этой задачи необходимо обеспечить идентификацию информационных потоков строгое ранжирование доступа к различным уровням информации.

4) сбои в программных продуктах и телекоммуникационных системах. Технологические сбои в работе программных продуктов могут нарушить работу предприятия, могут быть созданы бизнес-риски, приводящие к порче оборудования или выпуску бракованной продукции. Кроме того, программное обеспечение требует постоянного и системного обновления, появляются новые

компьютерные системы безопасности, а использование устаревших операционных систем или пользовательских конфигураций не всегда совместимо с новинками.

5) нарушение правил конфиденциальности при работе с информацией. Распространение конфиденциальной информации может осуществляться как случайно, так и намеренно и связано с отсутствием должного контроля за действиями персонала и слабой защитой конфиденциальной информации. Любая конфиденциальная информация должна быть представлена отдельным перечнем, подлежащим защите со стороны владельца.

6) идентификация пользователей информации для организации доступа к определенным потокам информации и защита от несанкционированного доступа. Для этого необходимо использовать как технические, так и программные средства. На практике используют такие методы защиты, как препятствия на пути предполагаемого похитителя, оказание воздействия на элементы защищаемой системы, маскировка данных, регламентация правил поведения при работе с базами данных. Каждый из методов защиты информации реализуется с помощью организационных и технических средств. Разрабатывается внутренняя документация, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией, проводят инструктаж и периодические проверки знаний по организации безопасной работы, разграничивают зоны ответственности и ранжируют доступ к информации, внедряют программные продукты, которые защищают данные от копирования или уничтожения любыми пользователями. Кроме того, организуется резервное копирование и удаленное хранение наиболее важных массивов данных, перераспределяются ресурсы в случае нарушения работоспособности отдельных элементов системы. Чтобы исключить неправомерный доступ к информации применяют такие способы как идентификация и аутентификация.

7) надежная антивирусная защита, которая реализуется как через установку надежных антивирусных программ, так и через разработку протоколов использования внешних носителей данных.

8) средства шифрования информации, которые используются для того, чтобы посторонний человек не смог прочитать информацию и понять. Сейчас шифрование используется в различных сферах: интернет-торговле, онлайн-коммуникациях, финансах, в электронном документообороте, на государственной и военной службе и т. д. Оно требуется везде, где происходит сбор, хранение и передача конфиденциальной информации, в том числе и пользовательских данных.

Защита информации должна проходить на постоянной основе с использованием различных средств: программных, организационных, физических. На практике известны инструменты, способные обеспечить защиту информации. Система информационной защиты организации должна охватывать следующие направления:

- защита организации от внешнего информационного воздействия;
- повышение квалификации сотрудников при работе с информационными ресурсами;
- нормативно-правовое регулирование вопросов информационной безопасности.

Для каждой организации информация является ценным ресурсом обеспечения прибыли и роста объемов производства, что может быть использовано не только самой организацией, но и конкурентами. Основная цель получения информации – конкурентные преимущества. Причем информация может быть использована и для создания прямого ущерба. Без информационных технологий невозможно представить хозяйственную деятельность организации. В совокупности все перечисленные факты говорят о том, что необходимо постоянное обеспечение информационной безопасности предприятия.

Однако, есть и еще одна проблема – бесконтрольный доступ в интернет. И эта проблема уже имеет не только информационный и экономический, но и социальный характер. В контексте рассматриваемой нами проблемы бесконтрольный доступ к интернету нельзя назвать намеренными вредоносными действиями. Но может быть причиной снижения производительности труда работников. Повсеместное внедрение информационных технологий оказывает не только прямое влияние на экономическую безопасность, но и косвенное. Так, использование виртуальных технологий приводит к формированию психологии виртуализации, когда стираются барьеры между виртуальным миром и реальным. Данное свойство современных технологий, которое обеспечивает

простоту выполнения повседневных задач, оказывает воздействие на все общество в целом, имея возможность управления им. Это создает угрозу экономической безопасности как отдельным физическим лицам, так и организациям, снижает производительность труда и создает потери трудового времени.

Комплексность перечисленных выше проблем требует комплексного подхода к их решению. Можно выделить следующие направления обеспечения экономической безопасности с использованием информационных технологий:

- 1) защита экономических интересов конкретных лиц через защиту интеллектуальной собственности и обеспечение достойного вознаграждения за труд, для чего используются различные базы данных;
- 2) обеспечение безопасности персональных данных при использовании безналичных расчетов, торговых площадок, систем бронирования т. д., для чего необходимо использования особых идентификационных инструментов;
- 3) обеспечение финансовой безопасности конкретных лиц, через использование различных инструментов группы больших данных;
- 4) защита экономических интересов общества через обеспечение гарантий соблюдения законодательства в сфере проведения конкурсных процедур, путем использования электронных систем регистрации и обработки данных;
- 5) обеспечение бесперебойности всех производственных процессов через автоматизацию технологических процессов и производств, создание «умных» заводов и производств;
- 6) обеспечение финансовой платежеспособности, устойчивости и ликвидности организаций через развитие национальных платежных систем;
- 7) прогнозирование и управление рисками через мониторинг экономической, финансовой и правовой ситуации на международном и внутреннем рынках с использованием информационных технологий;
- 8) развитие импортозамещения для обеспечения финансовой независимости и минимизации рисков;
- 9) перспективное планирование деятельности на всех уровнях экономической системы с использованием многофакторного анализа;
- 10) разработка стратегии экономического развития с учетом минимизации рисков и угроз.

Перечисленные выше направления реализуются с использованием современных информационных технологий. Они влияют на скорость получения и обработки информации. Информационные технологии также влияют и на ускорение процесса производства через автоматизацию технологических процессов и производств.

Выводы (заключение)

Таким образом, информационные технологии в современном обществе являются основой обеспечения экономической безопасности государства и отдельных организаций.

Применение информационных технологий формирует информационную культуру, навыки работы и возможности.

Список литературы

- 1 Касперович С. А. Экономическая безопасность предприятия: сущность, цели и направления обеспечения / С. А. Касперович, Е. А. Дербинская // Труды БГТУ. – Минск: БГТУ, 2016. – № 7 (189). – С. 278 – 282.
- 2 Концепция национальной безопасности Республики Беларусь: утв. Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575: в ред. Указа Президента Республики Беларусь от 30 декабря 2011г. № 621 // Нац. правовой интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: <http://www.pravo.by/main.aspx?guid=3871&p2=1/12080>. – Дата доступа: 17.04.2024.
- 3 Лапыгин Д.Ю., Караман К.С. Обеспечение экономической безопасности инструментами информационных технологий / Д.Ю. Лапыгин, К.С. Караман // Экономическая безопасность. – 2023. – Том 6. – № 1. – С. 429-442. – [Электронный ресурс]. – Режим доступа: [10.18334/ecsec.6.1.117577](https://doi.org/10.18334/ecsec.6.1.117577). – Дата доступа: 17.04.2024.

- 4 Об организации мониторинга важнейших показателей экономической безопасности Республики Беларусь: постановление Совета Министров Республики Беларусь от 22 февраля 2007 г. № 226 (в ред. постановления Совета Министров от 16 декабря 2008 г. № 194-3) // Нац. правовой интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: <http://www.pravo.by/main.aspx?guid=3871&p2=1/12080>. – Дата доступа: 17.04.2024.
- 5 Пузилов В.В. Методология обеспечения экономической безопасности и ее трансформация в условиях информационного развития / В.В. Пузилов // Бизнес, инновации, экономика, 2021. – Вып. 5. – С. 54–61.
- 6 Серебрякова Н.А. Формирование системы обеспечения экономической безопасности предприятия / Н.А. Серебрякова, С.А. Волкова, Т.А. Волкова // Вестник ВГУИТ. 2016. №4 (70). – [Электронный ресурс]. – Режим доступа: URL: <https://cyberleninka.ru/article/n/formirovanie-sistemy-obespecheniya-ekonomicheskoy-bezopasnosti-predpriyatiya>. Дата доступа: 17.04.2024).
- 7 Скворцова И.А., Емелин В.Н. Влияние информационных систем в обеспечении экономической безопасности / И.А. Скворцова, В.Н. Емелин // Контентус, 2016. – №5 (46). – [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/vliyanie-informatsionnyh-sistem-v-obespechenii-ekonomicheskoy-bezopasnosti>. – Дата доступа: 17.04.2024.
- 8 Тарасова Н.В., Дорошкин С.Е. Влияние информационных технологий на экономическую безопасность / Н. В. Тарасова Н.В., С. Е. Дорошкин // Экономика и бизнес: теория и практика, 2020. — №2-2. – [Электронный ресурс]. – Режим доступа: URL: <https://cyberleninka.ru/article/n/vliyanie-informatsionnyh-tehnologiy-na-ekonomicheskuyu-bezopasnost> – Дата доступа: 17.04.2024. (дата обращения: 14.05.2024).

ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

THE PROBLEM OF INFORMATION SECURITY IN THE CONTEXT OF DIGITALIZATION OF SOCIETY

Магомедов Адам Абдурахимович,

студент 1 курса, Северо-Кавказский институт
(филиал) ВГУЮ (РПА Минюста России)

г. Махачкала, Россия

Email: m1gmdv@mail.ru

Magomedov Adam Abdurakhimovich

1st year student, North Caucasus Institute

(branch) VGUY (RPA of the Ministry of Justice of Russia)

Makhachkala, Russia

Email: m1gmdv@mail.ru

Аннотация: Мировые СМИ единодушно утверждают, что число случаев угрозы информационной безопасности защищенных сайтов не только не уменьшается, но и продолжает увеличиваться с неуклонным натиском. В эпоху, когда цифровая трансформация становится ключевым фактором процветания множества предприятий, на передний план выходит задача надёжной защиты информационных систем. В этой публикации мы освещаем вопросы информационной защиты, которые сопровождают широкомасштабное введение цифровых технологий в общество, анализируем и описываем конфликты, опасности и угрозы, которые вызывает цифровизация экономики.

Abstract: The world's mass media unanimously assert that the number of cases of threats to the information security of protected sites is not only not decreasing, but also continues to increase with a steady onslaught. In an era when digital transformation is becoming a key factor in the prosperity of many enterprises, the task of reliable protection of information systems comes to the fore. In this publication, we highlight the issues of information protection that accompany the large-scale introduction of digital technologies into society, analyze and describe the conflicts, dangers and threats caused by the digitalization of the economy.

Ключевые слова: информационная безопасность, цифровизация, цифровая трансформация, киберпреступность, новые информационные технологии, риски и угрозы цифровой экономики.

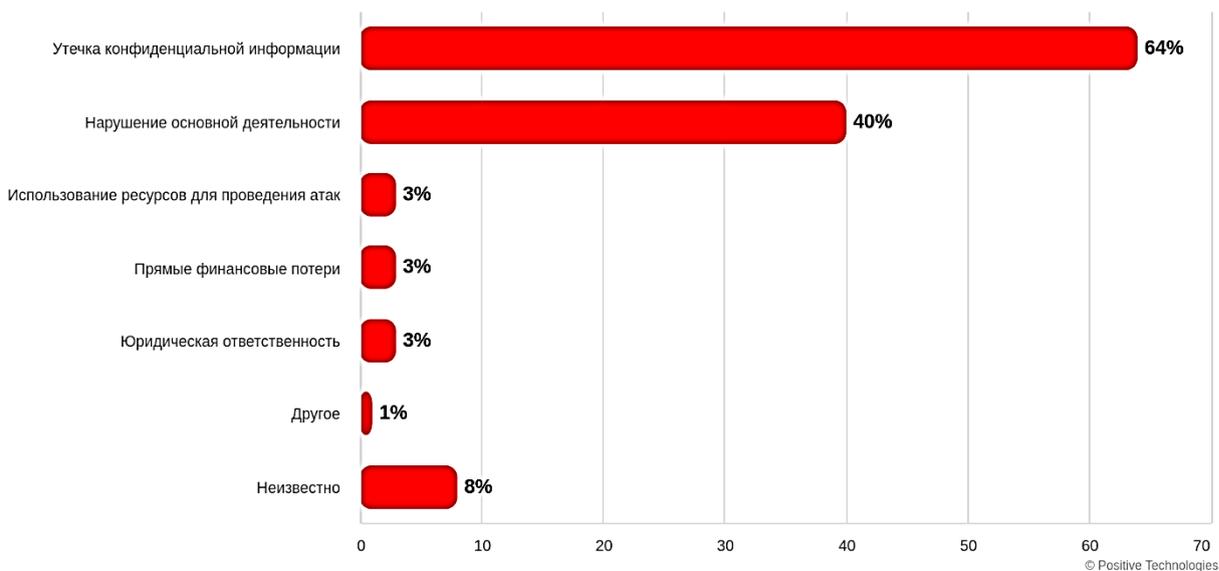
Keywords: information security, digitalization, digital transformation, cybercrime, new information technologies, risks and threats of the digital economy.

В эпоху цифровизации ни одна отрасль не обходится без использования компьютерных технологий для сбора, обработки и сохранения информации. Поэтому информация приобретает особую важность и становится ключевым ресурсом, требующим эффективных методов защиты. Превентивные действия по предотвращению угроз и рисков в условиях цифровой экономики, обеспечение безопасности информационно-технологической среды стали основой конкурентоспособности для человека, бизнеса и государства. Не секрет, что информационная безопасность играет важную роль в нашей жизни. Кибератаки на инфраструктуру, транспорт, банковскую сферу и другие области непосредственно затрагивают каждого из нас. В связи с этим возникает ряд вопросов: какие данные безопасно публиковать в сети, какими данными можно управлять, как обеспечить их защиту, и кто имеет доступ к ним. Решение этих и других связанных вопросов способствует повышению надежности информационной инфраструктуры государственных корпораций, бизнеса, защите частных лиц и страны в целом. Согласно информационной справке, на сегодняшний день количество активных пользователей кредитных карт на начало 2024 года

превысило 27 млн человек за год оно выросло на 6,6 млн. Это больше, чем количество заемщиков по кредитам наличными (24 млн человек) [3]. Такая ситуация возникает впервые, отмечает ЦБ в Анализе тенденций в сегменте розничного кредитования на основе данных кредитных бюро. 76% граждан РФ пользуются интернетом. Общее число мобильных телефонов в два раза превышает численность населения страны. Такой прогресс в цифровой сфере экономики порождает новые вызовы и риски для всех участников экономических процессов. Многие неправильно интерпретируют процесс цифровизации как простое оборудование компьютерными и информационными системами. Однако данная проблема гораздо более обширна: она затрагивает государственную политику, правовые и административные отношения. При удержании старой парадигмы, согласно которой конфиденциальные данные или данные, подлежащие охране, существуют лишь на бумаге и могут быть переданы через традиционную почту, обеспечивается высокий уровень безопасности, но низкая скорость обмена информацией. Поэтому цифровая экономика должна найти оптимальный баланс между безопасностью и высокой скоростью обмена данными, что в конечном итоге способствует увеличению ВВП и развитию экономики страны, а следовательно, улучшению качества жизни каждого гражданина. Мы находимся в переломном периоде, где старые порядки быстро уступают место новым технологиям, изменяется личная жизнь, происходит преобразование рабочих мест, возникают новые профессии и так далее. Применение современных информационных технологий приводит к увеличению эффективности всех сфер деятельности, расширяя возможности для проведения различных операций через компьютер и другие устройства, включая предоставление услуг, совершение транзакций и другие действия. Однако помимо явных преимуществ, цифровая трансформация несёт в себе значительные риски, связанные с проблемами обеспечения безопасности информации в информационной среде. При взаимодействии в сфере информации государственные интересы, интересы бизнеса и частных лиц заключаются в обеспечении двух ключевых аспектов безопасности: с одной стороны, конфиденциальные данные должны быть доступны законным пользователям, с другой стороны, должны быть надежно защищены от несанкционированного доступа. Главная цель обеспечения информационной безопасности на всех уровнях (личном, корпоративном, государственном) заключается в предотвращении любого ущерба. Несанкционированное распространение, изменение или уничтожение конфиденциальной информации, а также нарушение процессов ее обработки и передачи приносят неприемлемый ущерб как материальный, так и моральный для всех участников взаимоотношений. Появление организованной киберпреступности как новой формы преступлений требует от специалистов в области информационной и экономической безопасности выделения приоритетных задач по предотвращению киберугроз в следующих направлениях:

- 1) защита персональных данных граждан;
- 2) безопасность коммерческих информационных систем;
- 3) безопасность информационных систем государственных структур;
- 4) защита рабочей среды и технологий.

Киберугрозы и ущерб от киберпреступников вышли на второе место в мире после техногенных катастроф [1]. По данным ЦБ России, в первой половине 2023 года злоумышленники украли с банковских счетов и карт россиян порядка 4,5 млрд рублей [4]. Объем похищенных средств непрерывно растет не первый год, а в 2023 увеличился почти на 30% по сравнению со средними показателями 2022 года. Если говорить о потерях самих банков из-за действий киберпреступников, то в прошлом году ущерб оказался незначительным. Среди последствий атак выделяются утечки данных (64%), остановка работы отдельных сервисов или ключевых бизнес-процессов (40%). Подобные выводы были сделаны и в прошлогоднем исследовании, тогда доля утечек составляла 51%, а нарушение основной деятельности компании возникало в результате 42% инцидентов. Эта тенденция объяснима: сложные атаки на хорошо защищенные финансовые организации с целью кражи денег стали редким явлением на фоне роста более простых в реализации атак вымогателей и крупных утечек данных клиентов. В марте прошлого года в социальных сетях начала распространяться ссылка на сайт, на котором были личные данные пользователей «Яндекс.Еды» в виде карты, там были указаны адрес доставки, телефон, электронная почта, сумма заказов за последние полгода. По данным телеграм-канала «Утечки информации» от DLBI, в Сеть было



выложено порядка 49 млн строк. Позднее руководитель «Яндекс.Еды» Роман Маресов в блоге компании извинился перед пользователями за утечку и заверил, что компания пытается не дать данным пользователей распространиться дальше. Маресов также назвал утечку беспрецедентным случаем. В прошлом году также стало известно об утечках СДЭК. Сначала, в конце февраля, телеграм-каналы сообщали об утечке о клиентах доставки, которая содержала файл с 466 млн строк с ID и телефонами и еще один с 822 млн строк с ID, Ф.И.О. и адресами электронной почты. СДЭК официально подтверждала факт утечки, но заявила, что в базе нет номеров документов и иной важной персональной информации, в том числе платежной [8]. Злоумышленники сегодня не только продают базы данных, но и раздают их бесплатно, таким образом наказывая организации за отказ от уплаты выкупа. Стоимость таких баз и распространенность предложений о продаже и покупке на теневых площадках рассмотрены в следующем разделе [2]. Аналитики утверждают, что в одном из самых технологично продвинутых государств мира утечки персональных данных уже не являются редкостью. Они утверждают, что вероятность таких инцидентов высока, и, хотя можно принять меры для минимизации риска, полностью исключить утечки не удастся. В США, которая выступает в качестве лидера в области цифровых инноваций и определяет направления в этой сфере, становится очевидным, что проблема заключается в том, что слишком быстро внедряются передовые информационные технологии в различные отрасли [6]. В самих штатах по состоянию на февраль 2024 года самым значительным инцидентом с утечкой данных в Соединенных Штатах была утечка данных Yahoo, произошедшая в 2013-2016 годах. Этот инцидент, затронувший более трех миллиардов онлайн-пользователей, по-прежнему остается одной из самых значительных утечек данных во всем мире. Вторым по величине случаем стала утечка данных в Microsoft в январе 2021 года, в которой пострадали около 30 тысяч компаний в Соединенных Штатах и около 60 тысяч компаний по всему миру. [7] Новейшие технологии, пользующиеся популярностью, несут в себе определенные риски, так как могут содержать не только свежие вирусы, вредоносные программы, тайные устройства и уязвимости, но и угрозы несанкционированного управления, нарушения конфиденциальности и целостности информации. Поэтому важным аспектом внедрения новых технологий является обеспечение цифрового суверенитета, так как следуя за технологиями других стран, можно оказаться в подчиненном положении, став заложником в данной ситуации. Специалисты по информационной безопасности подчеркивают, что пришло время пересмотреть стандартные подходы к защите информации и улучшению надежности передовых технологий. Они рекомендуют использовать персонализированный метод для каждого отдельного объекта защиты, что включает в себя выбор защитных мер в соответствии с постоянным мониторингом тенденций в отдельных сегментах и оперативное внедрение корректировок. Переход традиционных экономических процессов в цифровую среду влечёт за собой необходимость тщательной разработки защитных механизмов для каждого из них, учитывая их уникальные особенности и динамически меняющиеся условия. Только персональный подход и предварительная работа над защитой

обеспечивают значительно более надежное обеспечение целостности, доступности и конфиденциальности данных в цифровых системах. На наш взгляд для борьбы с этими угрозами необходимо не только улучшать технические средства защиты, но и обучать пользователей основам кибербезопасности, а также в ст. 13.11 КоАП РФ внести изменения касательно размера административного штрафа за утечку персональных данных, к тому же за повторное совершение административного правонарушения тоже увеличить размер административного штрафа. Также же на наш взгляд необходимо ввести уголовную ответственность за использование, передачу, сбор и хранение персональных данных. Важно осознавать, что каждый человек, взаимодействуя с цифровыми технологиями, играет ключевую роль в обеспечении информационной безопасности. Принятие правильных мер для обеспечения безопасности информации в эпоху цифровой трансформации требует комплексного подхода и сотрудничества всех участников процесса. Только совместными усилиями государства, бизнеса и обычных пользователей мы сможем гарантировать надежную защиту цифровых данных и сохранить конфиденциальность в онлайн сфере.

Список использованной литературы:

1. Удалов, Д. В. Угрозы и вызовы цифровой экономики / Д. В. Удалов // ИБР. - 2018. - № 1 (30). - URL: <https://cyberleninka.ru/article/n/ugrozy-i-vyzovy-tsifrovoy-ekonomiki>
2. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года URL: <https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/>
3. Число пользователей кредитных карт впервые превысило число людей с кредитом наличными URL: <https://www.forbes.ru/finansy/509494-cislo-pol-zovatelej-kreditnyh-kart-vpervye-prevysilo-cislo-ludej-s-kreditom-nalichnymi>
4. ЦБ впервые раскрыл сумму предотвращенных хищений у россиян из банков- РБК URL: <https://www.rbc.ru/finances/01/06/2023/647893829a7947ded1447b20>
5. Проблемы информационной безопасности в условиях цифровой трансформации общества // Соловьева Т.В.
URL: <https://cyberleninka.ru/article/n/problemy-informatsionnoy-bezopasnosti-v-usloviyah-tsifrovoy-transformatsii-obschestva>
6. РСМД: Технологическая политика США
URL: <https://russiancouncil.ru/analytics-and-comments/analytics/tekhnologicheskaya-politika-ssha-v-usloviyakh-sopernichestva-s-kitaem/>
7. Самые значительные утечки данных в США по состоянию на февраль 2024 года в разбивке по последствиям URL: <https://www.statista.com/statistics/1448545/us-biggest-data-breaches/>
8. В России за год утекло более 660 млн записей с персональными данными URL: https://www.rbc.ru/technology_and_media/17/04/2023/643936229a7947134f0ce21c

**АКТУАЛЬНОСТЬ ИНКЛЮЗИВНОЙ ЗАНЯТОСТИ
В ЭКОНОМИКЕ БЕЛАРУСИ
RELEVANCE OF INCLUSIVE EMPLOYMENT IN THE ECONOMY OF BELARUS**

Н.В. Маковская

Могилевский государственный университет им. А.А. Кулешова

г. Могилев, Беларусь, e-mail: maknata@mail.ru

N.V. Makovskaya

Mogilev State University named after A.A. Kuleshov

Mogilev, Belarus, e-mail: maknata@mail.ru

Аннотация: Представлены актуальность и специфика социально-экономической модели инклюзивной занятости в национальной экономике Беларуси. Обоснованы ее преимущества и необходимость для современных условий развития.

Ключевые слова: инклюзия, занятость, рынок труда, трудоустройство, социальные условия.

Abstract: The relevance and specificity of the socio-economic model of inclusive employment in the national economy of Belarus is presented. Its advantages and necessity for modern development conditions are substantiated.

Keywords: inclusion, employment, labor market, employment, social conditions.

Введение

Инклюзивная занятость является новой социальной прерогативой современного белорусского рынка труда. Главной социальной целью инклюзивной занятости является «встроенность» в трудовую сферу общества социально уязвимых слоев населения, и прежде всего, граждан с ограниченными физическими возможностями. Существует необходимость привлечения внимания правительства, бизнеса, гражданского общества и всей общественности к проблемам социально уязвимых слоев населения, активизировать внутренние ресурсы для их поддержки, интегрировать новые формы взаимодействия и кооперации для реального их включения в активную экономическую и общественную жизнь. Привлечение внимания необходимо в контексте адаптации таких слоев населения в трудовую сферу государства.

Цель исследования. Обосновать необходимость создания модели инклюзивной занятости. Инклюзивную занятость целесообразно оформлять в виде специальной, социально ориентированной бизнес-модели, которая будет представлять собой уникальный способ ведения бизнеса, который направлен на устойчивые решения социальных проблем, снижение уровня бедности и создание безбарьерной среды и возможности самостоятельного получения дохода для социально уязвимого населения Республики Беларусь, сохраняя при этом коммерческую выгоду для предприятия и организаций.

Результаты и их обсуждение. Для предприятий и организаций, инклюзивные бизнес-модели - это возможность для роста и конкурентное преимущество, расширение рынка, использование инновационных подходов, укрепление систем снабжения, рост деловой репутации и имиджа, и, как следствие лояльности клиентов и власти. Для Республики Беларусь инклюзивная занятость воплощает в себе эффективный подход к социально-экономическому росту и развитию. Для граждан с ограниченными возможностями это наличие устойчивого дохода, расширение и возможность их профессиональных возможностей. Кроме этого, инклюзивная занятость служит источником качества жизни, социальной интеграции и гарантий, устойчивых средств к существованию.

Инклюзивная бизнес-модель, с включением в нее работников с ограниченными возможностями, имеет такую же структуру (клиенты, покупатели, партнеры и т.п.), как и стандартная производственно-коммерческая модель реализации хозяйственной деятельности. Такая модель способна обеспечить взаимовыгодное развитие с участием граждан страны с ограниченными способностями.

Одним из условия создания инклюзивной бизнес-модели, с включением в нее элементов инклюзивной занятости, является включение уязвимых слоев населения в организационную и производственно-сбытовую цепь. Таким образом, социально уязвимые слои населения с низким уровнем дохода получают шанс стать частью производственной структуры в качестве сотрудников, дистрибьюторов, розничных торговцев и т.п. Еще один вариант создания инклюзивного бизнеса, с включением инклюзивной занятости, подразумевает производство специфической продукции, имеющей спрос (например, разновидности ремесленной продукции, мелкие комплектующие детали и т.п.).

В условиях белорусской экономики инклюзивная занятость и бизнес-модели ее реализующие может иметь место в таких сферах как создание линейки доступных дешевых продуктов и услуг, ремесленничество, телекоммуникации, посредничество и т.п.

Отдельно, следует выделять значимость инклюзивной занятости, в рамках реализации целей устойчивого развития, которые генерируют отдельные инициативы по работе с гражданами с ограниченными возможностями. Такие инициативы позволяют встраивать инклюзивную занятость в рынки труда малых городов и сельских населенных пунктов, создавая новые предприятия, развивая кооперацию, вовлекая в трудовую деятельность социально-уязвимые слои населения, обеспечивая тем самым устойчивое развитие не только отдельным предприятиям и организациям, но и региону в целом.

В целом, для существования инклюзивной занятости есть необходимость в разработке и внедрении модели инклюзивной среды, которая будет адекватна образовательной инфраструктуре в стране и без барьерному пространству. Будет определять условия для формирования инклюзивной занятости на микроуровне. Понятно, что этому будет способствовать: нормативно-правовая база по инклюзивной занятости; создание образовательных центров по развитию инклюзивного образования; создание специальных социально-психологических служб, сопровождающих трудовой процесс социально уязвимых слоев населения; специальное материально-техническое обеспечение трудового процесса на инклюзивных рабочих местах, в том числе информационное; создание специальных адаптационных программ занятости на инклюзивных рабочих местах.

Важность инклюзивной занятости связана и с тем, что существует ментальная потребность в ее существовании, которая позволяет аргументировать ценность человека-работника не зависимо от его способностей и достижений; возможности человека в условиях его физической ограниченности; констатировать возможности людей с ограниченными возможностями в контексте их коммуникаций и общения; увидеть возможности в инклюзивной занятости как условия реализации профессионального образования.

Целесообразно различать виды инклюзии, которые формируют специфику инклюзивной занятости. Так, выделяют полную инклюзию – люди, имеющие инвалидность в опорно-двигательном аппарате, но способные к трудовой деятельности и частичную инклюзию – люди не ограничены в движениях, но требующие коррекционных мероприятий, связанных с восприятием окружающей среды. Эти виды инклюзии определяют как особенности организации трудового процесса, так и, в принципе, структуру организации как отдельного инклюзивного субъекта на рынке труда (предприятия, фирмы, где заняты исключительно работники с ограниченными возможностями). Если предприятие внедряет формы занятости в виде частичной инклюзии, то организация работы таких работников, связана со специальными адаптированными производственными программами, которые ориентированы на работников с ограниченными возможностями.

С точки зрения практической реализации концепции инклюзивной занятости в Беларуси первостепенное значение приобретает теоретико-методологическая основа для встраиваемости и анализа такой формы занятости в национальный рынок труда. Такой основой может стать концепция экстрабилити [1-2], которая предполагает использовать следующий набор методов для анализа инклюзивной занятости и трудоустройства:

- метод сравнительного анализа, позволяющий четко определить разницу, преимущества и недостатки в понятиях: «инклюзивное трудоустройство», «инклюзивная занятость», «сопровождающее трудоустройство», «социальная занятость инвалидов»;

- метод статистического мониторинга, направленный на определение современных тенденций в инклюзивной среде, в том числе, в инклюзивной занятости, на рынке труда;
- метод вторичного анализа данных основанный на социологических исследованиях, изучающих проблемы трудоустройства, барьеры при найме работников с ограниченными возможностями, условия найма и тенденции увольнения, существующие на рынке труда.

Заключение

Таким образом, для национальной экономики Беларуси представляет значимый интерес социально-экономическая модель инклюзивной занятости с учетом ее структуры, места на рынке труда, с определением источников финансирования на всех хозяйственных уровнях и наличием имеющейся инклюзивной среды. Такая модель, в свою очередь, потребует институциональное сопровождение инклюзивной занятости в Республике Беларусь.

Кроме этого, актуальность социально-экономической модели инклюзивной занятости позволит работникам с ограниченными возможностями самостоятельно формировать свой доход и иметь равный доступ к общественным благам. Существует социальная потребность в таком сегменте рынка труда как инклюзивная занятость, что позволит государственной политике углубить свою социальную направленность [3].

Социально-экономическая модель инклюзивной занятости представляет собой уникальный способ обеспечения благосостояния и реализации права на труд граждан с ограниченными способностями. Такая модель позволит решить социальные проблемы, связанные с данной категорией работников, повысить уровень их благосостояния, обеспечить уровень социальной конкурентоспособности работодателей за счет роста деловой репутации и имиджа. Следствием этого станет общая лояльность клиентов. Для государства инклюзивная модель занятости будет воплощать эффективный подход к социально-экономическому росту. Для граждан и работников с ограниченными способностями данная модель расширит возможности интеграции в трудовую среду и формировать свой личный доход для полноценного использования материальных благ.

Список литературы

1. Колпащиков О.Б. Экстрабилити людей с инвалидностью в инклюзивном и социальном проектировании // Экстрабилити как феномен инклюзивной культуры: материалы Всерос. науч.-практ. конф.- Екатеринбург: Изд-во Уральского университета, 2019. – 124с.
2. Антонова В.К., Присяжнюк Д.И. Креативный эффект, инвестиции и инклюзия как норма жизни: установка HR-менеджеров России в отношении инклюзивного трудоустройства // Журнал исследований социальной политики. – 2021.- Т.19.-№3. – С.373-388
3. Зенькова Л.П., Захарова С.Г., Крицкая Н.В., Мозоль А.А. Параметры рынка труда в Беларуси и Узбекистане как упреждающие индикаторы современных экономических кризисов // Бел.эконом. журнал. - № 1. – 2024.- С.85-98

ПРОБЛЕМЫ ФОРМИРОВАНИЯ ЦЕНОВЫХ ИНДИКАТОРОВ НА ТРАДИЦИОННЫХ И ЦИФРОВЫХ РЫНКАХ РФ И РБ
ISSUES OF PRICE INDICATORS DEVELOPING ON TRADITIONAL AND DIGITAL MARKETS OF RUSSIA AND BELARUS

^{1,2} А.И. Мелешкина

1. Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации,

Россия, 119571, г. Москва, проспект Вернадского, 82-84, email: ann.meleshkina@mail.ru

2. Московский государственный университет имени М.В. Ломоносова,

Россия, 119991, г. Москва, Ленинские горы, 1

^{1,2} A.I. Meleshkina

1. The Russian Presidential Academy of National Economy and Public Administration, 82 Prospekt Vernadskogo, Moscow, 119571, Russia, email: ann.meleshkina@mail.ru

2. Lomonosov Moscow State University, 1 Leninskiye Gory, Moscow, 119991, Russia

Аннотация: В исследовании рассматриваются методы формирования ценовых индикаторов на товарных рынках в условиях высокой экономической неопределенности как в результате санкционного давления, так и вследствие ухода зарубежных аналитических агентств, предоставлявших ранее рыночные индексы цен. Анализу подлежат две группы методов: на традиционных рынках – создание системы биржевых индексов и внебиржевых индикаторов, на цифровых рынках – совершенствование требований антимонопольного законодательства к совершению сделок экономической концентрации. Результаты проведенного анализа свидетельствуют о наличии пробелов как в правовых основах экономического регулирования, так и в технологических механизмах реализации стратегии формирования ценовых индикаторов. Результаты исследования могут представлять интерес как для участников товарных рынков РФ и РБ в качестве направления развития комплаенс-программ, так и для национальных и наднациональных регуляторов для разработки мер конкурентной и промышленной политики (в частности для общих товарных рынков Союзного государства).

Ключевые слова: ценовые индикаторы, товарный рынок, сделка экономической концентрации, биржа, индекс цен.

Abstract: The study examines methods for forming price indicators in commodity markets under high economic uncertainty, both as a result of sanction pressure and as a result of foreign analytical agencies market exit. Two groups of methods are subject to analysis: in traditional markets – creation of stock indices and off-exchange indicators, in digital markets – antitrust regulation of merger and acquisition. The results of analysis indicate the presence of gaps both in legal framework of economic regulation and in technological mechanisms for price indicators creation. The results of the study may be of interest both for participants in the commodity markets of Russia and Belarus as a direction for compliance programs development, and for national and supranational regulators for the development of competition and industrial policy measures (in particular for the common commodity markets of The Union State of Belarus and Russia).

Keywords: price indicators, commodity market, merger and acquisition, stock exchange, price index.

Введение

В течение 30 лет на постсоветском пространстве вместе с развитием рыночной экономики формировалась новая информационная инфраструктура, сердцевина которой – рыночные цены, без

информации о которых невозможны осмысленные предпринимательские и регуляторные решения. События 2022 года привели к тому, что система ценовых индикаторов, включающая информацию от зарубежных аналитических агентств и котировки зарубежных товарных бирж, применявшаяся регуляторами и компаниями в хозяйственной деятельности и правоприменении, оказалась нарушенной. Как результат – резкий рост неопределенности, в том числе правовой. Проблема «импортозамещения» в получении и интерпретации оценок ценовых индикаторов в разрезе товарных рынков связана с отсутствием систематических, сбалансированных решений в части мониторинга цен, анализа динамики цен в регуляторной практике как отраслевых ведомств, так и антимонопольных органов РФ и РБ.

Методология исследования

В рамках первой части исследования проводится анализ международного опыта формирования биржевых и внебиржевых индикаторов. Выбор индексов цен, подлежащих анализу, обусловлен доступностью информации о методике построения ценовых индикаторов (здесь и далее – термины «индекс цен» и «ценовой индикатор» используются как синонимы) и возможностью применения (с ограничениями или без) данных методик к условиям функционирования рынков на территории РФ и РБ.

Вторая часть исследования содержит анализ НПА в сфере регулирования рынков с платформами, с последующим обсуждением рисков, которые возникают в условиях правовой неопределенности.

В качестве методологии исследования используются подходы новой институциональной экономической теории, теории организации отраслевых рынков, а также экономического анализа права.

Результаты исследования и их обсуждение

Выявлены риски, связанные с практикой биржевой торговли, которая рассматривается регуляторами разных уровней как основной метод *формирования ценовых индикаторов* на территории ЕАЭС. Практика обязательной регистрации внебиржевых сделок сопряжена с ростом трансакционных издержек участников, и ее целесообразность не очевидна [1, 2]. Данный фактор должен быть учтен при разработке стратегии создания международной биржевой системы индикаторов товарных рынков, участие в которой подтвердила Белорусская универсальная товарная биржа.

Сбор и обработка статистической информации о ценах на товары предполагает наличие ответов на следующие группы вопросов:

- 1) Определение группы товаров, цены на которые подлежат мониторингу [3];
- 2) Определение географических границ товарного рынка, где осуществляется мониторинг цен [4];
- 3) Определение уровня рынка (розничный, оптовый) для сбора статистической информации о динамике цены товара;
- 4) Выбор временного интервала для исследования проблемы роста/снижения цен, предполагающего анализ обоснованности ценообразования [5];
- 5) Выбор источников и механизмов для осуществления мониторинга цен на основании уже имеющихся или возможных для создания источников, в том числе сбор информации напрямую от производителей товаров, или сбор информации через существующие ГИСы, включая официальные статистические системы РФ и РБ.

Результаты первой части исследования свидетельствуют о наличии ограничений в возможностях использования международного опыта формирования ценовых индексов в рамках регуляторной практики Союзного государства, что обусловлено наличием недостатков исследуемых методик как с точки зрения метода сбора информации, так и в формульном конструировании индексов.

Кроме того, можно сделать вывод о необходимости расширения пула информации – в дополнение к собираемой ценовой информации, которая подвергается анализу регуляторами разных уровней. Эта необходимость объясняется самой природой цены, которая является результатом взаимодействия спроса и предложения. Таким образом, проведение корректного анализа ценовых

индикаторов невозможно без учета факторов ценообразования.

Антимонопольный контроль сделок экономической концентрации на рынках РФ и РБ реализованы Федеральной антимонопольной службой (ФАС России) и Министерством антимонопольного регулирования и торговли Республики Беларусь (МАРТ РБ) соответственно. В 2022 году между данными ведомствами было подписано Соглашение о единых правилах конкуренции, предполагающее единые стандарты защиты конкуренции на территории Союзного государства. Кроме того, на территории ЕАЭС антимонопольный контроль осуществляет Департамент антимонопольного регулирования Евразийского экономического союза. Стоит отметить тот факт, что практика регулирования цифровых рынков и установления экономической обоснованности цен на рынках с платформами страдает от значительных пробелов в процедуре анализа цифровых рынков во всех вышеперечисленных инстанциях.

В июле 2023 года был принят Федеральный закон от 10.07.2023 № 301-ФЗ «О внесении изменений в Федеральный закон «О защите конкуренции», именуемый пятым антимонопольным пакетом. Цель нововведений в антимонопольное законодательство – совершенствование регулирования цифровых рынков. Среди ключевых положений 301-ФЗ, требующих дополнительной проработки со стороны регулятора и особого внимания со стороны участников цифровых рынков, – понятие сетевых эффектов.

«Сетевой эффект – свойство товарного рынка (товарных рынков), при котором потребительская ценность программы (совокупности программ) для электронных вычислительных машин в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», обеспечивающей совершение сделок между продавцами и покупателями определенных товаров (далее – цифровая платформа), изменяется в зависимости от изменения количества таких продавцов и покупателей».

В соответствии с принятыми поправками в антимонопольное законодательство учет сетевого эффекта является частью процедуры проведения анализа состояния конкуренции на товарных рынках с цифровыми платформами. При этом антимонопольный орган устанавливает наличие сетевых эффектов и определяет наличие возможности у платформы оказывать решающее влияние на условия обращения товара на рынке / устранять других участников рынка / создавать барьеры входа на рынок.

Основной проблемой в реализации данного положения Федерального закона № 301-ФЗ является отсутствие алгоритма оценки сетевого эффекта, что может вести к ошибкам в правоприменении и созданию отрицательных экономических эффектов для участников цифровых рынков.

Экономический смысл сетевого эффекта заключается не в факте его наличия, а в его параметрах:

1) Сетевой эффект может обладать разной интенсивностью. Сила сетевого эффекта в значительной степени зависит от стадии развития рынка – чем более зрелый рынок с точки зрения насыщения спроса, тем сильнее сетевой эффект. Однако зависимость «ценности» платформы для потребителей может иметь разные формы зависимости от количества пользователей платформы – линейную, степенную или показательную. Форма зависимости переменных позволяет определить, насколько быстро растет сетевой эффект и когда он начинает замедляться/снижаться. В зависимости от силы эффекта будет отличаться и возможность платформы оказывать влияние на условия конкуренции на рынке. Учет данного параметра в ходе антимонопольного регулирования рынка необходим для оценки преодолемости барьеров входа на цифровые рынки.

2) По направлению сетевые эффекты делятся на прямые и косвенные. Прямые сетевые эффекты характеризуются ситуацией, когда увеличение степени использования платформы ведет к прямому увеличению ее ценности для пользователей, увеличивая их желание платить за услуги платформы. Такого рода эффекты возникают на платформах мессенджерах, предоставляющих возможность обмена сообщениями между пользователями (чем больше пользователей мессенджера, тем привлекательнее он для аудитории).

Косвенный сетевой эффект возникает тогда, когда одна категория пользователей выигрывает от присоединения к платформе другой категории. Например, агрегатор такси становится более

востребованным для стороны предложения (таксистов), когда обладает большой аудиторией на стороне спроса (пассажирами, подключенными к сервису заказа такси в рамках платформы).

Направление сетевого эффекта определяет структуру цифрового рынка, его границы и емкость – эти параметры являются ключевыми для определения состояния конкуренции на цифровых рынках и последующего вынесения решения о наличии/отсутствии антимонопольных действий компании. В случае игнорирования прямых или косвенных сетевых эффектов возможны ошибки антимонопольного регулирования двух типов – слишком узкое определение границ рынка (в таком случае платформа с высокой вероятностью будет признана доминирующей на рынке и будет подвержена избыточному государственному регулированию), и слишком широкое определение границ рынка (в таком случае в границы рынка войдет значительное число компаний и злоупотребление доминирующим положением, проявляющееся в установлении монополично высоких цен или создании барьеров входа, останется незамеченным).

3) Сетевой эффект может быть как положительным, так и отрицательным. Выше говорилось о положительных сетевых эффектах (новый пользователь увеличивает полезность платформы для других пользователей), однако есть и противоположный тип сетевого эффекта. Отрицательный сетевой эффект – снижение полезности платформы для пользователей в случае присоединения нового участника. Такого рода ситуации возможны в условиях большой загрузки сервера и перегрузки сети. Положительные и отрицательные сетевые эффекты могут уравновешивать друг друга, не позволяя платформе безгранично расширяться. Этот фактор должен учитываться в рамках антимонопольной практики регулирования цифровых рынков при оценке возможности злоупотребления доминирующим положением хозяйствующего субъекта. В противном случае возможна ошибка антимонопольного регулирования, связанная с переоценкой положительных сетевых эффектов и завышением оценок рыночной власти компаний. Такие ошибки влекут за собой дополнительные предписания со стороны ФАС России и штрафные санкции.

Перечисленные выше параметры не находят отражения в пятом антимонопольном пакете, в связи с чем возрастает риск некорректного определения границ цифровых рынков и барьеров входа на рынки с платформами.

Кроме того, новые правила регулирования цифровых рынков не учитывают возможность потребителя использовать сразу несколько сетей одновременно. Это явление именуют множественной адресацией (multihoming). Мультихоуминг пользователя снижает его издержки переключения между платформами и ограничивает их рыночную власть.

Выводы (заключение)

Формирование системы ценовых индикаторов сталкивается с рядом ограничений с точки зрения соблюдения требований комплексности индексов цен и достоверности выводов, полученных на основе анализа их динамики. Проведенный анализ позволяет говорить об отсутствии универсальных индикаторов цен – как в привязке к целям формирования индикатора, так и по методам формульного построения.

Перечисленные проблемы в реализации антимонопольного регулирования цифровых рынков с платформами создают риски для участников рынков с точки зрения несения репутационных и финансовых издержек в случае ошибок правоприменения, одновременно приводя к росту административной нагрузки регулятора. В условиях, когда нормативно-правовая база имеет существенные пробелы, компании-участники рынков вынуждены самостоятельно предпринимать меры, направленные на снижение антимонопольных рисков – в рамках антимонопольного комплаенса. В ситуации правовой неопределенности требуются разъяснения со стороны ФАС России и МАРТ РБ относительно процедуры оценки сетевых эффектов на рынках с цифровыми платформами.

Список литературы

1. Laulajainen R. The geographical reach of a commodity exchange: The London metal exchange and beyond. *Resources Policy*. 1995. no. 21(2). P. 133-141.
2. Zeng Y., Dong C., Hook M., Sun J., Shi D. Can the Shanghai LNG Price Index indicate Chinese market? An econometric investigation using price discovery theory. *Frontiers in Energy*. 2020. no. 4. P. 726-739.
3. Elizalde J. A theoretical approach to market definition analysis. *European Journal of Law and Economics*. 2012. no. 34(3). P. 449-475.
4. Massey P. Market Definition and Market Power in Competition Analysis: Some Practical Issues. *The Economic and Social Review*. 2000.no.4. P. 309-328.
5. Gaynor M., Kleiner S., Vogt W. A structural approach to market definition with an application to the hospital industry. *The Journal of Industrial Economics*. 2013. no. 61(2). P. 243-289.

**ЭФФЕКТИВНАЯ ОРГАНИЗАЦИЯ БУХГАЛТЕРСКОГО УЧЕТА, КАК ОСНОВА
ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ СУБЪЕКТОВ МАЛОГО БИЗНЕСА
ТРАНСПОРТНОГО СЕГМЕНТА**
**EFFECTIVE ORGANIZATION OF ACCOUNTING AS A BASIS FOR ENSURING ECONOMIC
SECURITY OF SMALL BUSINESSES IN THE TRANSPORT SEGMENT**

А.Г. Мельник

Учреждение образования «Белорусский государственный университет пищевых и химических технологий»

Республика Беларусь, 212027, г. Могилев, пр. Шмидта, 3, email: melnik_buaa@mogilev.bgut.by

A.G. Melnik

**Educational Institution «Belarusian State University of Food and Chemical Technologies»
Republic of Belarus, 212027, Mogilev, Schmidt Ave., 3, email: melnik_buaa@mogilev.bgut.by**

Аннотация: В рамках научной проблематики исследования механизмов повышения экономической безопасности и эффективности посредством гармонизации системы бухгалтерского учета выполнен анализ теоретических основ учета использования топлива субъектами малого бизнеса. Выделены ключевые этапы работ по организации и осуществлению учета расхода топлива. Разработан алгоритм отражения в учете топлива, приобретенного за наличный расчет. Даны рекомендации по заполнению книг учета индивидуальными предпринимателями.

Ключевые слова: экономическая безопасность, малый бизнес, нормируемые расходы, учет топлива, средняя цена

Abstract: As part of the scientific problems of studying mechanisms for increasing economic security and efficiency through harmonization of the accounting system, an analysis of the theoretical foundations of accounting for fuel use by small businesses was carried out. The key stages of work on organizing and implementing fuel consumption accounting are highlighted. An algorithm has been developed for recording fuel purchased in cash. Recommendations are given for filling out accounting books by individual entrepreneurs.

Keywords: economic security, small business, standardized expenses, fuel accounting, average price

Введение

При выстраивании системы экономической безопасности субъекта хозяйствования немаловажная роль отводится эффективной организации учета и контроля. Рационально организованная учетно-аналитическая система позволяет получать своевременную достоверную информацию о состоянии субъекта, о достижении плановых (пороговых) значений, характеризующих цель развития, о рисках и угрозах и именно в этом выходной поток учетно-аналитической системы совпадает с определением цели экономической безопасности.

Значительная часть учетной работы субъектов малого бизнеса связана с учетом расходов по предпринимательской деятельности. В соответствии с пунктом 18 статьи 205 Налогового кодекса Республики Беларусь (далее – НК РБ) индивидуальный предприниматель при налогообложении доходов от осуществления предпринимательской деятельности подходным налогом может уменьшить налогооблагаемую базу на определенные расходы, группируемые по элементам [1].

Материал и методы исследования: Методология проведенного исследования основана на системном подходе с использованием таких общенаучных методов как: наблюдение, сравнение, при этом происходит накопление фактов и их описание, далее применяется обобщение и систематизация

данных, их анализ, синтез, логическое исследование собранных фактов, выработка суждений и умозаключений, создаются теоретические обобщения, используются методы системного анализа и устанавливаются границы их применения.

Результаты исследования и их обсуждение: При осуществлении пассажирских перевозок у субъектов малого бизнеса в составе расходов по предпринимательской деятельности значительную долю занимают расходы по списанию топлива, использованного в процессе осуществления предпринимательской деятельности. Данные расходы относятся к элементу «Материальные расходы» (подпункт 21.5 статьи 205 НК РБ).

Условно можно разделить работу по организации и осуществлению учета топлива, использованного в предпринимательской деятельности на три блока (рисунок 1).

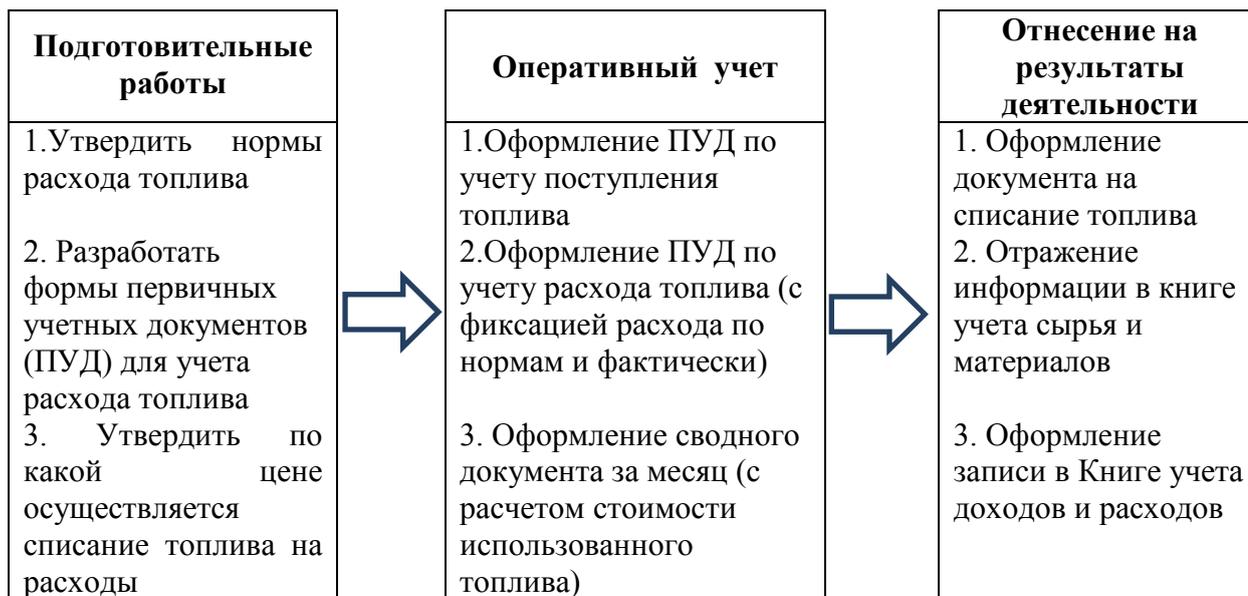


Рисунок – Блок-схема работ по организации и осуществлению учета расхода топлива

Подготовительные работы включают следующие аспекты:

1. Утверждение норм расхода топлива.

В соответствии с подпунктом 1.2 статьи 171 Налогового кодекса Республики Беларусь в состав нормируемых затрат включают стоимость топлива, израсходованного механическими транспортными средствами в пределах норм, установленных руководителем организации самостоятельно или на основании результатов испытаний, проведенных аккредитованной испытательной лабораторией [1].

Не зависимо от того какой вариант выберет индивидуальный предприниматель, необходимо обязательно используемые нормы расхода топлива утвердить решением (приказом).

Право индивидуальных предпринимателей самостоятельно устанавливать нормы расхода топлива для механических транспортных средств предусмотрено постановлением Совета министров №470 от 10.08.2020 г. «О порядке установления норм расхода топлива» [2].

Отметим, что Налоговый кодекс обладает большей юридической силой, чем постановление, поэтому руководствоваться индивидуальным предпринимателям необходимо Налоговым кодексом.

Если индивидуальный предприниматель принимает решение установить нормы расхода топлива самостоятельно, то устанавливаемая норма должна быть экономически обоснованной. Это означает, что необходимо произвести определенные мероприятия по установлению реальной нормы расхода топлива.

Считаем целесообразным при самостоятельном установлении нормы расхода топлива в качестве источников сведений использовать:

- нормативно-правовые акты Министерства транспорта и коммуникаций Республики Беларусь,

содержащие нормы расхода на соответствующие (или аналогичные) механические транспортные средства,

- информацию завода-изготовителя механических транспортных средств о норме расхода, содержащейся в сопроводительных документах (паспортах, руководствах по эксплуатации и др.),
- результаты замеров, проведенных индивидуальным предпринимателем самостоятельно и др.

Если индивидуальный предприниматель принимает решение осуществить замеры расхода топлива, необходимо результаты замеров и расчета нормы расхода оформлять документально.

2. Разработка форм первичных учетных документов для учета расхода топлива.

Форму первичного учетного документа, на основании которого в учете отражается стоимость израсходованного транспортным средством топлива, индивидуальный предприниматель определяет самостоятельно.

Оперативный учет движения топлива в баках автомобилей может осуществляться в любом разработанном и утвержденном к использованию первичном учетном документе. Форма такого документа должна соответствовать требованиям предъявляемым к содержанию первичных учетных документов предусмотренным постановлением Министерства налогов и сборов Республики Беларусь №5 от 30.01.2019 г. "Об утверждении Инструкции о порядке ведения учета доходов и расходов" (далее – Инструкция №5) [3].

Можно использовать для этих целей "Путевой лист". Стоит отметить, что в настоящее время перевозки могут осуществляться без оформления такого транспортного документа, как путевой лист. Те есть индивидуальный предприниматель оформляет путевой лист, если принимает решение о необходимости использования такого документа. Преимущества использования путевого листа в целях оперативного учета:

- наличие документа, являющегося основанием для учета движения топлива.

При разработке формы путевого листа целесообразно предусмотреть наличие (кроме обязательных реквизитов) следующей информации:

- показания спидометра при выезде и возврате с линии,
- пробег за отчетную дату,
- остатки топлива на начало и конец дня,
- количество заправленного топлива, с указанием номера, даты документа подтверждающего заправку (при заправке на автозаправочных станциях – чек),
- расход топлива по путевому листу по норме,
- фактический расход топлива.

Основанием для списания топлива на расходы являются накопительные ведомости данных первичных учетных документов в которых содержится информация о фактическом расходе топлива (в случаях, когда ведется путевой лист).

Необходимо разработать и утвердить форму сводного документа за месяц, в котором будет аккумулироваться информация из путевых листов и прочих первичных учетных документов. Например, это может быть карточка движения топлива, ведомость учета топлива за месяц или др.

Следует отметить, что разработанные формы документов необходимо утвердить к использованию в решении (приказе) индивидуального предпринимателя.

2. Утверждение цены списания топлива в расход.

Кроме того, необходимо решением индивидуального предпринимателя закрепить по какой стоимости списывается топливо в расход:

- по цене фактического приобретения топлива,
- по средней себестоимости,
- по стоимости первой оприходованной партии.

Индивидуальный предприниматель может приобретать топливо:

- самостоятельно,
- через подотчетных лиц (при наличии наемных работников).

Индивидуальный предприниматель вправе приобретать топливо:

- за наличный расчет,
- в безналичном порядке.

При безналичном приобретении топлива и заправке автомобилей по топливным картам не возникает сложностей в учете. В пункте 7.2 Инструкции №5 указано, что к иным документам подтверждающим совершение хозяйственных операций относятся отчеты поставщика по отпуску топлива. Таким образом, отчет поставщика по отпуску топлива за месяц является основанием для отражения приобретенного топлива в учете одновременно, что значительно облегчает учетный процесс.

При приобретении топлива за наличный расчет индивидуальному предпринимателю необходимо учитывать ряд нюансов:

- установлен предельно допустимый размер расчетов наличными денежными средствами с юридическими лицами и индивидуальными предпринимателями в день не более 100 базовых величин (пункт 90 Инструкции о порядке ведения кассовых операций и расчетов наличными денежными средствами №472 (далее – Инструкция №472))[4],

- чек АЗС не является первичным учетным документом и, следовательно, на основании только чека нельзя отразить поступление топлива в учетных регистрах при приобретении топлива (п.7 Инструкции №5),

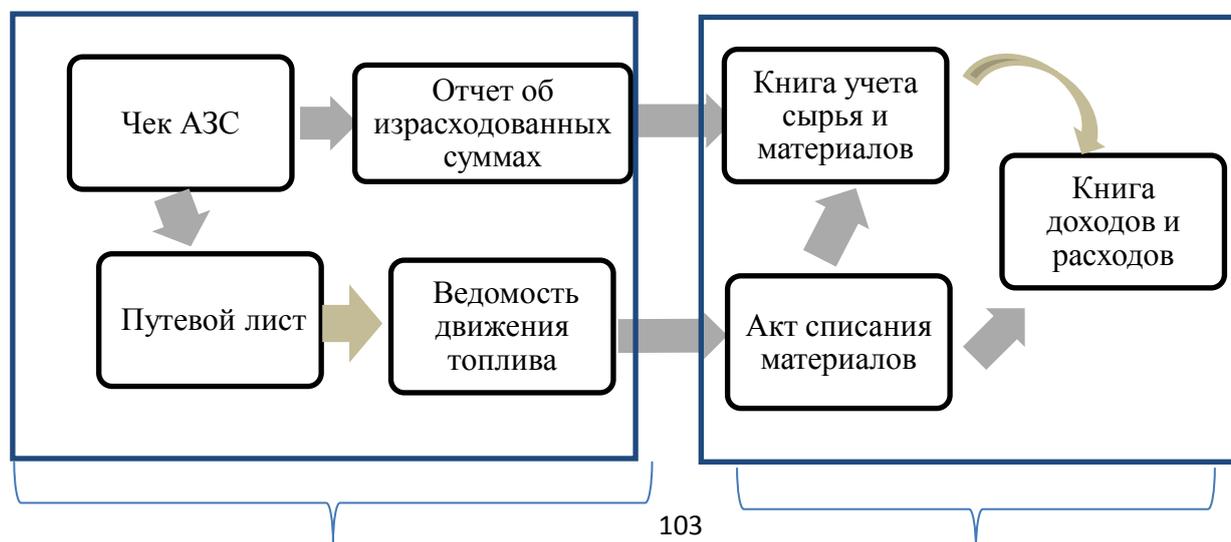
- выдачу наличных денежных средств под отчет на приобретение топлива и возврат неизрасходованных сумм необходимо оформлять документально в соответствии с требованиями главы 3 Инструкции №472,

- необходимо соблюдать сроки использования подотчетных сумм выданных на осуществление текущих операций - не более 10 рабочих дней и составления отчета об израсходованных средствах - не позднее 15 рабочих дней по истечении срока на который выданы денежные средства на текущие нужды (пункты 67 и 82 Инструкции №472).

В случае, когда индивидуальный предприниматель приобретает топливо за наличный расчет самостоятельно, он осуществляет записи в учетные регистры на основании документов, подтверждающих приобретение. Как отмечено выше, чек АЗС не является первичным учетным документом и соответственно не является основанием для отражения поступления топлива в Книге сырья и материалов. Поэтому индивидуальному предпринимателю, приобретающему топливо для использования в предпринимательской деятельности за наличный расчет, необходимо разработать и утвердить форму первичного учетного документа (например, приходный ордер), в котором будет указываться информация о количестве, цене и сумме приобретенного топлива. Такой первичный документ с приложенными чеками АЗС является основанием для принятия к учету приобретенного топлива и отражения приходной операции в Книге учета сырья и материалов.

При поступлении топлива через подотчетных лиц основанием для записи в учетные регистры являются отчеты об израсходованных суммах с приложенными к ним документами, подтверждающими осуществленные расходы по приобретению топлива (пункт 84 Инструкции №472).

На рисунке 2 представлен алгоритм отражения в учете топлива, приобретенного за наличный расчет подотчетным лицом.



Оперативный учет Отнесение на результаты деятельности

Рисунок 2 – Алгоритм отражения в учете топлива, приобретенного за наличный расчет

Информация из отчетов об израсходованных суммах переносится в книгу учета сырья и материалов (рисунок 3). В соответствии с положениями Инструкции № 5 индивидуальный предприниматель может принять решение о не использовании Книги учета сырья и материалов. Однако, тогда необходимо разработать и утвердить форму другого документа, который будет использоваться в качестве учетного регистра по учету сырья и материалов.

Наименование сырья, материалов		Дизельное топливо-К5 (в баке автомобиля VOLKSWAGEN AI 8118-1)								
Дата записи	наименование документа, его номер и дата	Поступило				Оплачено			Изъ	
		единица измерения	цена (руб.)	количество	стоимость (руб.)	наименование документа, его номер и дата	сумма (руб.)	наименование документа		
1	3	4	5	6	7	8		9	10	
01.01.24.	Акт снятия остатков топлива в баках автом.№1 от 31.12.23г.									
15.01.24.	Авансовый отчет Иванова И.И. №4 от 15.01.24.	л.	2,31	30,00	69,30	Чек продажи	87618	12.01.24.	69,30	
		л.	2,31	30,00	69,30	Чек продажи	88199	15.01.24.	69,30	

Рисунок 3 – Пример оформления фрагмента Книги учета сырья и материалов на поступление топлива

Следует отметить, что в целях ведения оперативного учета информация из чеков АЗС должна переноситься в документы, применяемые для оперативного учета. В нашем примере таким документом выступает ежедневный Путевой лист.

Обозначим, что Отчет об израсходованных суммах может быть предоставлен индивидуальному предпринимателю спустя значительное время (до 15 рабочих дней с даты приобретения топлива), поэтому особую актуальность для целей оперативного учета имеет запись информации из чеков АЗС в Путевой лист. Путевой лист сдается индивидуальному предпринимателю подотчетным лицом ежедневно по окончании рейса. Следовательно, у индивидуального предпринимателя будет всегда достоверная информация о приобретении, расходе топлива, остатках топлива в баках механических транспортных средств на каждую отчетную дату.

На рисунке 2 обозначено, что данные путевых листов о поступлении, расходе топлива (фактическом и нормативном), остатках на начало и конец дня переносятся в сводный документ по учету движения топлива. В нашем примере таким сводным документом выступает Ведомость движения топлива, в которой информация о поступлении, расходовании топлива и остатках топлива в баках механических транспортных средств накапливается в течение месяца. По окончании месяца на основании данных Ведомости движения топлива появляется возможность расчета средней цены топлива, которая будет использована для списания топлива на расходы по предпринимательской деятельности. Расчет средней цены осуществляется по формуле (1).

$$\bar{Ц} = \frac{(O_H^C + П^C)}{(O_H^K + П^K)} \quad (1)$$

где: O_H^C , O_H^K – остатки топлива в баках на начало месяца в стоимостном и натуральном измерении соответственно;

$П^C$, $П^K$ – поступление топлива в течение месяца в стоимостном и натуральном измерении соответственно.

Рекомендуем определиться с количеством знаков после запятой в средней цене топлива и зафиксировать эту информацию решением индивидуального предпринимателя.

Для отнесения на расходы топлива, использованного за отчетный месяц, необходимо оформить

документ на списание, на последнюю дату отчетного месяца, например, Акт на списание материалов. Считаю целесообразным разработать и утвердить решением индивидуального предпринимателя одну форму акта для списания любого вида сырья и материалов.

После оформления Акта на списание материалов необходимо отразить результаты списания в Книге учета сырья и материалов (рисунок 4).

Группа (руб.)	Израсходовано на производство товаров, выполнение работ, оказание услуг					Выбыло по прочим основаниям, не связанным с производством товаров, выполнением работ, оказанием услуг					Остаток			
	наименование документа, его номер и дата	единица измерения	цена (руб.)	количество	стоимость (руб.)	наименование документа, его номер и дата	единица измерения	цена (руб.)	количество	стоимость (руб.)	единица измерения	цена (руб.)	количество	стоимость (руб.)
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
	Акт списания материалов №2г от 29.02.24.	л.	2,3230	520,00	1207,94						л.		28,00	72,80

Рисунок 4 – Пример оформления фрагмента Книги учета сырья и материалов по списанию использованного топлива

Далее информация о списании топлива переносится в Книгу доходов и расходов. Инструкцией №5 не предусмотрено переноса данных из Книги учета сырья и материалов сразу в Книгу учета доходов и расходов. Поэтому индивидуальный предприниматель может использовать иные документы для отражения списания топлива на расходы, предварительно утвердив своим решением такой документ и порядок переноса данных .

Наиболее действенным средством по обеспечению экономической безопасности любого субъекта хозяйствования выступает инвентаризация. Для индивидуальных предпринимателей нет законодательно установленной обязанности проведения инвентаризации имущества. Однако, считаем, что без снятия остатков топлива в баках механических транспортных средств достоверность учетных данных об остатках и фактическом расходе будет под вопросом. В связи с этим рекомендуем разработать форму акта о снятии остатков топлива и оформлять его ежемесячно либо ежеквартально. Это позволит во-первых подтверждать достоверность учетной информации, и во-вторых за счет систематического внутреннего контроля основного элемента затрат для субъекта осуществляющего транспортные услуги обеспечивать его экономическую безопасность.

Список литературы

1. Налоговый кодекс Республики Беларусь // Консультант Плюс: Беларусь [Электрон.ресурс] / ООО "ЮрСпектр", Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024
2. О порядке установления норм расхода топлива, утв. пост. Совета министров Респ. Беларусь, 10.08.2020г. № 470 // Консультант Плюс: Беларусь [Электрон.ресурс] / ООО "ЮрСпектр", Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024
3. Инструкция о порядке ведения учета доходов и расходов, утв. пост. М-ва налогов и сборов Респ. Беларусь, 30.01.2019г. № 5 (в редакции постановления №11 от 29.0.24г.) // Консультант Плюс: Беларусь [Электрон.ресурс] / ООО "ЮрСпектр", Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024
4. Инструкция о порядках ведения кассовых операций и расчетов наличными денежными средствами, утв. Пост. Нац. банка Респ. Беларусь, 20.12.23г. №472 // Консультант Плюс: Беларусь [Электрон.ресурс] / ООО "ЮрСпектр", Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024

УДК 331.1; 331.55

ЗАНЯТОСТЬ В РЕАЛИЗАЦИИ ЦИФРОВЫХ ИНИЦИАТИВ EMPLOYMENT IN THE IMPLEMENTATION OF DIGITAL INITIATIVES

Миренкова И.В.

УО «Белорусская государственная сельскохозяйственная академия», Республика Беларусь,
213410, г.Горки, ул. Мичурина, 5, email: mirenkova@tut.by

Mirenkova I.V.

Belarusian State Agricultural Academy, Republic of Belarus,
213410, Gorki, Michurina str., 5, email: mirenkova@tut.by

Аннотация. Современный формат занятости в следствие активизации материально-технической базы, внедрении цифровых технологий в управленческие и производственные процессы, обусловило выработку новых подходов формирования рабочего места трудовых ресурсов, особенно в сельскохозяйственном производстве.

Ключевые слова: рабочее место, трудовые ресурсы, эффективная занятость.

Abstract. The modern employment format, due to the activation of the material and technical base, the introduction of digital technologies into management and production processes, has led to the development of new approaches to the formation of the workplace of labor resources, especially in agricultural production.

Keywords: job, agricultural production, labor resources, effective employment.

Введение

Организация рабочего места является основным звеном в системе управления трудовыми ресурсами сельхозорганизации. На основе внедрения инноваций как в области управления, так и производства изменяется оснащенность рабочих мест и их характеристики по интенсивности, уровню механизации, управлению, стоимости, коммутативным связям, длительности функционирования, требуемой квалификации, уровне оплаты труда, интенсивности труда, интеграции и кооперации и т. д.

Цель исследования

Рассмотрение воспроизводства рабочего места и трудового процесса в рабочей среде позволяет констатировать, что трудовые ресурсы являются важным элементом, определяющим функционирование рабочего места в процессе производства, а капитал и земля его материальной основой.

Данный подход указывает на необходимость изучения рабочего места, в комплексном сочетании его признаков, как основного звена обеспечивающего эффективную занятость и формирующего требования к определенному уровню соответствующих знаний и умений работников в современном сельскохозяйственном производстве.

Материал и методы исследования

Материалами для исследования выступили научные работы отечественных и зарубежных экономистов.

В процессе написания работы использовались методы теоретического исследования: системный, обобщения, сравнения и другие.

Результаты исследования и их обсуждение

Изучая характеристики рабочих мест [2], которые позволяют учесть, как можно больше факторов, позволяющих установить их влияние на эффективную занятость была разработана следующая классификация рабочих мест в сельском хозяйстве по технологическим параметрам:

- по отраслям производства: растениеводство, животноводство;
- по выполняемым функциям (категориям персонала): руководителя, специалиста, рабочих, других служащих;
- по отношению к создаваемому продукту: основное, вспомогательное, обслуживающее;
- по техническому уровню: ручные, механизированные, автоматизированные.
- по кооперированности: простое, многоагрегатное;
- по количеству исполнителей: индивидуальное, коллективное (бригадные);
- по степени использования в производственном процессе: функционирующие, не функционирующие;
- по времени использования: постоянные, временные (сезонные);
- по виду трудовых процессов: постоянные стационарные, постоянные условно-стационарные, временные с периодическим перемещением, временные с непрерывным перемещением;
- по числу смен: односменные, многосменные;
- по условиям труда: с нормальными условиями, с тяжелыми физическими условиями, с вредными условиями, с монотонным трудом.

При оценке рабочего места в сельском хозяйстве на основе приведенной классификации следует учитывать следующие характеристики:

- в растениеводстве рабочее место определено оборудованием, с помощью которого осуществляется трудовой процесс (место посевной, кабина комбайна), в животноводстве – это зона помещения, где находятся животные и оборудование, с помощью которых совершается трудовой процесс исполнителем;

- в связи с особенностями сельхозпроизводства, преобладают временные места, существующие только в период выполнения определенных работ (обработка почв, посев, уход за посевами, сбор урожая);

- постоянные рабочие места, не меняют свое расположение в пространстве и характерны для животноводческой отрасли (работника свиноводства, кормоцехов), ремонтных мастерских, подсобных предприятий (работника мельниц) и подразделяющиеся на постоянные стационарные (исполнитель осуществляет трудовые действия в ограниченном пространстве (оператор кормоцеха) и на постоянные условно-стационарные (характерна значительная пространственная протяженность (животноводы)). Временные (мобильные) рабочие места, определяющиеся перемещением исполнителей и средств, а также предметов труда характерны растениеводческой отрасли, транспорт, некоторым подразделениям животноводства, которые делятся на временные с периодическим перемещением (доочистка свеклы) и на временные с непрерывным перемещением (все механизированные работы, транспортные);

- на рабочих местах ручной работы выполнение трудовых процессов осуществляется ручными орудиями труда (прополочные работы, уход за животными), на механизированных – машин и механизмом, устройств для полного или частичного освобождения работника от выполняемой работы (технология машинного доения; на автоматизированных – машин и аппаратов выполняемых определенные технологические операции по заданным параметрам управляемым исполнительным (переработка продукции);

- отсутствие четких границ между рабочими местами при коллективном выполнении работ (на одном поле сбор продукции и сортировка, поточные посевные, уборочные работы);

- рабочие места занятых в основном производстве (животноводство, растениеводство), работников вспомогательных производств (автомобильный транспорт), обслуживающих производств;

- критерием отнесения рабочего места к функционирующему является закрепление за ним плана производства продукции, а при его отсутствии оно относится к не функционирующему (вакантному - отсутствие постоянно закрепленных работников, излишнему - не используется в течение ряда лет и не планируется в дальнейшем, резервному - нет постоянно закрепленного работника, но сохраняется на случай внеплановых работ).

Оцифровка в аграрной сфере (включая интернет, мобильные технологии и устройства, анализ

данных, искусственный интеллект, цифровые сервисы и приложения) меняют сельское хозяйство и продовольственную систему в целом: автоматизация сельскохозяйственной техники позволяет точно настраивать ресурсы и снижает потребность в ручном труде; удаленные спутниковые данные и датчики на месте повышают точность и снижают затраты на мониторинг роста урожая и качества земли или воды, а технологии отслеживания и цифровые логистические услуги открывают потенциал для оптимизации поставок агропродовольственных товаров, одновременно предоставляя потребителям достоверную информацию.

Как отмечает Томашевский К.Л.[3] «...цифровизация привела к появлению такой нетипичной занятости, как работа на основе интернет - платформ. Возник специальный термин «работник платформы», используемый для обозначения тех физических лиц, которые предлагают свой труд на интернет-платформе. Ведутся научные дискуссии как о статусе тех, кто работает посредством онлайн-платформы, так и том, могут ли сами интернет-платформы рассматриваться в качестве работодателей».

Это позволяет расширить классификацию, выделив отдельно цифровое рабочее место. Цифровое рабочее место (digitalworkplace) – это платформа, позволяющая работать и выполнять поставленные задачи, находясь за пределами рабочей среды.

Цифровая платформа — система средств, поддерживающая использование цифровых процессов, ресурсов и сервисов значительным количеством субъектов цифровой экосистемы и обеспечивающая возможность их бесшовного взаимодействия[4].

Цифровизация ускоряет передвижение материальных продуктов по цепочке образования стоимости, совершенствует интеграционные и кооперационные связи с учетом возможностей получения дополнительных эффектов на основе точности исполнения технологических регламентов, повышает эксплуатационные характеристики технических средств, обеспечивает информационное обеспечение управленческих решений. Такой подход модернизации рабочих мест неизбежно будет приводить к сокращению времени на производство продукта, что в свою очередь отразится на численности занятости и требованиям к их знаниям, умениям, компетенциям, будет привлекать более квалифицированный труд, что приведет к росту уровня заработной платы. При этом возникает тенденция сокращения количества занятых.

Доходность рабочего места является главным условием роста эффективной занятости и зависит от следующих параметров:

- технологией производства и требуемой квалификации по ее обслуживанию;
- уровнем трудоемкости выполняемых технологических операций или заданий;
- нормативами нагрузки на единицу рабочего места;
- выбора оплаты труда и стимулирования.
- организацией труда и его производительностью.

Для сельского хозяйства характерен низкий уровень заработной платы и наличие большого удельного веса низкооплачиваемых рабочих мест, что приводит к дефициту рабочей силы на работах с низким уровнем механизации.

Цифровизация ускоряет передвижение материальных продуктов по цепочке образования стоимости, что способствует рациональности использования рабочего времени и созданию эффективной занятости.

Создание цифровых рабочих мест – это объединение оборудования, транспортных средств, передаточных устройств и других элементов технологии в единое информационное пространство, что позволяет часть функционала работника при достижении результата возложить на оборудование, применять дистанционное управления, усилить контроль над рабочим процессом.

В Республике Беларусь в программе социально-экономическое развитие Республики Беларусь на 2021-2025 годы предусматривается в главе «Цифровая трансформация» довести долю сектора информационно-коммуникационных технологий в ВВП – не менее 7,5% в 2025 году. Цифровая трансформация экономики предполагает организацию цифровой информационной среды путем формирования нормативной правовой базы и внедрения действенных инструментов управления процессами цифровизации экономики.[1]

Выводы (заключение)

Таким образом, рост эффективной занятости за счет увеличения машинного времени в процессе производства, при цифровизации технологического процесса является фактором уменьшения предложения на рынке труда и изменения профессиональных требований к исполнителям. Реализация цифровых инициатив, процесс, который неизбежно охватит все сферы сельскохозяйственного труда и поэтому требует, прежде всего, реализации проектов за счет государства и проработки рисков занятости с поиском возможностей создания дополнительных высокооплачиваемых рабочих мест.

Список литературы:

1. Указ Президента Республики Беларусь 29.06.2021 №29 Об утверждении Программы социально-экономического развития Республики Беларусь на 2021-2025 годы [Электронный ресурс].- Режим доступа: <https://pravo.by/document/?guid=3871&p0=P32100292>.- Дата доступа: 05.02.2022.
2. Организация, нормирование и оплата труда в агропромышленном комплексе, Учебное пособие, Жудро М.К., Шапиро С.Б., 2012
3. Томашевский К.Л.. Цифровизация и ее влияние на рынок труда и трудовые отношения (теоретический и сравнительно-правовой аспекты) /К.Л. Томашевский // Вестник СПбГУ. Право. – 2020. – Т. 11. Вып. 2– с.398–413.
4. Цифровое рабочее место [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Цифровое_рабочее_место. – Дата доступа: 15.11.2021.

**РИСК-МОНИТОРИНГ РЕАЛИЗАЦИИ СТРАТЕГИИ РОСТА
TENDENCIES OF FORMATION OF THE MECHANISM OF IMPLEMENTATION OF RISK
STRATEGY**

А.А. Миренков, кан. экон. наук, доцент

Учреждение образования «Белорусский государственный университет пищевых и химических технологий»

Республика Беларусь, 212027, г. Могилев, пр. Шмидта, 3

Anatoly Mirenkov

Educational Institution «Belarusian State University of Food and Chemical Technologies»

Republic of Belarus, 212027, Mogilev, Schmidt Ave., 3

Аннотация: в статье рассматриваются тенденции формирования риск-стратегии при активизации конструктивных функций управления рисками на основе использования системного подхода, позволяющего управлению рисками осуществлять корректирующие и предупреждающие действия в рамках системы управления рисками для достижения целевых показателей.

Ключевые слова: риск, рискованная ситуация, система рисков, стратегия управления рисками, механизм управления, процедуры, методы.

Summary: the article deals with the trends of risk strategy formation in the activation of constructive risk functions based on the use of a systematic approach that allows risk management to carry out corrective and preventive actions within the risk system to achieve targets.

Key words: risk, risk situation, risk system, risk strategy, management mechanism, procedures, methods.

Введение.

В экономическом развитии любого бизнеса на каждом этапе его функционирования формируются стратегии, которые обеспечивают достижение целевых параметров, обеспечивающих выход на максимальные уровни освоения отраслевых технологий при наилучшем финансовом результате.

Достижение целей стратегического роста в условиях все возрастающей конкуренции при увеличении числа производителей и постоянном изменении цен на продукцию и сырье, что требует от субъектов бизнеса учитывать неблагоприятные случайностей и обосновывать выбор оптимальных управленческих решений принятие рисков.

Белорусский ученый Л.Ф. Догиль указывает на то, что «решения и действия в условиях риска эффективны, если позволяют приблизиться к цели» [1, с.30]. В этой связи риск-мониторинг на всех этапах принятия управленческих решений должен быть нацелен на достижении минимального отклонения от целевых параметров и поиск путей выхода из неблагоприятных риск – ситуаций.

Риски– это системное явление, объективно существующие в динамически развивающихся структурах аграрного производства, сформированное через факторы деструктивного и конструктивного взаимодействия в условиях частичной или полной неопределенности с учетом особенного и специфического их представления в информационных потоках и качеству их интерпретации управляющей структурой [2, с.123]. При достижении намеченных целей идентификация и оценка потенциально возможных исходов является инструментарием контрольно-аналитических функций управления.

Изменение стратегических задач и возможностей управляющей системы основывается на таких действиях как их избежание, удержание, передача или снижению степени влияния. Процесс координации этих действий в соответствии с целями управляющей системы может быть реализован

на основе разработки систем и процедур риск-стратегии, частью которой является риск-мониторинг, отслеживающий динамические изменения целевых параметров экономического роста.

Основная часть. Риск-мониторинг, как элемент действий управляющей системы является упорядоченной системой контроля развития ситуации для адекватного реагирования на отклонения показателей, которые могут привести к изменению траектории роста. Оценка степени возможного проявления рисков в экономических системах позволяет учитывать имеющиеся в распоряжении руководства фактах, отражающих выявленные проблемы и зарезервировать вариант решения в соответствии с диапазоном возможных изменений риск-ситуаций в пределах выбранной риск-стратегии. Объективную основу управления риск-ситуациями составляет сочетание факторов в системе, направления их изменения и вероятность проявления. В зависимости от выявленных отклонений целевых параметров, рассматривается необходимость адекватной интерпретации всей информации менеджментом для выбора управленческих решений изменения ситуации в пределах траектории роста. Мониторинг рисков является важнейшим инструментом, позволяющим руководству регулировать возникающие проблемы на основе плана, чтобы избежать провалов в работе. Соответственно риск –мониторинг будет нацелен на выполнение трех основных задач - контролировать, информировать и корректировать. Важное значение в решении этих задач является этап идентификации риск-ситуации от которого зависит своевременность и качество корректирующих действий.

Цель идентификации и анализа риска состоит в выявлении возникающей проблемы и оценке потенциальных возможностей выигрыша или проигрыша при выборе вариантов принимаемых решений исходя из возможного сочетания риск-факторов. Обобщение теоретических исследований с учетом реализации возможностей управления риск-стратегией позволяет предложить методику идентификации и анализа внутриотраслевых рисков, которая включает несколько этапов и согласовывается с уровнями управления, целевыми установками каждой структурной единицы изучаемой системы как в целом, так и по структурным элементам.

Таблица 1.1. – Методические аспекты идентификации и анализа рисков

Этап	Характеристика вариантов	Возможности
Определение цели развития системы или подсистем	Выбор целевого показателя: отраслевой доход, прибыль, валовая продукция и т.д.	Управление стратегией и разработка механизма ее реализации
Систематизация риск-факторов	Проводится исходя из выбранного целевого показателя (по уровню затрат, объему производства, прибыли и т.д.)	Определяет взаимосвязи и взаимозависимости
Структуризация риск-факторов и результатов по объектам управления	Распределяются риск-факторы по стадиям процесса воспроизводства (заготовительно - накопительная; производственно-технологическая; распределительно-реализационная)	Распределение вероятности потерь или выигрыша при проявлении риска изменения целевого показателя
Оценка управляемости	Регулируемые, слабо регулируемые, частично-регулируемые.	Выбор методов разрешения риск-ситуации

Примечание –Разработано автором на основе собственных исследований

Данный подход позволяет на основе выбранных классификаций и применения в комплексе алгоритмов и инструментария анализа и идентификации риск-факторов своевременно выявлять возможности разрешения риск-ситуации.

Корректирующие действия – это меры воздействия на факторы риск-системы, отражающее допустимый уровень риска при приведении ее в состояние при котором сохраняются возможности достижения поставленных целей. Для менеджера необходимо знать какие факторы и в каком

направлении могут быть изменены на основе выбора из возможных альтернативных комбинаций. Это возможно при соединении объективных знаний о системе риска-ситуации, ее структуре, динамике и темпах изменения. Выбор управленческого решения зависит от типа риск-ситуации и возможности ее корректировки или адаптации относительно потенциальных возможностей и производственного потенциала. Риск-ситуации подразделяются на управляемые и неуправляемые. Прогнозирующие решения по изменению риск-ситуации всегда основывается на специальном исследовании, которое дает возможность обосновать развитие риск-стратегии. Полноценное исследование всегда связано с информацией и ее асимметричность во многих случаях может быть оценена тем или иным методом на основе опыта и знаний представителей управляющей системы. Соответственно их ошибки также переходят в риски принятия неверных управленческих решений. Следует рассматривать «риск-систему» - как экономическую категорию, которая формируется на основе риск-ситуации объективно возникающей проблемы и структуры управления, обеспечивающей ее анализ и разрешение.

Поэтому при системном подходе и интегральной оценки рисков, в сложившейся экономической среде важно планомерно проводить мониторинг устойчивости систем, которые могут быть – оптимистическими (отлаженными), маргинальными (приграничными), адаптивными (приспосабливаемыми), пессимистическими. Для каждого типа устойчивости системы в соответствии с отраслевыми особенностями бизнес-единицы должна разрабатываться модели риск-стратегии с учетом целевых установок и диапазона их возможностей по преодолению выявленных несоответствий.

Таблица . – Изменение риск-факторов и уровень их регулирования

Риск-фактор	Тип риск-ситуации
Отсутствие или недостаток материальных производственных ресурсов	частично регулируемые
Природно-климатические	слабо регулируемые
Отсутствие или недостаток технологического оборудования	регулируемые
Недостаток трудовых ресурсов	регулируемые
Нарушение технологического регламента (организация производства)	частично регулируемые
Рост внутреннего потребления продукции	регулируемые
Невостребованность продукции	частично регулируемые
Совместное влияние факторов	частично регулируемые

Примечание – Составлено автором на основании собственных исследований

Идентификации рисков по уровню регулировки риск-ситуации дает возможность объединить различные этапы изучения проблем в единый процесс. Комплексность идентификации отраслевых рисков способствует организации управленческой деятельности по реализации риск-стратегии.

Для идентификации рисков с учетом особенностей организации аграрного производства необходимо, как нам видится, их форматирование проводить по циклам (стадиям) воспроизводства, к которым следует отнести заготовительно-накопительную, производственно-технологическую, распределительно-реализационную стадии, финансово-результативный и управляющий блок

Объединение управляющей системой вышеперечисленных стадий отражает не только определенный этап кругооборота капитала, но и взаимосвязь системы факторов, выделенных на предыдущем уровне исследования.

Заготовительно-накопительная стадия формирования производственных запасов и их хранения характеризует этап снабжения технологического процесса и связана как с рисками оптимальности наличия производственных запасов, так и уровнем затрат при их хранении. На стадии управления заготовительным процессом решаются две взаимодополняющие задачи – поиск возможностей снижения затрат на хранение материальных ресурсов и обеспечение непрерывности производственного процесса. При этом основной риск, который может нарушить функционирование системы в пределах плановых показателей, – это отсутствие сырья и материалов в достаточном объеме и в сроки, предусмотренные технологическим регламентом.

Имеется три основных причины возникновения риск-ситуации на данной стадии:

- отсутствие финансовых ресурсов у самой организации по причине нерационального использования денежных средств или недополученные их из-за низкой окупаемости затрат в предыдущем периоде;
- недостаток на рынке предложений материальных ресурсов и услуг в объеме и качестве, требуемом для организации технологического процесса;
- отсутствие необходимой реакции на ситуацию менеджмента.

Производственно-технологическая стадия кругооборота средств обеспечивается применением разработанных технологий, соединяющих в процесс функции использования основных средств, сырья и материалов, труда и биологических активов. На данной стадии кругооборота средств формируются затраты. Проявление рисков связаны с увеличением затрат как по причине ошибок или стечения неблагоприятных ситуаций на предыдущей стадии (заготовительно-накопительной), так и сбоя определенных функций в технологическом процессе, в том числе и за счет лимитирующих факторов внешнего воздействия природно-климатических условий, организации работ и эффективности использования трудового капитала. На данной стадии в наибольшей степени возможны и необходимы в ряде случаев корректирующие действия менеджмента по реагированию на риск-ситуации для обеспечения общей стратегической цели.

Распределительно-реализационная стадия кругооборота средств характеризуется итоговым результатом отчетного периода как продукцией, так и ее распределением по каналам использования. Риски, формируемые на этой стадии, связаны как с качественными параметрами полученной и прошедшей производственно-функциональную стадию продукции, ее справедливой стоимостью, так и востребованностью данного вида товара как на рынках, так и внутривладельческом потреблении.

Идентификация рисков по степени их концентрации и проявлению на данном этапе связана с внутренними и внешними факторами. Структуризация локальных управляемых риск-систем по циклам воспроизводства в растениеводстве позволят конкретизировать причины формирования риск-ситуации и возможные направления их корректировки по факторам и взаимосвязанным с ними показателям.

Важность данного уровня исследования определяется не только набором выявленных факторов, которые влияют на вариацию дохода в отрасли, но и определяют организацию управления процессами. Это позволит делегировать полномочия при формировании риск-стратегии конкретным исполнителям, закрепив за ними определенные направления ее реализации. Идентификация концентрации проблем по циклам производства основана на том, что риск имеет вероятностный характер. По мнению А. П. Альгина [9], риск имеет три главных компонента: вероятность получения желаемого результата; вероятность наступления нежелательных последствий (неудачи) в ходе выбора альтернативы и ее реализации; вероятность отклонения от выбранной цели. В аграрном производстве изменение риск-факторов на каждом производственном цикле может проходить с различной степенью вероятности и даже в противоположных направлениях. Поэтому оценка вероятности проявления риска в анализируемых подсистемах является важной задачей менеджмента. От того, насколько достоверно будет оценена ситуация на перспективу, будет зависеть подготовленность системы к корректировке процессов для обеспечения ее устойчивости достижения цели. Каждая из выделенных риск-систем имеет определенное сочетание и специфику проявления факторов и вероятности их проявления, формируя общую величину риска, которую можно представить как функцию изменения всех риск факторов по системным моделям различных уровней, формирующих доходность отрасли растениеводства. При этом параметры интерпретируются управляющей системой в соответствии с целями и объектами изучения. Каждая риск-ситуация задействует систему факторов разного уровня соподчиненности. Изучение возможных сценариев событий для выбора управленческого решения необходимо основывать на значимости того или иного риска в системе с учетом изменчивости всех их связей при реализации функций. Из-за того, что нельзя учесть изменчивость всех без исключения факторов, необходимо выделять основные проблемные зоны на разных стадиях управления.

Идентификация рисков управляющей системой по циклам воспроизводства в растениеводстве

необходима для оценки внутренних предпосылок, которые отражают процессы возможных причин с описанием состава показателей по факторам и результатам и которые представлены в таблице 2.18.

Таблица 2 . – Структуризация причин и показателей рисков по циклам воспроизводства в растениеводстве

Циклы воспроизводства (стадии)	Причина риска	Риск-система	Возможные изменения показателей	
			факторов	результатов
Заготовительная-накопительная	1. Недостаточное количество посевного материала, удобрений, ядохимикатов, топлива и т. д. 2. Незапланированное повышение их стоимости	Элементы и статьи материальных производственных затрат	Объем ресурсов, цена, структура	Снижение площади посева, уменьшение объема производства, рост затрат на гектар посева, снижение урожайности
Производственно-технологическая	1. Природно-климатические; 2. Отсутствие или недостаток технологического оборудования; 3. Недостаток трудовых ресурсов; 4. Нарушение технологического регламента	Затраты – объем производства	Биологической урожайности, фактической урожайности, гибель посевов, потери продукции за счет растягивания сроков уборки	Рост затрат на гектар посева, уменьшение объема производства и реализации, снижение качества продукции
Распределительно-реализационная	1. Рост внутреннего потребления продукции; 2. Невостребованность продукции; 3. Изменение цен реализации.	Объем реализации – прибыль	Объем реализации, выручка от реализации, структура реализации	Прибыль

Примечание – Составлено автором на основании собственных исследований

Управляющая система на данном этапе должна уметь реагировать на изменение риск-ситуации и устранять выявленные проблемы или изменять траекторию их изменения в положительном направлении. На этой стадии идентификации риска важно понимание проблем персоналом. Поэтому предварительный этап идентификации концентрации рисков по циклам производства следует проводить с использованием методов экспертной оценки. Этот метод формируется из опыта и понимания проблем менеджмента разного уровня. Алгоритм метода состоит в разработке анкеты, отборе специалистов-экспертов (директора, агрономы, начальники участков, инженеры); опросе и обработке ответов. Для анкетирования предложено оценивать опасность по циклу воспроизводства с использованием десятибалльной шкалы. По результатам анкетного опроса проводится ранжирование рисков по среднему баллу, выставленному респондентами, по каждой причине возможного риска.

Таким образом, установлено, что мониторинг рисков , при их комплексной оценке на различных стадиях достижения стратегии роста позволяет: а) выбирать направления поиска регулировки ситуации риска при разработке риск-стратегии; б) устанавливать сочетание факторов в зависимости от времени выявления проблемы и ее решаемости в определенном периоде; в) принимать

стратегические и тактические управленческие решения на научной основе. Это будет способствовать противостоянию неблагоприятному развитию ситуации или ориентировке на успех при рационализации производственного процесса в пределах безопасного уровня изменения системы риск-факторов.

Список использованных источников:

1. Догиль, Л. Ф. Управление рисками и страхование в бизнесе / Л. Ф. Догиль. – Минск: Мисанта, 2014. – 321 с.
2. Миренков, А. А. Механизм реализации риск-стратегии в аграрных организациях / А. А. Миренков // Вест. Бел.гос. с.-х. акад. – 2016. – № 2. – С. 17–20.

УДК 004.056

**МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ:
ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ**
**INTERNATIONAL COOPERATION IN THE FIELD OF CYBERSECURITY: PROBLEMS AND
PROSPECTS**

В.А. Потеряев

**Ростовский институт (филиал) Всероссийского государственного университета юстиции (РПА
Минюста России), Ростов-на-Дону, e-mail: vadim.poteryayev@bk.ru**

V.A. Poteryayev

**Rostov Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of
Russia), Rostov-on-Don, e-mail: vadim.poteryayev@bk.ru**

Аннотация: В данной статье рассматривается актуальная проблематика международного сотрудничества в сфере кибербезопасности. Был проведен анализ основных факторов, влияющих на развитие данной области, а также были выдвинуты стратегии для улучшения уровня сотрудничества между различными странами. Также был проведен анализ Доктрины информационной безопасности Российской Федерации. Было приведено в пример участие Японии в различных переговорах и встречах, а также существующие соглашения по информационной безопасности, негосударственный вклад Японии и России в эту область, играющий существенную роль в защите информационных ресурсов и данных.

Ключевые слова: международное сотрудничество, кибербезопасность, Интернет, киберугрозы, информационная безопасность, защита данных, сети.

Abstract: This article discusses the topical issues of international cooperation in the field of cybersecurity. The analysis of the main factors influencing the development of this area was carried out, and strategies were put forward to improve the level of cooperation between different countries. An analysis of the Information Security Doctrine of the Russian Federation was also carried out. The example was given of Japan's participation in various negotiations and meetings, as well as existing agreements on information security, the non-governmental contribution of Japan and Russia in this area, which plays a significant role in protecting information resources and data.

Keywords: international cooperation, cybersecurity, Internet, cyber threats, information security, data protection, networks.

Введение

Защита информационной безопасности имеет ключевое значение в современном цифровом мире, поскольку рост технологий приносит определенные угрозы, особенно в виде кибератак. Борьба с киберпреступностью требует комплексного подхода, способного как предотвратить, так и смягчить последствия таких инцидентов. Реакция на угрозу должна происходить не только со стороны частного сектора и государства, но и через партнерство между ними. Сотрудничество в области кибербезопасности между странами, разработка передовых технологий, увеличение осведомленности пользователей – все это должно стать приоритетным направлением в данной сфере. Россия, а также страны Запада и Азии имеют разные подходы к терминологии в данной области, что отражает их особенности и понимание проблемы[1].

Материалы и методы исследования

Методологической основой написания научной статьи выступает: изучение научных публикаций, статей, книг и докладов по теме международного сотрудничества в области кибербезопасности, анализ существующих исследований и выводы предыдущих авторов; анализ конкретных случаев сотрудничества между различными странами или международными

организациями в области кибербезопасности, выявление успешных и неудачных практик; изучение официальных документов, регулятивных актов, стратегий и планов по сотрудничеству в области кибербезопасности между различными странами и международными организациями.

Результаты и их обсуждение

Кибербезопасность – это комплекс мероприятий, направленный на защиту информационных систем, электронных данных и сетей от несанкционированного доступа, несанкционированного использования, изменения или уничтожения[2]. Основная цель кибербезопасности заключается в обеспечении конфиденциальности, целостности и доступности информации в условиях воздействия компьютерных угроз. Кибербезопасность включает различные меры, включая шифрование данных, использование антивирусного программного обеспечения, контроль доступа к ресурсам, обучение сотрудников и многое другое.

Кибербезопасность является необходимым условием развития информационного общества. Ее можно определить, как набор стратегий и действий, необходимых для защиты соединенных сетей от несанкционированного доступа, кражи, разрушения и других злоумышленных действий. Важно обеспечить непрерывное качество безопасности, сохраняя доступность, целостность и конфиденциальность для авторизованных пользователей.

Необходимость обсуждения данной темы была подчеркнута присутствием председателя правительства Российской Федерации Д.А. Медведева на церемонии открытия Всемирной конференции. Он отметил, что количество пользователей интернета в российском сегменте увеличилось до 80 миллионов человек, что составляет более половины населения страны. Интернет-экономика России оценивается примерно в 3% валового внутреннего продукта. Многие российские IT-компании активно развиваются и успешно выходят на международные рынки, предоставляя различные услуги, включая государственные.

Проблемы кибербезопасности постоянно обновляются и модифицируются, требуя более усердной борьбы и качественного роста усилий по их преодолению.

На сегодняшний день, в эпоху цифровой экономики, крайне важно находить общие интересы в области кибербезопасности между странами-участниками международного сообщества. Совместные усилия и проведение совместных мероприятий по защите этих интересов будут играть ключевую роль в развитии международного сотрудничества. Поскольку киберугрозы являются серьезной проблемой для национальных интересов стран, в том числе для международной стабильности и безопасности, международное сотрудничество в области кибербезопасности будет направлено на выявление и пресечение киберугроз, а также на обеспечение глобальной информационной безопасности [3].

Основными направлениями международного сотрудничества в области кибербезопасности являются:

– Разработка международных стандартов и правил в области кибербезопасности. Данный аспект является одним из важнейших в современном информационном обществе. В этом контексте особое значение имеют международные документы, такие как Конвенция о киберпреступности, Глобальная Программа Кибербезопасности ISO и рекомендации по кибербезопасности Совета Европы.

– Обмен информацией и опытом в области кибербезопасности. Государства активно обмениваются информацией о киберугрозах и опытом по их предотвращению и противодействию.

– Сотрудничество в области подготовки кадров в сфере кибербезопасности. Данное направление создано с целью обеспечения эффективного реагирования на угрозы в сети.

– Сотрудничество в разработке и внедрении новых технологий в области кибербезопасности. Государства работают вместе над созданием и применением инновационных технологий, способных повысить уровень кибербезопасности в мире [4].

Киберпространство играет серьезную стратегическую роль в мировой экономике и политике, что подчеркивает важность международного сотрудничества и координации усилий в этой области. Однако в настоящее время уровень сотрудничества между странами в области кибербезопасности остается недостаточным. Причины данной ситуации включают в себя:

1. Разнообразие национальных подходов к регулированию киберпространства.

2. Отсутствие универсального определения кибербезопасности и единой системы оценки рисков.

3. Недостаток доверия между странами и опасения относительно утечки конфиденциальной информации.

4. Различия в уровне технологического развития и возможностях в области киберзащиты.

Из этого вытекает ряд проблем международного сотрудничества в области кибербезопасности:

– Трансграничность киберугроз. Киберугрозы не ограничиваются рамками государств, поэтому сотрудничество в этой сфере требует тесного взаимодействия между странами.

– Различия в подходах к кибербезопасности. Государства придерживаются различных подходов к кибербезопасности, что может затруднять их совместную деятельность в этой области [5].

Отсутствие доверия между государствами. Необходимость установления доверия между странами может помешать эффективному сотрудничеству в области кибербезопасности.

Для достижения успеха в сфере кибербезопасности международное сотрудничество должно базироваться на принципах взаимной ответственности, уважения суверенитета государств и сотрудничества.

Россия с 1998 года активно поддерживает развитие международного сотрудничества в сфере информационной безопасности на различных уровнях. На данный момент было подписано около 14 договоров и соглашений. Некоторые из них, включая соглашение с правительством Бразилии от 14 мая 2010 года, не действуют, а одно соглашение с Южно-Африканской Республикой от 4 сентября 2017 года еще не вступило в силу. Однако, продолжается работа в данном направлении.

Согласно Доктрине информационной безопасности Российской Федерации (официально утверждённой указом Президента РФ от 5 декабря 2016 г), киберпространство все чаще используется для военно-политических и противоправных целей[6].

В доктрине выделены пять основных блоков киберугроз, охватывающих различные аспекты угрозы для национальной безопасности:

1) воздействие иностранных государств на критическую информационную инфраструктуру РФ (системы энергообеспечения, управления транспортом, водоснабжения и т. д.);

2) использование спецслужбами иностранных государств и подконтрольными общественными организациями киберпространства для подрыва суверенитета и дестабилизации социально-политической обстановки в России;

3) рост масштабов киберпреступности;

4) отставание России в сфере разработки собственного программного обеспечения;

5) использование отдельными государствами технологического доминирования в глобальном информационном пространстве для достижения экономического и геополитического преимущества.

Для противодействия угрозам в киберпространстве Россия планирует укреплять сотрудничество с зарубежными партнерами, развивать собственные силы и средства в области кибербезопасности, а также стремиться к созданию системы стратегического удержания и предотвращения военных конфликтов.

В условиях возрастающих угроз в информационном пространстве гражданское общество активноведёт работу по поиску наиболее эффективных способов борьбы с современными вызовами, объединяя усилия профессионалов.

Как сообщается, негосударственный сектор готов внести свой вклад в обеспечение информационной безопасности, делая информационную среду по-настоящему безопасной.

На основе этих тенденций в России 30 мая 2018 года было принято решение о регистрации Национальной ассоциации международной информационной безопасности (НАМИБ) [7]. Также с инициативы Института проблем информационной безопасности МГУ имени М.В. Ломоносова, 25 апреля 2010 года был образован Международный исследовательский консорциум информационной безопасности (МИКИБ).

По результатам двенадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» и шестнадцатой научной конференции МИКИБ (16-19.04.2018 г., Гармиш-Партенкирхен, Германия), эксперты пришли к выводу, что развитию цифровой экономики необходимо уделить особое

внимание, учитывая ее инвестиционную привлекательность. Однако инвесторы пока не до конца осознают угрозы информационной безопасности в переходный период к цифровой эре и не готовы вложить средства в ее обеспечение.

На тринадцатом форуме по проблемам информационной безопасности президент НАМИБ Шестюк В.П. и президент Совета по кибербезопасности Германии Дюнн Х.-В. согласовали меморандум о взаимопонимании 24 апреля 2019 года [8].

В последние годы кибербезопасность стала одним из ключевых аспектов внешней политики Японии. Страна активно участвует в дипломатических переговорах, торговых соглашениях и международных встречах, посвященных вопросам кибербезопасности и информационно-коммуникационных технологий (ИКТ). Для координации усилий с партнерами по созданию и соблюдению правил управления киберпространством, а также поддержки инициатив в развивающихся странах, Министерство иностранных дел Японии создало специальный отдел по кибербезопасности, в котором работают пятнадцать сотрудников [9].

По данным Министерства иностранных дел Японии, на сегодняшний день у Японии заключено четыре соглашения на международном уровне по вопросам безопасности. Последнее из заключенных - соглашение с Австралией, после подписания соглашений с США, НАТО и Францией. Данное соглашение устанавливает процедуры для защиты конфиденциальной информации, предоставляемой Японией и Австралией на взаимной основе, в соответствии с национальными законами и правилами обеих стран. Ожидается, что оно способствует укреплению сотрудничества в области безопасности между Японией и Австралией, а также трехстороннего сотрудничества с их общим союзником - США.

В рамках Вассенаарских договоренностей, которые были подписаны Россией, США и Японией, государства-участники обязались препятствовать онлайн-продажам электронных систем наблюдения и проникновения, разработанных для обхода мониторинговых инструментов и систем противодействия взлому. Эти меры направлены на контроль за экспортом вооружений и технологий двойного назначения, чтобы предотвратить их неправомерное использование [10].

В 2017 году в Японии было учреждено Агентство поддержки кибербезопасности в промышленности (ICPA) – новый оперативный орган, который находится под юрисдикцией Министерства торговли и экономики. Его основная задача заключается в защите промышленности и критической инфраструктуры страны от кибератак. Для достижения этой цели агентство планирует привлечение "белых хакеров" с целью усиления безопасности ключевых отраслей экономики, таких как электросети, газоснабжение, нефтепереработка, химическая промышленность и ядерная энергетика.

В том же году правительство Японии создало "институт по исследованию кибератак", который предназначен для обучения государственных служащих с целью предотвращения, преодоления и снижения последствий кибератак на критически важные объекты инфраструктуры страны. Этот учебный центр является первым в своем роде в Японии и сосредоточен на предотвращении киберинцидентов в системах электропитания, а также на предотвращении утечек промышленной информации. Он подчинен Агентству содействия развитию ИКТ (IPA) [11].

Все вышесказанное доказывает, что международное сотрудничество в области кибербезопасности становится все более важным в контексте современного цифрового мира, где киберугрозы представляют серьезную угрозу для глобальной безопасности. Кибератаки и киберпреступность могут иметь разрушительные последствия для государств, компаний и обычных граждан. Поэтому совместные усилия стран по защите киберпространства становятся все более актуальными, и работы в данном направлении ведутся [12].

Одной из перспектив международного сотрудничества в области кибербезопасности является обмен информацией о киберугрозах и инцидентах. Это позволяет оперативно реагировать на угрозы и эффективно бороться с киберпреступниками. Также важно проводить совместные тренировки и учения для повышения квалификации специалистов и разработки общих стратегий по обеспечению кибербезопасности.

Другой перспективой является разработка международных норм и стандартов в области кибербезопасности, которые были бы обязательны для всех государств. Это позволило бы установить единые правила игры и усилить защиту киберпространства.

Кроме того, важно сотрудничество в области кибербезопасности между государствами и частным сектором, так как многие киберугрозы направлены как на государственные, так и на частные цели. Совместные проекты и инициативы помогут укрепить защиту как критической киберинфраструктуры, так и информации граждан.

Таким образом, дальнейшее развитие международного сотрудничества в области кибербезопасности имеет большое значение для обеспечения цифровой безопасности глобального сообщества и предотвращения киберугроз в будущем.

Выводы

Подводя итог, можно сказать, что наш образ жизни и обращение с различного рода информацией крайне изменилось после появления таких вещей как Интернет и искусственный интеллект, а потому международное сотрудничество в области кибербезопасности играет ключевую роль в предотвращении киберугроз и защите интернет-пространства.

Во всех национальных стратегиях, политиках или руководящих принципах в области информационной безопасности (ИБ), установлено, что сотрудничество через государственные границы является ключевым вопросом, поскольку кибербезопасность не ограничивается территориальными границами. Важно укреплять сотрудничество в области ИБ и кибербезопасности между странами, а также содействовать партнерству между правительством и промышленностью, поскольку это способствует формированию нормативно-правовой и организационной основы для создания глобальной системы информационной безопасности. И как показал опыт сотрудничества между различными странами, обмен информацией и лучшими практиками помогает укрепить кибербезопасность на глобальном уровне [13].

Однако, с увеличением числа кибератак и развитием новых технологий, необходимо постоянно совершенствовать международное сотрудничество в этой области. Важно разрабатывать общие стандарты и правила, координировать усилия в области кибербезопасности и проводить совместные учения для улучшения реагирования на угрозы.

Поэтому дальнейшие перспективы международного сотрудничества в области кибербезопасности включают в себя укрепление партнерских отношений между странами, расширение сферы обмена информацией и знаний, а также развитие совместных проектов и программ по защите киберпространства.

Только совместными усилиями международного сообщества можно достичь значительных результатов в обеспечении кибербезопасности и защите информационных ресурсов от киберугроз.

Список использованных источников:

1. Зиновьева Е.С. Международная информационная безопасность: монография / Е.С. Зиновьева; Моск. гос. ин-т междунар. отношений (ун-т) МИД России, каф.мировых политических процессов – М.: МГИМО-Университет, 2013.

2. Аксенов, С. В. Международное сотрудничество в области кибербезопасности: состояние и перспективы. М.: РУДН, 2023.

3. Министерство иностранных дел Российской Федерации. Внешняя политика. Многосторонние договоры. [Электронный ресурс] – Режим доступа: http://www.mid.ru/ru/foreign_policy/international_contracts/2_contract (дата обращения: 19.09.2020).

4. Кибербезопасность в контексте устойчивого развития: вызовы и возможности / под ред. В. А. Баранова. - М.: ИМЭМО РАН, 2023. - 200 с.

5. Гуляев, В. В. Международное сотрудничество в области кибербезопасности: проблемы и перспективы. М.: ИНФРА-М, 2023.

6. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. № 646 // Российская газета. - 6 декабря 2016 г.
7. Федеральная налоговая служба. [Электронный ресурс] – Режим доступа: <https://egrul.nalog.ru/index.html> (дата обращения: 20.10.2020).
8. Национальная Ассоциация международной информационной безопасности. [Электронный ресурс] – Режим доступа: <http://namib.online>; (дата обращения: 20.10.2020).
9. Хатауэй М., Демчак К., Кербен Д., МакАрдл Д., Спидальери Ф. Киберготовность Японии: краткий обзор. [Электронный ресурс] – Режим доступа: <https://analytica.digital.report/wpcontent/uploads/2017/05/CRI-Japan-RU.pdf>. (дата обращения: 25.10.2020).
10. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies / PUBLIC DOCUMENTS Volume IV Background Documents, Plenaryrelated, and Other Statements. Compiled by the Wassenaar Arrangement Secretariat December 2019. [Электронныйресурс] – Режимдоступа: <https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-006-Public-Docs-Vol-IV-BackgroundDocs-and-Plenary-related-and-other-Statements-Dec.-2019.pdf> (датаобращения: 30.10.2020).
11. Яковлева А.В. Вакуленко П.С. Общество 5.0 и кибербезопасность Японии // Экономика и предпринимательство. – 2019. – № 4 (105). С. 225-230.
12. Павлов, А. Н. (2023). Международное сотрудничество в области кибербезопасности: теория и практика. М.: Юрайт.
13. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (ч. 2) // Вопросы кибербезопасности. 2014. №1 (2). С. 5–12.

**МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ
BANKCARD FRAUD**

А.А. Пильдунча, Л.В. Шаронина

Ростовский институт (филиал) ФБГО ВО «Всероссийский государственный университет юстиции (РПА Минюста России) в г. Ростове-на-Дону, 344002, г. Ростов-на-Дону, Соборный пер., 26/71, email: nastya.pilduncha.05@mail.ru, sharoninal@mail.ru

A.A. Pilduncha, L.V. Sharonina

Rostov Institute (branch) of the All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) in Rostov-on-Don, 344002, 26/71 lane. Cathedral, Rostov-on-Don, 344002, Russia, email: nastya.pilduncha.05@mail.ru, sharoninal@mail.ru

Аннотация: В статье рассматриваются популярные виды мошенничества, связанные с использованием банковских карт, а также способы их предотвращения. Приводятся примеры инноваций в системе безопасного использования платежных карт, разработанных с использованием технологий искусственного интеллекта для предотвращения мошеннических операций и улучшения системы безопасности.

Ключевые слова: мошенничество, банковские карты, скимминг, фишинг, вишинг, траппинг, искусственный интеллект.

Annotation: The article discusses popular types of fraud related to the use of bank cards, as well as ways to prevent them. Examples of innovations in the system of secure use of payment cards developed using artificial intelligence technologies to prevent fraudulent transactions and improve the security system are given.

Keywords: fraud, bank cards, skimming, phishing, vishing, trapping, artificial intelligence.

Введение

Сейчас высокую распространённость получили банковские карты, ими очень легко расплачиваться в магазине, путешествовать, удобно получать заработную плату [1]. Даже трудно представить, как совсем недавно все ещё получали зарплату наличными. В наше время это возможно, но в редких случаях.

Конечно, стоит отметить, что их популярность набирает охваты. Поскольку не нужно всегда в кармане носить большое количество монет, а в бумажнике стопки денег. При этом кредитные, банковские карты очень привлекают злоумышленников. Они могут, не прикладывая больших усилий быстро разбогатеть, используя, зачастую, только смекалку, хитрость и обман.

Мошенничество - способ кражи денег у юридического, физического лица незаконным путём. Возможна также, кража личной информации, за которой последуют списания с карт. Стоит отметить, что в XX веке мошенничество с банковскими картами является одним из самых популяризированных преступлений. Это говорит об актуальности данной темы.

Цель исследования

Целью работы является выявление основных видов мошенничества с банковскими картами; разработка правил для предотвращения незаконных списаний.

Материал исследования

Проведем анализ статистических данных по мошенническим операциям с банковскими картами. В 2023 году объем незаконных операций без согласия клиентов увеличился на 11,48% по сравнению с 2022 годом, при этом наблюдается рост объема денежных переводов по картам

(+10,54%, достигнув 136,38 трлн рублей). Объем операций по банковским картам представлен в табл. 1 [2].

Таблица 1

2022 год		2023 год	
Объём операций, млн. руб	Количество операций, тыс. ед	Объём операций, млн руб	Количество операций, тыс. ед
14165,44	876,59	15791,41	1165,99

Отмечается, что в 2023 году количество мошеннических операций с использованием карт равно 84,72% (наивысший показатель среди остальных типов операций), по счетам (без использования карт) – 7,34%, через СБП – 7%(рис.1) [2].



Рис.1. Показатели мошеннических операций с платежными средствами, тыс.

В настоящее время выделяются следующие виды (методы) мошенничества с банковскими картами.

1. «Скимминг» включает создание так называемых "безлицевых карт" или "клонов карт" с использованием специального аппарата – скиммера, который мошенники устанавливают на банкоматы или терминалы оплаты, в результате чего извлекается конфиденциальная информация с магнитной полосы карты клиента, после чего производится копия данных карты оплаты. Для получения кода доступа к карте устанавливается скрытая камера или специальное устройство на клавиатуре банкомата, которое фиксирует введенные цифры. После этого преступники могут без ограничений использовать денежные средства на карте. А владелец, в свою очередь, может столкнуться с затруднениями в доказательстве своей непричастности к несанкционированным операциям [3].

2. Фишинг заключается в незаконном получении мошенниками персональных данных владельца карты. Например, преступники отправляют псевдо сообщения от коммерческих банков, сообщая о предполагаемых изменениях в системе защиты, при этом пытаются выведать информацию у собственника по карте (номер, пин-код) либо ответить на сообщение, перейти на псевдо сайт банка и заполнить форму.

3. Вишинг – данный метод схож с фишингом, только с помощью использования телефонных звонков обманым путем мошенники узнают личные данные клиентов банков. Например, клиент получает звонок от автоинформатора, представляющегося сотрудником банка, который сообщает о попытке незаконного списания средств со счета. Мошенники уговаривают клиента перезвонить по указанному номеру. Однако этот номер является фиктивным, и звонок по нему перенаправляет на

поддельного оператора службы безопасности, который просит клиента ввести данные карты через телефонную клавиатуру [4].

4. Метод "траппинга" заключается в установке специального устройства на банкомат, которое задерживает карту. При этом карта не возвращается клиенту (а, следовательно, и деньги не могут быть получены, пока карта не будет извлечена). В течение того времени, когда человек идет в свой банк, мошенники извлекают застрявшую карту из банкомата, удаляют устройство, вставляют карту заново и далее списывают платежные средства с оставленной карты.

5. «Бесконтактная кража» - метод похищения денежных средств со счета без необходимости извлечения карты из кошелька и ввода пин-кода. Например, в многолюдных местах мошенники прикладывают бесконтактный считыватель к сумкам, карманам одежды и идет мгновенный перевод средств.

6. «Наблюдать за плечами» - происходит похищение личных данных владельца карты в момент совершения оплаты. Не только сторонние мошенники представляют угрозу, но и недобросовестные работники торговли, услуг и банковского сектора. Схема проста: мошенник, получивший карту для оплаты, может сделать фотографию, записать данные или просто запомнить их, чтобы впоследствии совершить транзакции в интернете.

7. «Списывание денег дважды», когда при совершении платежа покупатель передает карту оператору, а тот сообщает об ошибке в транзакции. Это действие может повторяться несколько раз. Однако через некоторое время владелец карты обнаруживает, что деньги были списаны дважды за одну покупку.

В современной экономике предстоит переход на новые методы защиты и идентификации клиентов. Они заменят устаревшие и не совсем надёжные в сфере безопасности. Пластиковые карты будут оснащены различными новейшими разработками и будут представлять из себя мини-компьютер. Приведем примеры новых методов защиты.

1. Карта с биометрической защитой (со сканером отпечатков пальцев владельца). Чтобы воспользоваться картой, необходимо разблокировать её, просто приложив палец к специальному участку карты, который заменяет ввод PIN-кода. Такие карты, например, MasterCard, были представлены в США в октябре 2014 года, и начиная с 2015 года прошли испытания в Польше и Норвегии. На данный момент в России ни один банк не выпускает такие карты, хотя их появление на российском рынке могло бы способствовать развитию системы защиты карт и бесконтактных платежей в стране[4].

2. Карта с дисплеем – представляет собой передовую технологию для генерации и использования одноразовых паролей. Этот тип карты (Visa Platinum) объединяет традиционную банковскую карту с безопасным способом совершения операций в интернет-магазинах и интернет-банке. В дополнение к чипу и магнитной полосе на карте установлены микродисплей и сенсорная клавиатура, которые позволяют владельцу генерировать одноразовые пароли при совершении операций в интернет-банке и оплате покупок онлайн. Внедрение подобных карт российскими банками поспособствует обеспечению повышенной безопасности для клиентов, уменьшению убытков от мошенничества, увеличению объема банковских операций, проводимых в Интернете.

3. Карта «по требованию», где магнитная полоса формируется динамически в соответствии с инструкциями владельца. Прежде чем произвести операцию по оплате, владелец вводит пароль на интегрированной клавиатуре. Эта технология может быть интегрирована с картами, оснащенными экранами, что обеспечит дополнительный уровень безопасности.

4. Карта с регулярно обновляющимся кодом защиты, при использовании которой потребуются ввести трехзначный код (имеет способность автоматически обновляться каждые три часа).

Современные учёные изучают вопросы, связанные с применением технологий искусственного интеллекта (ИИ) в целях предотвращения мошенничества с банковскими картами. Искусственный интеллект должен быть объективен и справедлив, не опираться на национальность, пол и другие характеристики. При этом очень важно, чтобы он был подконтролен человеку.

Определены некоторые риски: расстройство системы безопасности, причинение вреда человеку, ненадёжность его решений. Для устранения этих рисков, например, Сбербанк одним из первых в России утвердил принципы этики ИИ. Они дают сотрудникам ориентиры, как поступать в

ситуациях этических дилемм, которые могут возникнуть при взаимодействии с ИИ. ВТБ для решения этих проблем внедрил систему управления моделями [5].

Итак, искусственный интеллект – хорошая возможность сделать свои счета и вклады недопустимыми для мошенников, и он имеет большие перспективы в развитии. Конечно же, есть множество рисков, но во многих странах он уже используется. Поэтому, данная технология считается очень нужной и полезной, которую стоит внедрить как можно быстрее, поскольку потребители надеются на обеспечение безопасности своих счетов со стороны банка. При этом важно не забывать об информировании населения о новых видах мошенничества [6].

Внедрение искусственного интеллекта делает более безопасным выполнение большинства денежных операций онлайн: можно будет быстрее и эффективнее распознавать новые виды мошенничества, а также обнаруживать подозрительные операции и предотвращать их проведение [7].

Рассмотрим основные правила безопасного использования банковских карт при совершении платежей.

Нельзя оставлять карту в доступных местах и отдавать в чужие руки.

Стоит подключить СМС уведомления по всем операциям. Если вы получили уведомление о списании средств за покупку, не нужно снова повторять платёж. Если же всё-таки деньги были списаны дважды, необходимо срочно обратиться в банк.

Сотрудники Центрального банка рекомендуют носить карту в защищённом фольгой отсеке бумажника. Также, лучше установите максимальную сумму по списаниям с карты.

Если оплачиваете покупку безналичным способом, то важно следить, как её в вашем присутствии пропускают через терминал. Обязательно сохраняйте чек.

Необходимо запомнить пин-код, неприемлемо писать его на самой карте или бумаге. Конечно же, не нужно говорить его даже операторам банка.

При онлайн покупках рекомендовано завести отдельную карту, которую необходимо хранить в недоступных для посторонних местах. А для карты, которую вы используете для оплаты через терминалы нужно отключить всевозможные операции в интернете.

При потере или краже банковской карты нужно незамедлительно обратиться в банк через горячую линию.

Выводы

Итак, для большей эффективности, нужно придерживаться указанным правилам с использованием платёжных карт по защите от мошенников. Именно они в дальнейшем могут послужить гарантией комфортных условий для работы с картами, как для банка, так и для клиента. Противодействие злоумышленникам, которые желают похитить средства с банковских карт разными способами, требует комплексного подхода. Искусственный интеллект – новая возможность для банков и пользователей обезопасить свои сбережения, вклады. Конечно, существуют определенные риски, однако без внедрения ИИ рисков по потере денежных средств будет ещё больше. С помощью технологий ИИ можно будет быстрее и эффективнее распознавать новые виды мошенничества, предоставлять необходимую информацию сотрудникам, обнаруживать подозрительные операции и предотвращать их проведение. Использование возможностей искусственного интеллекта значительно усилит действующие меры противодействия и создаст синергетический эффект по борьбе с мошенничеством в банковской сфере.

Список литературы:

1. Банк России [Электронный ресурс]. URL: https://cbr.ru/analytics/ib/operations_survey/2023/ (дата обращения: 19.04.2024)
2. Карта под контролем: способы защиты денег на банковском счете. URL: <https://tass.ru/ekonomika/4459891> (дата обращения: 19.04.2024)
3. Назарчук Н.П. Банковские карты как инструмент расчетов и кредитования: Монография. Минобрнауки России, ТГТУ. Тамбов: Издательство Юконф, 2022. 110 с.

4. Теория и практика деятельности финансово-кредитных организаций на рынке банковских карт: монография / Л. Н. Бондарева, М. М. Микушина, А. Ю. Сергеева [и др.]; под науч. ред. В. А. Шапошникова. Екатеринбург: Изд-во Рос. гос. проф.-пед. ун-та, 2023. 112 с.
5. Искусственный интеллект в финансах: как банки используют нейросети [Электронный ресурс]. URL: <https://trends.rbc.ru>(дата обращения: 09.04.2024)
6. [Вовк Ю.Д., Шаронина Л.В. Развитие и использование рынка платежных систем России // Правовое образование. Сб. науч.тр. Изд-во:Ростовский институт \(филиал\) федерального государственного бюджетного образовательного учреждения высшего образования "Всероссийский государственный университет юстиции \(РПА Минюста России\)" в г. Ростове-на-Дону \(Ростов-на-Дону\). Т.14. С.226-233.](#)
7. Багреева Е.Г., Исмаилов Н.Э.и др. Искусственный интеллект как противодействие мошенничеству в банковской сфере //Евразийская адвокатура. 2022. № 2 (57). С. 90-95.

УДК 94 (476) + 378.115

**ФОРМИРОВАНИЕ ПРЕДПРИНИМАТЕЛЬСКИХ И ПРОФЕССИОНАЛЬНЫХ
КОМПЕТЕНЦИЙ У СПЕЦИАЛИСТОВ ИНЖЕНЕРНО-ЭКОНОМИЧЕСКОГО И
ТЕХНИЧЕСКОГО ПРОФИЛЯ ПРИ ПРЕПОДАВАНИИ СОЦИАЛЬНО-ГУМАНИТАРНЫХ
ДИСЦИПЛИН**

**FORMATION OF ENTREPRENEURIAL AND PROFESSIONAL COMPETENCIES AMONG
ENGINEERING, ECONOMIC AND TECHNICAL SPECIALISTS WHEN TEACHING SOCIAL
AND HUMANITARIAN DISCIPLINES**

И. А. Пушкин

Учреждение образования «Белорусский государственный университет пищевых и химических технологий», Беларусь, 212027, г. Могилев, п-т Шмидта, 3.

I. A. Pushkin

**Belarusian State University of Food and Chemical Technology, 3, Shmidt Avenue Mogilev, 212027
Belarus.**

Аннотация. Раскрыты и проанализированы методические и методологические аспекты формирования профессиональных, предпринимательских компетенций и обоснованной патриотической позиции у специалистов инженерно-экономического и технического профиля при преподавании социально-гуманитарных дисциплин. Сделан вывод, что в современных условиях одновременное формирование патриотизма и профессиональных (предпринимательских) компетенций является основой укрепления экономической, продовольственной и информационной безопасности Союзного государства Беларуси и России.

Ключевые слова: Беларусь; экономическая безопасность; предпринимательские и профессиональные компетенции; социально-гуманитарные дисциплины; подготовка кадров

Abstract. The article reveals and analyzes the methodological and methodological aspects of the formation of professional, entrepreneurial competencies and a justified patriotic position among specialists in engineering, economics and technology when teaching social and humanitarian disciplines. It is concluded that in modern conditions the simultaneous formation of patriotism and professional (entrepreneurial) competencies is the basis for strengthening the economic, food and information security of the Union State of Belarus and Russia.

Keywords: Belarus; economic security; entrepreneurial and professional competencies; social and humanitarian disciplines; personnel training

Введение

На современном этапе развития общества всё более актуальным становится понимание задач национального и экономического развития государства. Одной из наиболее важных является обеспечение экономической, продовольственной и информационной безопасности. Этого невозможно достичь без должной подготовки высококвалифицированных специалистов инженерно-экономического и технического профиля. При этом неотъемлемым и необходимым является одновременное формирование патриотизма и профессиональных, особенно предпринимательских, компетенций у выпускников высших учебных заведений.

Наша цель – рассмотреть некоторые методические и методологические аспекты подготовки специалистов по обеспечению экономической, продовольственной и информационной безопасности Союзного государства Беларуси и России при преподавании социально-гуманитарных дисциплин.

Основная часть

Формированию профессиональных, социальных, личностных компетенций и обоснованной патриотической позиции способствуют учебные дисциплины социально-гуманитарного профиля, преподаваемые в Белорусском государственном университете пищевых и химических технологий: «История белорусской государственности», «Социология управления», «Экономика», «Правовое

обеспечение хозяйственной деятельности», «Этика и психология деловых отношений», «Правовое обеспечение бизнеса», «Коррупция и ее общественная опасность», «Основы управления интеллектуальной собственностью», «Историко-культурное наследие города Могилёва», «Великая Отечественная война советского народа».

В целях вовлечения студентов в поиск и управление знаниями, приобретения опыта самостоятельного решения различных задач, обеспечения воспитательной функции учебного процесса преподаватели кафедры социально-гуманитарных дисциплин используют современные технические средства обучения, технологии проблемно-модульного обучения, учебно-исследовательской деятельности, проектные (составление бизнес-планов), коммуникативные (дискуссии, учебные дебаты, пресс-конференции), игровые (участие в деловых, ролевых, имитационных играх) технологии, анализ ситуаций и т.д. Внедряются отдельные педагогические технологии: учебно-методические комплексы (в том числе электронные); вариативные модели самостоятельной работы студентов, блок-модульная, модульно-рейтинговая и кредитная системы, информационные технологии, кейс-метод, методы активного обучения. Для организации контрольной деятельности используются рейтинговые (промежуточные тесты, как разрабатываемые преподавателем, так и изданные другими), кредитно-модульные системы оценок за учебную, исследовательскую и контролируемую самостоятельную работу студентов[1].

Регулярно обновляемые учебные программы, предназначенные для реализации на первой ступени высшего образования в рамках цикла социально-гуманитарных дисциплин, акцентированы на компетентном подходе к обучению, значительное усиление роли и доли самостоятельной работы студентов, использование современных инновационных педагогических технологий. В рамках совместного сотрудничества преподавателя и обучающегося программы выступают своеобразными «навигаторами» по усвоению знаний, информации и приобретению практикоориентированных, жизненно важных навыков.

Подавляющее большинство дисциплин гуманитарного профиля полностью оснащены учебно-методическими пособиями, разработаны и внедрены в учебный процесс лекционные курсы в формате презентаций и электронных учебно-методических комплексов (получены регистрационные удостоверения Государственного реестра информационных ресурсов). При изучении дисциплин предусмотрены лекции, практические занятия, экскурсии на предприятия, по Могилёву и музеям города, написание рефератов (учебно-исследовательских работ), промежуточное тестирование, а также устный или письменный зачёт. На практических занятиях и в ходе управляемой самостоятельной работы студенты создают бизнес-планы, инновационные предложения для предприятий пищевой промышленности[2–4].

Накоплен определенный опыт одновременного формирования патриотизма и профессиональных, предпринимательских компетенций при преподавании следующих дисциплин: «История Беларуси» в последнее время заменена на «Историю белорусской государственности», «Правовое обеспечение хозяйственной деятельности», «Основы управления интеллектуальной собственностью», «Историко-культурное наследие города Могилёва», «Правовое обеспечение бизнеса», «Великая Отечественная война советского народа».

Патриотизм – это политический принцип и социальное чувство, осознанная любовь к своему народу, его традициям, привязанность к Родине, преданность ей и готовность идти ради неё на жертвы. Оно предусматривает гордость за достижения и культуру своей Родины, стремление сохранить ее характер и культурные особенности и самоидентификацию (особое эмоциональное переживание своей принадлежности к стране и своему гражданству, языку, традициям) с другими представителями своей Родины. народа, стремление защитить интересы Родины и народа.

Предпринимательские компетенции – личностные или деловые качества, навыки, модели поведения, обладание которыми помогает успешно решать определенную бизнес-задачу и достигать высоких результатов. Чем большее количество предпринимательских компетенций имеет в своем арсенале человек, тем больше вероятность, что он сможет справиться со стоящими перед ним бизнес-задачами.

При изучении «Истории Беларуси», «Истории белорусской государственности», «Историко-культурного наследия города Могилёва», «Великой Отечественной войны советского народа»

рассматриваются закономерности и процессы государственно-политического, социально-экономического, конфессионального, культурного и духовного развития белорусского народа в контексте восточнославянской истории с учетом особенностей цивилизационного развития; события Второй мировой и Великой Отечественной войн, их взаимозависимости и влияния на судьбы народов СССР, Европы и всего мира, вклад белорусского народа в разгром агрессоров, сохранение своей свободы и национальной идентичности, истоки патриотизма и Великой Победы [4–6].

Будущие специалисты знакомятся с деятельностью известных людей, связанной с историей и культурой Беларуси, основными памятниками материального и духовного наследия; учатся характеризовать и анализировать социально-экономическую историю, а также культуру, поведение, сознание, менталитет населения разных национальностей и вероисповедания в контексте личностных и общественных (государственных) интересов, плюрализма взглядов и объединяющего чувства патриотизма. Студенты приобретают навыки определения связи общеисторических процессов и явлений с отдельными событиями городской жизни, формирования толерантности, использования историко-культурного наследия в своей будущей практической хозяйственной деятельности.

Дисциплины «Правовое обеспечение хозяйственной деятельности», «Правовое обеспечение бизнеса» обеспечивают овладение студентами навыками работы с действующими нормативно-правовыми актами, умением искать правовую информацию и использовать её в практической работе коммерческих и некоммерческих организаций на всех стадиях создания, реорганизации и ликвидации юридических лиц. Развитие правовой культуры и чувства ответственности при выполнении задач социально-экономического развития страны происходит на практических занятиях при решении проблемных ситуаций и задач в хозяйственной деятельности, при выполнении творческих заданий и написании рефератов. Студенты вместе с преподавателем выступают в роли экспертов.

На занятиях «Основы управления интеллектуальной собственностью» студенты учатся разрабатывать изобретения, полезные модели, промышленные образцы, товарные знаки, фирменные наименования, географические указания, заключать авторские, издательские и лицензионные договора в контексте избранной специальности [2, 3]. Основа их предложений – культурное и историческое наследие белорусского народа, в том числе XIX и XX веков, когда Беларусь и Россия совместно развивались в составе Российской империи и СССР.

При этом основной акцент делается на белорусское Приднестровье, которое является наиболее интересным регионом Восточной Европы. Неслучайно здесь были обнаружены древнейшие поселения первобытных людей на территории Беларуси. На протяжении веков Могилёвская область (губерния) и город Могилёв находились в центре столкновения человеческих интересов и конфликтов: религиозных, межгосударственных, национальных. Но могилёвцы старались оставить после себя добро, величие, красоту и благородные стремления, воплощенные в памятниках материальной и духовной культуры. Могилёв пережил богатство и величие, войны и разрушения, взлёты и падения. Несмотря ни на что, историко-культурное наследие сохранило свою самобытность, достойную памяти и сохранения [6–11].

Любые знания о прошлом Могилёвщины, нашей «малой Родины», приближают их к нам, обогащают наши чувства, наполняют окружающее пространство и время событиями и лицами. История и культурное наследие позволяют нам увидеть в далеком прошлом, каким было его будущее, по крайней мере, позволяют нам извлечь из него уроки. Выражая гордость за прошлое, мы надеемся, что будущие поколения будут гордиться сегодняшним днем, действиями и поступками людей первой половины XXI века.

Из большого количества событий и лиц выбираются наиболее интересные, которые могут быть использованы современниками в своей практической деятельности. В ходе подготовки студентами бизнес-планов или инновационных проектов историко-культурное наследие Беларуси и Могилёва находит свое применение в сфере производства и реализации продуктов питания, туризма, рекламы, создания архитектурно-географической и ландшафтной среды, в названиях брендов продуктов питания, предприятий, фирм, магазинов, кафе, ресторанов, товаров, блюд и т.п. Студенты, работая над созданием пищевого продукта, предприятия по его производству или реализации, объекта общественного питания, разрабатывают: название, внешний вид, торговую марку, бренд, дизайн (упаковку, витрину, стенд и т.п.), цветовое решение, рекламу. Должны быть обоснованы

инновационность проекта, затраты и прибыль, сфера использования и реализации, категория потребителей, пути продвижения на рынок, сопутствующие товары, относящиеся к объекту бизнес-плана, возможность появления новых видов товаров или просчитываются пути расширения бизнеса[1, 4].

Обязательным является экономическое, историческое и патриотическо-воспитательное обоснование, связь с предметом дисциплины и специализацией студентов. Например, в 2020 году бизнес-проекты и управляемая самостоятельная работа были посвящены в основном 75-летию Победы, в 2021 году – 80-летию начала Великой Отечественной войны и 30-летию Независимости Республики Беларусь, в 2023 и 2024 гг. освобождению Беларуси от гитлеровских захватчиков. Предметом использования были способы и формы увековечивания памяти о событиях и участниках Великой Отечественной (Второй мировой) войны, досуг и условия быта участников боёв, жизнь населения на оккупированной территории и в период восстановления страны, героический труд в тылу и т. п.; события, предшествовавшие и свидетельствовавшие о первых годах существования суверенной Республики Беларусь, внешнеполитические обстоятельства, условия жизни населения, деятельность лиц, повлиявших на развитие процесса национально-государственного строительства и т.п.

Заключение

Преподавание знаний о национально-государственном строительстве Беларуси, историко-культурном наследии родной земли, деятельности юридических лиц, объектах интеллектуальной собственности и их использовании, актуализирует у студентов и выпускников уважение к историческому прошлому своего народа, гордость за свои достижения, активизирует деятельность по созданию нового и прогрессивного, способствует формированию патриотизма и профессиональных (предпринимательских) компетенций, практических навыков, необходимых и достаточных для решения и выполнения социальных, социально-профессиональных и личностных задач, функций выпускников учреждений высшего образования технического профиля. Что, безусловно, является основой укрепления экономической, продовольственной и информационной безопасности Союзного государства Беларуси и России в современных условиях.

Список литературы

1. Пушкін, І. А. Фарміраванне патрыятызму і прафесійных кампетэнцый у тэхнічных установах вышэйшай адукацыі праз выкарыстанне культурна-гістарычнага асяроддзя Беларусі / І. А. Пушкін // Качество подготовки специалистов в техническом университете : проблемы, перспективы, инновационные подходы : материалы VI Международной научно-методической конференции, 18 ноября 2022 г., Могилев / Учреждение образования «Белорусский государственный университет пищевых и химических технологий» ; редкол. : А. С. Носиков (отв. ред.) [и др.]. – Могилев : БГУТ, 2022. – С. 275–277.
2. Дыжова, А.А. Методы и средства исследований: Конспект лекций / А.А. Дыжова. – Могилев: УО МГУП, 2009. – 128 с.
3. Дыжова, А.А. [Основы управления интеллектуальной собственностью: Конспект лекций / А.А. Дыжова. – Могилев: УО МГУП, 2007. – 130 с.](#)
4. Пушкін, І. А. Гістарычная і культурная спадчына горада Магілёва: Курс лекцый / І. А. Пушкін. – Магілёў: УА МДУХ, 2006. – 150 с.
5. История белорусской государственности / Г. В. Алексашина [и др.]; под ред. Н. И. Полетаевой. – Минск : «Экоперспектива», 2023 – 239 с.
6. Костеров, А. П. Оборонительные бои на могилевском направлении летом 1941 года: монография / А.П.Костеров. – Минск: БГУ, 2010. – 186 с.

7. Агеев, А. Г. Перекрестки Могилёвской истории / А. Г. Агеев, Я. И. Климуть, И. А. Пушкин. – Минск: ООО "Туринфо", 2004. – 216 с.
8. Агееў, А. Р. Фарміраванне і дзейнасць Магілёўскага Беларускага Камітэта (1917–1918): манаграфія / А. Р. Агееў, І. А. Пушкін. – Магілёў : МДУ імя А. А. Куляшова, 2017. – 292 с.
9. Ад Магдэбургскага права да сучаснага самакіравання: зборнік навуковых матэрыялаў / уклад., аўт. прадмовы І. А. Пушкін, А. Р. Агееў. – Магілёў: МДУХ, 2017. – 184 с.
10. Курков, И. Могилёвщина: легенды, события, люди / И. Курков, И. Пушкин. – Минск: Медиафакт, 2008. – 368 с.
11. Пушкін, І. А. Грамадская і культурна-асветніцкая дзейнасць нацыянальных меншасцей у Беларускай ССР (1919–1991) : манаграфія / І. А. Пушкін. – Магілёў : МДУХ, 2018. – 423 с.

ПРОФИЛАКТИКА И ПРЕДУПРЕЖДЕНИЕ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ

Серпионов Кирилл Сергеевич студент 4 курса очной формы обучения по направлению подготовки 40.03.01 Юриспруденция Ростовского института (филиала) ВГУЮ (РПА Минюста России) e-mail: Serpion2015@yandex.ru

Научный руководитель: доктор экономических наук, профессор, Ростовского института (филиала) ВГУЮ (РПА Минюста России) Алибеков Шахизин Ильмутдинович

Аннотация. В настоящей научной работе автор изучает меры и методы профилактики экономических преступлений в современном обществе. Автор рассматривает различные аспекты преступности в сфере экономики, анализирует причины возникновения экономических преступлений, а также предлагает эффективные стратегии предупреждения таких преступлений. В работе освещены современные подходы к детектированию, контролю и пресечению экономических преступлений, включая правовые, уголовные, экономические и социальные аспекты. Автор также рассматривает роль государства, общественных институтов и бизнес-структур в профилактике экономической преступности.

Ключевые слова: Профилактика, предупреждение, экономические преступления, меры, анализ, стратегии, детектирование, контроль, правовые аспекты, уголовные аспекты, социальные аспекты, государство, общественные институты.

Экономическая преступность - одна из структурных частей преступности, включающая в себя совокупность всех совершенных сфер экономики противоправных деяний, посягающих на отношения собственности, правомерность предпринимательства и свободу экономической деятельности¹.

В целом по стране в 2014 году выявлено свыше 60 тысяч тяжких и особо тяжких преступлений экономической направленности, в том числе только по городу Москве - 8602 преступления экономической направленности, их удельный вес в общей массе правонарушений составил 4,7%. Сумма установленного в ходе расследования уголовных дел экономической на- материального ущерба в г. Москве составила 48,0 млрд. рублей. На стадии окончания уголовных дел размер его возмещения составил 5,31 млрд. рублей (11,0%). За январь-апрель 2023 года правоохранительные органы выявили 45 829 экономических преступлений¹, следует из статистики МВД. Это приблизительно на 4000 меньше, чем за аналогичный период в прошлом году. Самый большой процент — 39,9% — это преступления против собственности. Общее количество таких нарушений — 16 298. Большая часть из них связаны с мошенничеством (ст. 159-159.3 и 159.5-159.6 УК). В сфере экономической деятельности выявлено 13 655 или 33,5% проступков.

В целом количество лиц, привлеченных к уголовной ответственности по экономическим составам, возросло на 13,3% по сравнению с прошлым годом. Аналогичная тенденция прослеживается в увеличении на 37% числа выявленных лиц по фактам получения взятки. Средняя сумма взятки в г. Москве по выявленным преступлениям осталась на уровне прошлого года - 327 тысяч рублей (в среднем по России - 139 т. р.)². В сентябре 2016 года Всероссийская антикоррупционная общественная приемная «Чистые руки» опубликовала доклад, где говорилось, что в 2016 году средний размер взятки в России увеличился до 800 000 рублей. Это на 25% больше,

¹Волынский А.Ф., Лапин В.О. Расследование экономических преступлений. Учебное пособие. - М.: Академия экономической безопасности МВД России, 2011 -124 с. 2.

чем в 2015 году.

В ходе роста числа совершенных экономических преступлений, появление новых способов их совершения, а также усугубляется экономической ситуацией, остро встает вопрос о профилактике преступлений в сфере экономики.

Так, главными направлениями борьбы с экономической преступностью являются: применение комплекса оперативно- розыскных мероприятий; борьба с незаконной предпринимательской деятельностью; предупреждение совершения преступлений в бюджетной сфере; привлечение к ответственности лиц, совершивших экономическое преступление; - обеспечение возмещения государству, физическим и юридическим лицам убытков от экономических преступлений; информационная поддержка борьбы с экономической преступностью.

Данные преступления являются основой теневой экономики, поэтому противодействия им должно осуществляться в едином комплексе мер (правовых, экономических, социальных, политических) реализации государственной политики в данной сфере общественных отношений².

Предупреждению экономической преступности основная роль принадлежит системе мер общесоциального уровня: стабилизация экономики, рост производства, обеспечение занятости населения, достижение баланса экономической эффективности и социальной справедливости.

Неустойчивость экономики усугубляется введением санкций против России, а также снижением цен на нефть, что влечет за собой целый ряд проблем. К экономическим мерам предупреждения относят: стимуляция частного предпринимательского поведения, установление ответственности за использование недобросовестной конкуренции, дискредитация «нечестных» экономических финансовых партнеров, исключение клановых проявлений монополизма, связанные с коррупцией, недопущение получения сверхприбылей противоправными способами. ответственности за невыполнение экономических обязательств, несоблюдение финансово-кредитной, платежной и договорной, но если оздоровление возможно лишь в долгосрочной перспективе, то правовые меры способны снизить уровень совершения преступлений в сфере экономики сразу же после их принятия и реализации. Прежде всего, это изменения в законодательстве, причем не однократные, а систематические, ведь с развитием науки и техники появляются все новые и новые виды и способы совершения преступлений².

К примеру, в российском законодательстве отсутствует сам термин «экономическое преступление», что затрудняет его квалификацию. Должны быть устранены все недостатки и пробелы законодательства о предпринимательской деятельности, законодательства о банках и банковской деятельности, законодательства о деятельности небанковских финансовых учреждений и т. д.

Особое внимание стоит уделить отсутствующей в России уголовной ответственности юридических лиц. Это является проблемой, требующей особого внимания, поскольку это может способствовать облегчению возможности экономических преступлений. Отсутствие уголовной ответственности для юридических лиц может создавать ситуацию, в которой компании и организации, в том числе их руководители, могут нести ответственность только административно или гражданско-правовым путем. Это может ослабить стимул для соблюдения законов и норм, поскольку последствия могут быть менее серьезными. Отсутствие уголовной ответственности для юридических лиц также может привести к недостаточной защите прав и интересов граждан и других

²Миронцева А.В. Миронцев Р.Н. Приватизация в России: перезагрузка / Финансовая аналитика: | проблемы и решения. - 2015. - № 28 (262). - С. 30-38. Вакула А.И., Земельное право, учебное пособие / Донской государственный технический университет. Ростов-на-Дону, 2016 г., с. 182.

сторон, пострадавших от экономических преступлений. Поэтому необходимо уделить внимание этой проблеме и рассмотреть возможные изменения в законодательстве с целью введения уголовной ответственности для юридических лиц, чтобы предотвратить и сдерживать экономические преступления.

Угроза применения мер уголовного характера делает более строгим внутренний контроль в коммерческих структурах и предприятиях, и это усилит их заинтересованность в соблюдении требований закона, даже вопреки экономическим интересам. А угроза репутации компании поможет менеджерам справиться с соблазном обойти закон. Основные проблемы правовой профилактики экономической преступности заключаются в большом распространении схем мошенничества. Именно они, балансируя на грани уголовно наказуемого деяния и спора хозяйствующих субъектов. вследствие несовершенства действующего законодательства, не нашли адекватной уголовно-правовой оценки и должного отражения в следственной практике. Поэтому необходимо совершенствовать российские правовые нормы и процедуры, вводить в гражданское и корпоративное законодательство РФ специализированную экономическую терминологию, что будет способствовать большей доказуемости экономических преступлений, соотнести наказание с причиненным ущербом.

Кроме того, наведение порядка в сфере бизнеса позволит повысить инвестиционную привлекательность российского рынка. Введение новых механизмов также облегчит применение правовых мер по отношению к организациям, причастным к незаконному выводу капиталов и активов за рубеж и ускорит их возвращение в Российскую Федерацию. Помимо этого, это позволит эффективно бороться с фиктивными юридическими лицами³. основным мерам профилактики экономических преступлений следует также отнести информирование граждан.

Повышение знаний граждан в сфере экономики будет способствовать большей защищенности от посягательств со стороны мошенников. В общегосударственном масштабе осуществлением данного направления уже занимается ЦБ РФ: ведется разработка сайта, на котором будут размещены аксиомы экономики. Среди граждан должна идти активная пропаганда правовых знаний, необходимых для добросовестного и правомерного поведения в сфере экономических отношений, а также успехов предпринимателей, компаний, и других субъектов экономических отношений, добившихся их правомерным путем⁴.

Использование специальных познаний экспертов-бухгалтеров в судебно-следственной практике позволяет в полной мере установить и оценить признаки искажений экономической информации, определить и количественно измерить возникшие в результате этого негативные экономические явления и ситуации, выявить степень их влияния на финансовые результаты деятельности субъекта хозяйствования. Результат исследования поставленных на разрешение судебно-бухгалтерской экспертизы вопросов подтверждается письменными доказательствами и заключением эксперта.

Как самостоятельный источник доказательств судебно-бухгалтерская экспертиза использует средства экономического анализа исходных данных, содержащихся в доказательствах, приобщенных к делу. Следователь, судья, рассматривая дела о хищениях, налоговых правонарушениях, споры экономического характера, исследует финансовые учетные документы, поэтому им необходимо знание методов исследования экономических, финансовых данных бухгалтерского учета. Без этого

³Тимошенко В. Уголовная ответственность юридических лиц: быть или не быть. Гарант.ру портал), 2015 ресурс]. (информационно-правовой [Электронный доступа: <http://www.garant.ru/article/621968/>, свободный. Загл. с экрана.

⁴Методика анализа и оценки инвестиционной привлекательности организаций / Бухучет в сельском хозяйстве. 2015. - № 2. С. 76-86.

невозможно самостоятельно проводить работу по расследованию преступлений и контролировать полноту и всесторонность исследования материалов дела, осуществляемого экспертом. На практике зачастую следователи, расследующие экономические преступления, не обладают минимальными экономическими знаниями. Проведение экспертизы должно происходить в соответствии с уголовно процессуальным законодательством и иными нормативными актами и не должно нарушать прав участников процесса, так как доказательства, полученные с нарушением закона, признаются не имеющими юридической силы и не могут быть положены в основу обвинения, а также использоваться для доказывания обстоятельств по уголовному делу. Заключение эксперта, так же, как и любое другое доказательство, не имеет заранее установленной силы и должно оцениваться в совокупности с иными доказательствами.

В юридической литературе справедливо отмечается, что «как другие источники доказательств, экспертиза является процессуальным источником сведений о фактах, имеющих значение для дела». Более того, в Уголовно-процессуальном кодексе Российской Федерации также указано, что доказательствами по уголовному делу являются любые фактические данные, на основе которых следователь или суд определяют наличие или отсутствие общественно опасного деяния, степень вины лица, совершившего это деяние, и иные обстоятельства, имеющие значение для правильного разрешения дела. Эти данные устанавливаются показаниями свидетеля, потерпевшего, подозреваемого, обвиняемого, заключением эксперта, протоколами следственных и судебных действий и иными документами. Поэтому познания эксперта-бухгалтера по своему содержанию не ограничиваются только лишь учетно-экономическими, а представляют собой более широкие экономико-правовые и другие знания⁵.

Из этого можно сделать вывод о том, что значительную помощь эксперты-бухгалтеры оказывают органам следствия и суду и в выполнении ими задач по профилактике и предупреждению экономических преступлений. В этих целях, проводя судебно-бухгалтерские экспертизы по расследуемым или рассматриваемым делам, эксперты указывают в своих заключениях меры, которые следует принять, чтобы устранить имеющиеся в учете и контроле недостатки и условия, способствовавшие совершению преступлений.

Кроме того, население должно осознавать реальность наказания за совершенные экономические преступления. Таким образом, в борьбе с экономической преступностью выделяют две группы взаимосвязанных проблем. С одной стороны, это обеспечение защиты бизнеса от преступных посягательств и от неправомерной и неразумной деятельности государственных институтов. С другой стороны, в защите от неэффективного и криминального бизнеса нуждаются отдельные граждане, государственные институты и государство в целом⁶.

Предупреждением экономических преступлений занимаются правоохранительные органы (МВД, прокуратура, ФСБ), они способны принимать меры, попадающие в рамки их компетенции на различных стадиях экономических правонарушений. Стоит отметить то, что органам внутренних дел отводится наиболее важное место в системе структур, занимающихся расследованием преступлений в сфере экономики, так как в МВД имеются специализированные подразделения по борьбе с экономическими преступлениями. Деятельность этих подразделений направлена: на выявление

⁵Алибеков, Ш. И. Судебно-бухгалтерская экспертиза: практическое пособие / Ш. И. Алибеков. – Москва: Юстицинформ, 2006.

⁶Экономические преступления : учебное пособие / Н. Г. Вольдимарова ; Гос. образовательное учреждение высш. проф. образования "Российская правовая акад. М-ва юстиции Российской Федерации. - Москва : ГОУ ВПО РПА Минюста России, 2007. - 177 с.; 21 см.; ISBN 978-5-89172-105-0

причин и условий совершения преступлений в сфере экономики; информирование органов государственной власти, органов местного самоуправления, собственников имущества о необходимости устранения причин и условий, способствующих совершению преступлений экономической направленности; проведение оперативно-розыскных мероприятий по выявлению лиц, занимающихся приготовлением к преступлению и покушением на преступление в сфере экономики, и принятие к ним соответствующих мер предупреждения и пресечения; выявление и разоблачение организованных преступных групп, действующих в сфере экономики. Длительный процесс противозаконных, криминальных действий в сфере экономики нуждается в изменении законодательства. Корректировка действий правоохранительных органов и программы федерального уровня по борьбе с криминальными действиями, затрагивающими экономику, – необходима. С помощью грамотной расстановки в вышеуказанных моментах возможно сокращение преступлений в экономике до минимальных значений. Опирайтесь на старые правовые акты, правовые формы не стоит. Время идет, а, соответственно, законы должны идти в ногу со временем. Нужны комплексные специальные законы, которые в дальнейшем будут развиваться, совершенствоваться, дополняться. В случае с экономическими преступлениями нужно постоянно искать новые пути расследования данных видов преступления, ведь динамика совершения этих преступлений растет, можно сказать, ежеминутно, а следовательно мошенники находят новые пути обхождения преград в совершении противозаконных действий⁷.

Итак, обсуждаемая тема "Профилактика и предупреждение экономических преступлений" является крайне актуальной в современном обществе. Ведь экономическая безопасность общества напрямую зависит от количества совершенных преступлений экономической направленности. Для их профилактики требуется разработать ряд мер, включающий в себя, как государственный уровень, так и уровень предприятий и отдельных граждан. Так как в настоящее время профилактика экономических преступлений не совсем развита в правоохранительных органах, её нужно совершенствовать под существующие разновидности мошеннических действий. Нужно усилить осуществление профилактики с прокурорской стороны, с позиции правоохранительных органов также необходимо улучшение работы по направлению профилактики в области экономических преступлений, а также сплоченная работа всех силовых структур, нацеленная на результат, уменьшение уровня экономической преступности.

Список использованных источников:

1. Волынский А.Ф., Лапин В.О. Расследование экономических преступлений. Учебное пособие. - М.: Академия экономической безопасности МВД России, 2011 -124 с. 2.
2. Бабанская Л.С., Сулейманов Р.А. Теневые процессы в экономике / Взаимодействие науки и бизнеса. Сборник научных статей по материалам международной научно-практической конференции. Лаборатория прикладных экономических исследований имени Кейнса. - 2015, С.12-15. |
3. Миронцева А.В. Миронцев Р.Н. Приватизация в России: перезагрузка / Финансовая аналитика: | проблемы и решения. - 2015. - № 28 (262). - С. 30-38. Вакула А.И., Земельное право, учебное пособие / Донской государственный технический университет. Ростов-на-Дону, 2016 г., с. 182.

⁷Алиев В.М. Современные тенденции в распространении экономической преступности // Безопасность бизнеса. –г. Москва 2018. – № 3.

4. Тимошенко В. Уголовная ответственность юридических лиц: быть или не быть. Гарант.ру портал), 2015 ресурс]. (информационно-правовой [Электронный доступа: <http://www.garant.ru/article/621968/>, свободный. Загл. с экрана.

5. Методика анализа и оценки инвестиционной привлекательности организаций / Бухучет в сельском хозяйстве. 2015. - № 2. С. 76-86.

6. Экономические преступления : учебное пособие / Н. Г. Вольдимарова ; Гос. образовательное учреждение высш. проф. образования "Российская правовая акад. М-ва юстиции Российской Федерации. - Москва : ГОУ ВПО РПА Минюста России, 2007. - 177 с.; 21 см.; ISBN 978-5-89172-105-07

7. Алиев В.М. Современные тенденции в распространении экономической преступности // Безопасность бизнеса. – г. Москва 2018. – № 3.

ПОДХОДЫ К ОЦЕНКЕ ПРОДОВОЛЬСТВЕННОЙ НЕЗАВИСИМОСТИ РЕГИОНОВ
APPROACHES TO ASSESSING FOOD INDEPENDENCE OF REGIONS

Стельмах Елена Викторовна

Институт комплексного анализа региональных проблем ДВО РАН,
ул. Шолом-Алейхема 4, г. Биробиджан, 679016,

e-mail: stelmahlena69@mail.ru

Stelmakh Elena V.

INSTITUTE FOR COMPLEX ANALYSIS OF REGIONAL PROBLEMS FAR EASTERN
BRANCH RUSSIAN ACADEMY OF SCIENCES (ICARP FEB RAS)

4 Sholom-AleikhemSt. Birobidzhan 679016, Russia

Аннотация: В статье рассматривается авторский подход к категорированию показателей продовольственной независимости для территории регионов. Определяется, что для объективной оценки показателя самообеспечения продукцией собственного производства необходимо оценивать именно уровень продовольственной зависимости, который выражается в процентном показателе доли произведенного товара от значения индикатора. Вводится определение продовольственной зависимости - как доля отечественной сельскохозяйственной продукции, сырья и продовольствия, выраженная в процентах, которая необходима субъекту для достижения показателей индикаторов Доктрины продовольственной безопасности, проводится категорирование уровней продовольственной зависимости по товарным позициям Доктрины продовольственной безопасности. Обосновывается разработка шкалы и матрицы продовольственной зависимости, которые могут выступать в качестве шаблона при оценке показателей собственного производства для всех субъектов Российской Федерации, что позволит обеспечить полную независимость от экономических санкций.

Ключевые слова: продовольственная независимость, самообеспечение категорирование, индикаторы, регион, шкала продовольственной зависимости.

Abstract: The article discusses the author's approach to categorizing indicators of food independence for regional territories. It is determined that in order to objectively assess the indicator of self-sufficiency in self-produced products, it is necessary to evaluate precisely the level of food dependence, which is expressed as a percentage of the share of produced goods from the indicator value. A definition of food dependence is introduced - as the share of domestic agricultural products, raw materials and food, expressed as a percentage, which is necessary for a subject to achieve the indicators of the Food Security Doctrine; the levels of food dependence are categorized according to the product positions of the Food Security Doctrine. The development of a scale and matrix of food dependence is substantiated, which can act as a template when assessing indicators of own production for all subjects of the Russian Federation.

Keywords: food independence, self-sufficiency, categorization, indicators, region, food dependence scale.

Введение

Решение вопросов продовольственной безопасности является актуальным в связи с современным состоянием политических отношений России с недружественными странами, следствием которых выступают экономические санкции.

Доктрина продовольственной безопасности определяет продовольственную безопасность как самостоятельный структурный элемент [4]. Для экономической оценки продовольственной безопасности отмечается достаточно большое количество методов и моделей [3,5,9,11]. Однако, следует отметить, что существующие методики слабо интегрируются в процесс оценки продовольственной безопасности территорий на региональном уровне, для оценки самообеспечения административно-территориальных единиц, которые в Российской Федерации представлены субъектами. Климатические и почвенные условия субъектов характеризуются региональными

природными особенностями, поэтому оценка их продовольственной безопасности по единой методике представляется некорректной. Следовательно, возникает необходимость разработки подходов оценки продовольственной независимости для территорий регионального уровня.

На сегодняшний день большинство моделей применимы, для анализа продовольственной безопасности на государственном или международном уровне [3,7]. Отсутствует система комплексного прогнозирования и планирования в АПК [1]. Наиболее приемлемым вариантом оценки продовольственной безопасности, на региональном уровне считаем методику Антамошкиной Е.Н., которая предусматривает оценку региональной продовольственной безопасности через оценку уровня продовольственной самообеспеченности региона, уровня удовлетворения физиологическими потребностями населения и уровня экономической доступности продовольствия [2].

Объекты и методы исследований

При оценке показателей производства сельскохозяйственной продукции используются данные Федеральной службы государственной статистики. Основу статистической выборки составили статистические данные с 2005 по 2021 года. Для рассмотрения данных по производству продукции сельского хозяйства используются показатели для хозяйств, всех категорий, в фактически действовавших ценах, за обозначенный период. При расчёте показателей по фактическому производству сельскохозяйственной продукции и необходимому количеству товаров автор опирается на показатели-индикаторы, которые определяются Доктриной продовольственной безопасности Российской Федерации. При решении поставленных задач используется экономико-статистический метод, метод анализа и синтеза. При разработке шкалы продовольственной зависимости используется метод категорирования индикатора производства для 5 групп товарных позиций.

Результаты и их обсуждение

По мнению автора, для объективной оценки уровня самообеспечения необходимо оценивать именно то количество продовольствия, которого не хватает региону. То есть, нужно рассматривать показатели продовольственной зависимости. Рассмотрим данный подход для территории Еврейской автономной области. В таблице 1 показана динамика производства сельскохозяйственной продукции на территории области с 2005 по 2021 года [6,7,8,].

Таблица 1

Производство сельскохозяйственной продукции
в Еврейской автономной области за 2005 -2021 гг.

Table 1

Товар (тыс. тонн)	Период						
	2005	2016	2017	2018	2019	2020	2021
Зерно	22,4	8,9	11,1	9,6	5,4	8,8	7,0
Скот и птица на убой	<u>2,5 -18%</u> 13,7	<u>1,6 - 14%</u> 11,4	<u>1,3- 11%</u> 11,8	<u>1,4 -12 %</u> 11,7	<u>2,1 - 18 %</u> 11,5	<u>1,2 -10 %</u> 11,4	<u>0,9 - 8 %</u> 11,0
Картофель	<u>112,6- 662%</u> 17,0	<u>35,9 - 242</u> % 14,6	<u>38,7 - 265</u> % 14, 6	<u>42,1 -292</u> % 14,4	<u>17,9 -126 %</u> 14,2	<u>34,6 -247 %</u> 14,0	<u>32,0 -230 %</u> 13,9
Молоко	<u>24,2 -39%</u> 61,3	<u>8,9 - 16 %</u> 53,4	<u>9,4 - 18 %</u> 52,6	<u>9,1- 17 %</u> 52,0	<u>9,3 - 18 %</u> 51,4	<u>9,4 - 18 %</u> 50, 8	<u>9,5 - 19 %</u> 50, 0
Яйцо (тыс.шт)	<u>19,3 - 39%</u> 49,0	<u>16,5- 38</u> % 42,7	<u>14,2-34 %</u> 42,1	<u>13,0 -31</u> % 41,6	<u>9,7 -23 %</u> 41,2	<u>12,8 - 31 %</u> 40,7	<u>12,7 - 32 %</u> 40,0
Плоды и ягоды	<u>2,7 - 14,3%</u> 18,8	<u>1,4 - 8,5</u> % %	<u>1,0 - 6,2</u> % %	<u>1,4 -8,7</u> % %	<u>1,2 -8%</u> 15,8	<u>1,7 -11%</u> 15,7	<u>1,3 -8%</u> 15,4

		16,4	16,2	16,0			
Овощи	<u>33,6- 127%</u> 26,4	<u>17,5 - 76</u> %	<u>15,1 - 70</u> %	<u>14,5 - 65</u> %	<u>7,4 - 33 %</u> 22,2	<u>9,3 - 42 %</u> 21,9	<u>9,34 - 43 %</u> 21,6
Численность населения (тыс. человек)	188,7	164,2	153,6	159,9	158,3	156,5	154,0

Agricultural production in the Jewish Autonomous Region for 2005 -2021

В числителе указывается то количество продукции, которое было произведено, в знаменателе приводится необходимое значение, с учетом численности населения и рекомендуемых норм рационального питания. Далее, на основе расчёта разницы между индикатором и количеством произведённой продукции, рассчитаем недостающие показатели по товарным позициям. Результаты расчётов отражает таблица 2. По товарной позиции зерно расчёт не проводится, поскольку в чистом виде оно не употребляется в пищу и не присутствует в рекомендуемых нормах потребления. Товарная позиция - яйцо вообще отсутствует в Доктрине продовольственной безопасности. Курсивом, со знаком плюс, приводятся значения продуктов, производство которых имеет избыточное значение. Остальные значения отражают недостающее количество товара. Из таблицы мы чётко видим, что показатели продовольственной зависимости с 2005 по 2021 года увеличились по продукции животноводства, соответственно - скот и птица на убой и молоко. По картофелю, несмотря на его сохраняющееся общее перепроизводство в 2021 году, мы видим общее падение самообеспеченности до 135 %. По овощам область зависит на 47 % и эта зависимость выросла с 2005 года. По плодам и ягодам также отмечается рост зависимости до 47 %, хотя в 2005 году отмечается перепроизводство этого товара.

Таблица 2

Показатели продовольственной зависимости Еврейской автономной области с 2005 по 2021 гг.

Table 2

Indicators of food dependence of the Jewish Autonomous Region from 2005 to 2021

Товар (тыс. тонн)	Период						
	2005	2016	2017	2018	2019	2020	2021
Скот и птица на убой	67 %	71 %	74 %	73 %	74%	75 %	77 %
Картофель	+ 567 %	+ 147 %	+170 %	+ 197 %	+ 31 %	+ 152 %	+ 135 %
Молоко	51 %	74 %	82 %	73 %	71 %	82 %	71 %
Плоды и ягоды	46 %	51%	54 %	51%	52 %	49 %	52 %
Овощи	+ 37 %	14 %	20 %	25 %	57 %	48 %	47 %
Численность населения (тыс. человек)	188,7	164,2	162,0	159,9	158,3	156,5	154,0

В целом, обладая достаточными посевными площадями [10], область характеризуется продовольственной зависимостью по всем индикаторам, кроме картофеля.

Следует отметить, что применение подхода к оценке продовольственной безопасности, именно через недостающее количество собственно произведенной сельскохозяйственной продукции, наиболее объективно характеризует данную категорию, поскольку демонстрирует динамику зависимости региона от внешних поставок. Кроме того, мы видим конкретный количественный показатель, отражающий рост продовольственной зависимости субъекта, что исключает возможность

цифровых коллизий при отражении результатов производства. Соответственно для продовольственной зависимости можно сформулировать следующее определение:

Продовольственная зависимость - это доля отечественной сельскохозяйственной продукции, сырья и продовольствия, выраженная в процентах, которая необходима субъекту для достижения показателей индикаторов Доктрины продовольственной безопасности.

Далее, на основе категорирования доли произведённого товара от показателя индикатора, предлагаем три уровня продовольственной зависимости для товарных позиций - высокий, средний и низкий. Для каждого уровня вводится буквенное обозначение, соответственно - В, С и Н. Например, доля недостающего молока составляет 51 %, что соответствует среднему уровню зависимости, а вот доля недостающего мяса в 71 % соответствует высокому уровню продовольственной зависимости.

Таблица 3

Шкала продовольственной зависимости

Table 3

Наименование товара	Уровни продовольственной зависимости субъекта			
	Высокий В	Средний С	Низкий Н	Индикатор производства
1. Зерно	65-95	33-64	1-32	не менее 95%
2. Картофель				
3. Сахар	62-90	31-61	1-30	не менее 90%
4. Растительное масло				
5. Молоко и молокопродукты				
6. Овощи и бахчевые	58-85	29-57	1-28	не менее 85%
7. Мясо и мясопродукты				
8. Рыбодукты				
9. Соль поваренная	52-75	26-51	1-25	не менее 75%
10. Семена основных сельхоз. культур отечественной селекции				
11. Фрукты и ягоды	42-60	21-41	1-20	не менее 60%

Товарные позиции структурированы в соответствии с процентным показателем для индикатора из Доктрины. Категорирование по перепроизводству требует доработки, поэтому на данный момент по картофелю и овощам (на 2005 год) предлагается ввести обозначение П - перепроизводство. Итогом такого категорирования выступает рабочий вариант матрицы продовольственной зависимости субъекта, пример которой отражает таблица 4. Показатели продовольственной обеспеченности, которые отражают недостаток сельскохозяйственной продукции на основе шкалы продовольственной зависимости, наиболее объективно отражают ситуацию в регионе. Чётко просматривается необходимость внешних поставок продовольствия, как из других регионов Российской Федерации, так и из-за границы, что в условиях экономических санкций существенно влияет не только на цену продукции, но и на возможность её фактической доставки.

Таблица 4

Матрица продовольственной зависимости Еврейской автономной области с 2005 по 2021 гг.

Table 4

Matrix of food dependence of the Jewish Autonomous Region from 2005 to 2021

	Период						
	2005	2016	2017	2018	2019	2020	2021
Говар (тыс. тонн)							
Скот и птица на убой	В	В	В	В	В	В	В
Картофель	<i>П</i>						
Молоко	Н	В	В	В	В	В	В
Плоды и ягоды	В	В	В	В	В	В	В
Овощи	<i>П</i>	Н	Н	Н	С	С	С
Численность населения (тыс. человек)	188,7	164,2	62,0	159,9	158,3	156,5	154,0

Заключение

Таким образом, можно сделать вывод - оценка продовольственной независимости региона должна проводиться на основе объективных показателей, характеризующих процентный показатель недостающего количества сельскохозяйственной продукции собственного производства. Считаем необходимым одновременное проведение мониторинга пахотного фонда и оценки по шкале продовольственной зависимости территорий всех субъектов Российской Федерации, что позволит определить оптимальные направления сельскохозяйственного землепользования для повышения уровня продовольственной независимости.

Список использованных источников:

1. Алтухов А.И. Основные мировые тенденции в обеспечении продовольственной безопасности // Вестник национального института бизнеса. 2022. № 1 (45). С.9-19.
2. Антамошкина Е.Н. Методика анализа продовольственной безопасности на макрорегиональном уровне // Национальные интересы: приоритеты и безопасность. 2015. С. 25- 34.
3. Кошелев В.М., Приемко В.В. О продовольственной независимости и её показателях // Экономика сельского хозяйства России. 2014. № 12. С.32-39
4. Об утверждении Доктрины продовольственной безопасности Российской Федерации: указ Президента РФ от 21.01.2020 № 20 // Собрание законодательства РФ. 2020. № 4. Ст. 345.
5. Оболенцев И.А., Корнилов М.Я., Синюков М.И. Продовольственная безопасность России: еще один взгляд на проблему. М.: Изд-во РАГС, 2006, 218 с.
6. Регионы России. Социально-экономические показатели. 2019. URL: https://rosstat.gov.ru/bgd/regl/b19_01/Main.htm. (дата обращения: 10.02.2024).
7. Регионы России. Социально-экономические показатели. 2022: URL: https://rosstat.gov.ru/storage/mediabank/Region_Pokaz_2022.pdf. (дата обращения: 12.01.2024).
8. Социально-экономические характеристики г. Биробиджан и районов ЕАО Стат. Сб. / Комстат ЕАО 2001 г.- 143 С.
9. Стельмах Е.В. Правовые аспекты продовольственной независимости субъектов Российской Федерации. Финансовый бизнес. 2022. № 10. Ч.2. С.130-134.
10. Стельмах Е.В., Комарова Т.М., Соловченков С.А. Посевные площади как фактор формирования продовольственной независимости Еврейской автономной области. [Siberian Journal of Life Sciences and Agriculture](#). 2023. Т. 15. № 1. С. 164-178.
11. Таранов П.М. Модель двухкритериального анализа российского продовольственного рынка: конкурентоспособность и продовольственная безопасность // Аграрный научный журнал. 2011. № 8. С. 91-94.

REFERENCES:

1. Altuhov A.I. Osnovnye mirovye tendencii v obespechenii prodovol'stvennoj bezopasnosti // Vestnik nacional'nogo instituta biznesa. 2022. № 1 (45). S.9-19.
2. Antamoshkina E.N. Metodika analiza prodovol'stvennoj bezopasnosti na makroregional'nom urovne // Nacional'nye interesy: priority i bezopasnost'. 2015. S. 25- 34.
3. Koshelev V.M., Priemko V.V. O prodovol'stvennoj nezavisimosti i eyo pokazatelyah // Ekonomika sel'skogo hozyajstva Rossii. 2014. № 12. S.32-39
4. Ob utverzhdenii Doktriny prodovol'stvennoj bezopasnosti Rossijskoj Federacii: ukaz Prezidenta RF ot 21.01.2020 № 20 // Sobranie zakonodatel'stva RF. 2020. № 4. St. 345.
5. Obolencev I.A., Kornilov M.YA., Sinyukov M.I. Prodovol'stvennaya bezopasnost' Rossii: eshche odin vzglyad na problemu. M.: Izd-vo RAGS,2006, 218 s.
6. Regiony Rossii. Social'no-ekonomicheskie pokazateli. 2019. URL: https://rosstat.gov.ru/bgd/regl/b19_01/Main.htm. (data obrashcheniya: 10.02.2024).
7. Regiony Rossii. Social'no-ekonomicheskie pokazateli. 2022: URL: https://rosstat.gov.ru/storage/mediabank/Region_Pokaz_2022.pdf. (data obrashcheniya: 12.01.2024).
8. Social'no-ekonomicheskie harakteristiki g. Birobidzhan i rajonov EAO Stat. Sb. / Komstat EAO 2001 g.- 143 S.
9. Stel'mah E.V. Pravovye aspekty prodovol'stvennoj nezavisimosti sub"ektov Rossijskoj Federacii. Finansovyy biznes. 2022. № 10. CH.2. S.130-134.
10. Stel'mah E.V., Komarova T.M., Solovchenkov S.A.Posevnye ploschadi kak faktor formirovaniya prodovol'stvennoj nezavisimosti Evrejskoj avtonomnoj oblasti. Siberian Journal of Life Sciences and Agriculture. 2023. T. 15. № 1. S. 164-178.
11. Taranov P.M. Model' dvuhkriterial'nogo analiza rossijskogo prodovol'stvennogo rynka: konkurentosposobnost' i prodovol'stvennaya bezopasnost' // Agrarnyy nauchnyj zhurnal. 2011. № 8. S. 91-94.

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СУДЕБНОЙ СИСТЕМЕ РОССИЙСКОЙ ФЕДЕРАЦИИ ДЛЯ БЕЗОПАСНОСТИ ПРАВ ГРАЖДАН
PROBLEMS OF LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE IN THE JUDICIAL SYSTEM OF THE RUSSIAN FEDERATION FOR THE SECURITY OF CITIZENS' RIGHTS

Я.В. Точасов

Колледж Ростовского Института (филиал) ВГУЮ (РПА Минюста России), Россия, 344000, г. Ростов-на-Дону, ул. 31 линия 4/19, email: tochasov_yaroslav@mail.ru

Y.V. Tochasov

College of the Rostov Institute (branch) VGUY (RPA of the Ministry of Justice of Russia), Rostov-on-Don, 31 line 4/19, Rostov-on-Don , 344000, Russia, email: tochasov_yaroslav@mail.ru

Аннотация: Исследуется актуальная тема внедрения и использования искусственного интеллекта в юридической практике. Проводится анализ значимости использования ИИ в судебной системе с учетом обеспечения прав граждан на территории России. Обсуждаются как позитивные стороны внедрения технологий ИИ, так и потенциальные проблемы, касающиеся этических, юридических и социальных аспектов использования искусственного интеллекта в судопроизводстве. Статья обращает внимание на необходимость правового регулирования процессов принятия решений на основе ИИ, учитывая прозрачность алгоритмов, ответственность за ошибки и обеспечение конфиденциальности персональных данных граждан. Предлагаются возможные пути решения проблем, связанных с использованием искусственного интеллекта в судебной системе, через разработку четких норм и стандартов, способствующих балансу между развитием технологий и соблюдением правовых принципов.

Ключевые слова: Искусственный интеллект, судебная система, преимущества, проблемы, законодательство

Abstract: The current topic of the introduction and use of artificial intelligence in legal practice is highlighted. The authors analyze the importance of using AI in the judicial system, taking into account ensuring the rights of citizens in Russia. Both the positive aspects of the introduction of AI technologies and potential problems related to the ethical, legal and social aspects of the use of artificial intelligence in legal proceedings are discussed. The article draws attention to the need for legal regulation of AI-based decision-making processes, taking into account the transparency of algorithms, responsibility for errors and ensuring the confidentiality of personal data of citizens. Possible solutions to the problems associated with the use of artificial intelligence in the judicial system are proposed through the development of clear norms and standards that promote a balance between the development of technology and compliance with legal principles.

Keywords: Artificial intelligence, judicial system, advantages, problems, legislation

Введение

Робототехника и искусственный интеллект стали одной из самых известных и активно обсуждаемых технологических тенденций нашего века [1]. Искусственный интеллект (далее – ИИ) является главной технологией XXI века, которой охвачены все развитые государства мира. Так, более 37 стран к настоящему времени разработали национальные стратегии развития ИИ [2]. В нашей стране принят Указ Президента РФ «О развитии искусственного интеллекта в Российской Федерации» [3]. Поэтому сам факт появления этого документа в нашей стране, подтверждает заинтересованность государства в технологическом развитии нашего общества, необходимость внедрения технологий нейронных сетей в различные области общественных отношений.

Стоит отметить, что ИИ может быть также полезен для судебной системы и развития юстиции России. С увеличением объема информации и сложности юридических вопросов, применение

современных технологий в судебных процессах может значительно улучшить эффективность и точность принятия решений.

Преимущества нейронных сетей, для судов и юстиции, заключается в том, что они на данный момент могут распознавать информацию по заданным параметрам и использовать алгоритмы машинного обучения для повышения скорости работы юристов. Их способность пропускать через себя и систематизировать огромные массивы информации может также помочь юристу повысить качество работы [4].

Вместе с положительными эффектами внедрения ИИ в судебную систему существуют проблемы и опасности внедрения данной методики. Использование искусственного интеллекта в судебной системе может привести к нарушению прав граждан по ряду причин. Во-первых, алгоритмы машинного обучения могут быть подвержены предвзятости и дискриминации, основанными на неполных или пристрастных данных, что может привести к несправедливым решениям. Недостаточная прозрачность и объяснимость работы таких систем также могут создать проблемы, так как граждане не всегда могут понять принятые решения или их обоснование.

Кроме того, использование ИИ в судебной системе может создать уязвимости для кибератак и манипуляций, что может привести к утечке конфиденциальной информации или подделке доказательств. Также возникает вопрос о том, кто несет ответственность за ошибочные решения, принятые на основе данных, обработанных алгоритмами ИИ.

Еще одной проблемой может стать потенциальная угроза приватности граждан, поскольку использование ИИ в судебных процессах может включать обширный сбор и анализ персональных данных. Это может привести к нарушению права на конфиденциальность информации и угрозе личной безопасности.

Таким образом, использование систем ИИ в судебной системе представляет собой сложную задачу, требующую тщательного анализа и разработки соответствующих нормативно-правовых актов по обеспечению безопасности прав граждан.

Цель исследования – цель данного исследования заключается в выявлении основных проблем правового регулирования применения искусственного интеллекта в судебной системе России с целью обеспечения безопасности и защиты прав граждан. Анализируя существующие нормативные акты и практику использования ИИ в судопроизводстве, исследование направлено на выявление потенциальных угроз для прав граждан, связанных с использованием алгоритмов машинного обучения, проблемы прозрачности и объяснимости решений, а также возможных нарушений конфиденциальности и безопасности данных.

Материалы и методы исследования. Изучение мирового и российского законодательства помогло определить проблемы правового регулирования ИИ в судебной системе России. Необходимо отметить, что в Российской Федерации нормативно-правовой базы именно в области использования машинного интеллекта в судебной системе нет.

Объектом исследования является законодательство Российской Федерации по регулированию вопросов ИИ.

Предметом исследования является правовое регулирование вопросов ИИ в судебной системе.

В написания данной статьи было проведён анализ научной литературы, публицистических статей, касающихся использования ИИ в судебной системе, а также проблем его правового регулирования. Также были изучены нормативно-правовые акты России и Европейского Союза, в которых осуществляется правовое регулирование машинного интеллекта, а также его использования в судебной системе, что значительно помогло определить его проблемы.

Результаты исследования и их обсуждения. Судебная система является фундаментальной составляющей любого правового государства. Её развитие напрямую влияет на общественную стабильность и доверие к правосудию. Современный мир сталкивается с огромными вызовами, требующими инновационных подходов к судопроизводству. Машинный интеллект предлагает уникальные возможности для модернизации и повышения эффективности судопроизводства.

Согласно Указа Президента РФ «О развитии искусственного интеллекта в Российской Федерации» «ИИ – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при

выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их» [3].

Использование ИИ в судебной системе может значительно сократить затраты времени и ресурсов, ускоряя процессы судопроизводства и снижая потребность в человеческом труде. Применение машинного интеллекта позволяет значительно ускорить процесс рассмотрения дел. Автоматизация рутинных задач, таких как обработка документов и поиск релевантной информации, освобождает время судей для более сложных и творческих задач.

Также ИИ способен обрабатывать большие объемы данных и выявлять скрытые закономерности, что помогает судьям принимать более обоснованные решения. Например, системы машинного обучения могут анализировать исторические данные о судебных делах и предсказывать вероятность исхода нового дела.

Важно обратить внимание на то, что использование ИИ повышает эффективность судебной системы. Автоматизация процессов и уменьшение времени на рассмотрение дел позволяют увеличить количество рассматриваемых дел без увеличения нагрузки на судей.

Наконец, применение ИИ может улучшить качество правосудия. Благодаря автоматизации процессов и использованию больших объемов данных, ИИ может помочь устранить субъективность и предвзятость в принятии решений.

Исходя из всего вышеуказанного следует вывод о том, что использование ИИ в судебной системе России имеет множество преимуществ, включая ускорение процессов, повышение эффективности и улучшение качества правосудия.

Например, нейронная сеть может применяться как помощник юристу для протоколирования судебных заседаний. Для примера можно привести Ростовскую область. Внедрение ИИ обсуждалось на заседании правительства Ростовской области, которое, 13 декабря 2023 года, вел, губернатор области Василий Голубев, рассматривался вопрос о достижении «цифровой зрелости» в ключевых секторах экономики, социальной сфере и государственном управлении к 2023 году. Минцифры области сообщили, что в 2023 году был успешно протестирован пилотный проект по использованию ИИ в департаменте мировых судей и в 2024 году он будет внедрен на всех 230 участках. Компьютерный интеллект поможет выполнять большой объём несложной работы, в частности – формировать протоколы заседаний [5].

Решение правительства Ростовской области по использованию ИИ в протоколировании судебных заседаний улучшит эффективность работы судов, повысит прозрачность и доступность судебных решений, а также поможет сократить затраты на процессы судопроизводства. Это в свою очередь приведет к усилению доверия граждан к судебной системе и улучшению правосудия в целом.

В данной теме нельзя обойти вопрос возможности в будущем заменить живого судью на ИИ. В последние годы в правоведческой среде все чаще обсуждается вопрос о том, можно ли автоматизировать весь процесс отправления правосудия, т.е. заменить судью нейронной сетью, которая будет способна на основе представленных доказательств и фактических обстоятельств дела, выносить соответствующее решение, и таким образом осуществлять «электронное правосудие» [6]. Важно отметить, что для осуществления такого правосудия необходимо создавать законы.

Формирование нормативно-правовой базы в области использования ИИ в судебной системе является важным фактором для обеспечения эффективности, прозрачности и справедливости судебных процессов. Она определяет правила игры, гарантирует защиту прав граждан и устанавливает стандарты для применения нейронных сетей в судебной практике. Попытки формирования такой базы в этой области предпринимаются как на уровне отдельных государств, так и на региональных и международных уровнях. Особенно выделяется деятельность Европейского союза в этой области [7].

В декабре 2018 года был принят первый международный документ, который целиком посвящен применению искусственного интеллекта в сфере правосудия. Этот документ называется "Европейская этическая хартия о применении искусственного интеллекта в судебных системах". Его утвердила Европейская комиссия по эффективности правосудия, которая входит в состав Совета Европы. В Хартии сформулированы пять принципов применения искусственного интеллекта:

1. «Принцип соблюдения основных прав». Данный принцип обеспечивает создание и использование средств и сервисов, базирующихся на искусственном интеллекте, отвечающих фундаментальным правам человека

2. «Принцип недискриминации». Смысл этого принципа заключается в том, что при использовании методов обработки данных, которые могут привести к группировке или классификации отдельных лиц или групп лиц, государственные и частные участники должны убедиться, что эти методы не способствуют дискриминации и не допускают бесконтекстного анализа или использования данных.

3. «Принцип качества и безопасности». Этот принцип закрепляет, что обработка судебных решений и данных должна осуществляться с использованием сертифицированных источников и нематериальных данных, применяя модели, разработанные на междисциплинарной основе, в безопасной технологической среде.

4. «Принцип прозрачности, беспристрастности и достоверности». В соответствии с этим принципом методы обработки данных должны быть доступны и понятны, а также должен быть разрешен проведение внешнего аудита.

5. «Принцип контроля пользователем». Согласно этому принципу необходимо отказаться от предписывающего подхода и дать возможность пользователю стать информированным участником, позволяя ему контролировать свой выбор [8].

Доктор юридических наук Бертовский Лев Владимирович в своих научных работах отмечает, что в данной хартии наиболее важным представляется принцип контроля пользователя. В соответствии, с которым, судья человек должен иметь возможность опровергнуть предложение ИИ и принять собственное решение по делу, а участники процесса должны иметь возможность прямого обращения к человеческому суду (состоящего из людей) и оспорить решение, принятое искусственным интеллектом [9].

Основываясь на этом принципе хартии можно предположить, что в будущем машинный интеллект может использоваться только как помощник для судьи. В.В. Момотов, судья Верховного суда РФ, отмечает, что взаимодействие судей и работников аппарата суда с технологией ИИ должно приводить к синергии, при сохранении в таком партнерстве главенствующей роли человека [10].

Сегодня в России нормативно-правовой базы в именно области использования ИИ в судебной системе нет. Но в будущем её можно было сделать по аналогу «Европейской этической хартии о применении искусственного интеллекта в судебных системах». Нормативно правовые акты должны в первую очередь решать ключевые проблемы, возникающие при использовании искусственного интеллекта в судопроизводстве. В рамках данной хотелось бы рассмотреть те самые ключевые проблемы и возможные способы их решения.

Во-первых, хотелось бы рассмотреть проблему недостаточной прозрачности и объяснимости принимаемых решений. Алгоритмы искусственного интеллекта могут быть сложными и непонятными для людей, поэтому недостаточная прозрачность использования ИИ в судебной системе может привести к нарушению прав граждан и подрыву доверия к судебной системе. В частности, судьи и административные органы могут использовать ИИ для принятия решений, которые не подлежат контролю и не могут быть обжалованы. Для решения данной проблемы следует закрепить на законодательном уровне нормы, которые позволят гражданам иметь доступ о том, как работает ИИ в суде, а также иметь возможность обжаловать решение или информации, которую он предоставил судье или же сотрудникам суда.

Использование ИИ в судебной системе также связано с обеспечением информационной безопасности. Судебная система открыла для себя возможность хранения данных на облачных серверах, что расширило пространство для хранения, но также создает риски для утечки персональных данных при их использовании искусственным интеллектом. Это указывает на необходимость создания механизмов защиты от несанкционированного доступа и внесения изменений в электронные документы.

В целом, для решения проблемы безопасности данных при использовании ИИ в судебной системе России необходимо создать правовую основу, которая бы обеспечивала безопасность данных. Это может быть достигнуто через закрепление в законодательстве норм, которые бы

регламентировали использование ИИ в судебной системе, обеспечивали безопасность данных. Также должны быть установлены наказания в Уголовном кодексе Российской Федерации, которые будут регулировать вторжение в базу данных, которые будут использоваться машинным интеллектом.

Также возникает проблема ответственности за ошибки при использовании технологий ИИ в судах. С одной стороны, ответственность за ошибки должны нести разработчики самого машинного интеллекта. Именно они могут допустить ошибки в программных кодах нейронной сети, из-за которых она будет неправильно считывать или предоставлять информацию, а также выносить какое-либо решение. С другой же стороны ошибки, возникающие у ИИ, могут быть и при его неправильном использовании работников суда. Тогда же стоит наказывать уже их, т.к. в данном случае они виноваты в ошибках компьютерного интеллекта. Данные ошибки могут быть ключевыми и нести большую важности в жизни людей.

Для решения проблемы ответственности необходимо закрепить в законодательстве четкие нормы, определяющие ответственность за использование ИИ в судебной системе. В этих нормах должно быть чётко прописано кто и в каких случаях будет нести ответственность за ошибки искусственного интеллекта.

Также в российское законодательство необходимо будет интерпретировать «Принцип недискриминации» и «Принцип контроля пользователем», которые будут препятствовать тому, что ИИ может полностью «захватить» судебную систему.

Заключение

На основе проведённого исследования, можно сказать, что использование ИИ в судебной системе представляет собой как позитивные аспекты, так и потенциальные риски, которые требуют внимательного внедрения и управления. Важно учитывать не только технологические возможности, но и этические, юридические и социальные последствия применения искусственного интеллекта в правовой сфере.

Решение проблем, связанных с использованием ИИ в судебной системе, может быть найдено через правовое регулирование, включающее в себя разработку четких норм и стандартов, регулирующих процессы принятия решений на основе искусственного интеллекта. Необходимо также обеспечить прозрачность алгоритмов, высокую степень ответственности за ошибки и негативные последствия, а также защиту персональных данных граждан при использовании ИИ в судебной деятельности.

Продвижение в области правового регулирования использования искусственного интеллекта в судебной системе поможет обеспечить сбалансированное развитие технологий и правовых норм, повысить доверие общества к судебной системе и защитить права и свободы человека в условиях цифровизации общества.

В заключении можно с уверенностью поддержать высказывание президента РФ В.В. Путина: «Искусственный интеллект становится верным помощником, открывающим новые горизонты для реализации целого ряда задач, которые стоят перед человечеством»[11], и подтвердить, что российская судебная система идет в поступательном режиме в этом направлении.

Список литературы

1. Морхат П. М. Правосубъективность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: специальность 12.00.03 гражданское право; предпринимательское право; семейное право; международное частное право: диссертация на соискание доктора юридических наук / Морхат, М. П.; Российская государственная академия интеллектуальной собственности. Москва, 2018. 420 с.

2. Бушманов Р. В., Накусова, Ф. А. Современные подходы к нормативному определению понятия искусственного интеллекта в Российском праве // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2021. № 10 (137). С. 39-42.

3. Указ Президента РФ от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в РФ»

[Электронный ресурс]. URL: <http://www.kremlin.ru/acts/bank/44731> (дата обращения: 24.04.2024).

4. Мачанский С. Г. Применение искусственного интеллекта в судебной и правоохранительных системах // электронный сборник трудов молодых специалистов Полоцкого государственного университета имени Евфросинии Полоцкой. Юридические науки. 2019. № 27.; URL: https://journals.psu.by/specialists_legal_sciences/article/view/4894 дата обращения: 23.04.2024).

5. Штомплева С.В. В 2024 году искусственный интеллект будет использован в работе мировых судей / [Электронный ресурс] Официальный портал Правительства Ростовской Области : [сайт]. URL: <https://www.donland.ru/news/24923/> (дата обращения: 23.04.2024).

6. Федотова Е. Л., Гончаров Ф. Ю. Использование искусственного интеллекта в судебном процессе // Цифровые технологии в юриспруденции: генезис и перспективы: Материалы I Международной межвузовской научно-практической конференции (Москва, 28 февраля 2020 г.). Красноярск: Издательство Красноярского государственного аграрного университета, 2020. С. 185-193.

7. Марченко А. Ю. Правовой анализ новейшего законодательства ЕС о применении технологий искусственного интеллекта : специальность 12.00.10 «Международное право; Европейское право » : Диссертация на соискание кандидата юридических наук / Марченко, А. Ю. ; Московский государственный институт международных отношений(университет) МИД РФ. — Москва , 2022. — 188 с.

8. «Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях» от 03.12.2018 [Электронный ресурс]. URL: <https://rm.coe.int/rule-of-law-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4> (дата обращения: 24.04.2024).

9. Бертовский Л. В. Суд и искусственный интеллект // Актуальные вопросы производства криминалистических экспертиз и оценки результатов судебно-экспертной деятельности: материалы Всероссийской (национальной) научно-практической конференции. (Красноярск, 1 апреля 2021 г.). Красноярск: Издательство Красноярского государственного аграрного университета, 2021. С. 17-21.

10. Момотов, В. В. Искусственный интеллект в судопроизводстве: состояние, перспективы использования // Вестник Университета имени О. Е. Кутафина. 2021. № 5 (81). С. 188-191.

11. Никольский А. Путин назвал искусственный интеллект основой для нового рывка в развитии человечества / [Электронный ресурс] ТАСС : [сайт]. URL: <https://tass.ru/ekonomika/10172451?ysclid=lvm7ogvaus261121346> (дата обращения: 24.04.2024).

СОДЕРЖАНИЕ

1	Производство молока в регионе в контексте предельного анализа, Алексеева Н.А.	3
2	Состояние мирового рынка пищевой промышленности и его влияние на продовольственную безопасность Казахстана Ахметова А.А., Кожаметова А.Г., Мажитова Б.Б.	7
3	Роль цифровой грамотности в экономическом развитии Казахстана Адай А.С., Кенесова А.М., Тетисбаева Д.Г.	15
4	Организационные изменения сопротивление персонала и методы его преодоления Ашуральнев М.Р.	19
5	Концепции контроллинга в отечественной и зарубежной практике экономического управления на микроуровне Банцевич Е.Е., Козлов А.П.	25
6	Современные кибератаки как угроза информационной безопасности российской федерации Гальцова Л.Е.	35
7	Угрозы информационной безопасности как фактор социальных конфликтов в постиндустриальном обществе Гасангусенова А.М.	39
8	Учетные аспекты обеспечения экономической безопасности Джамалухдинова Н.Х.	43
9	Факторы риска при принятии управленческих решений в период цифровой трансформации экономики РФ Докторова Н.П.	45
10	Обеспечение устойчивого экономического развития сельскохозяйственных организаций на основе совершенствования инфоструктуры Журова И.В.	50
11	Социальная ответственность организации как фактор снижения социально-экономической напряженности в обществе Зиралова Д.	55
12	Защита прав человека в эпоху глобализации и информационных технологий Киселева В.А.	60
13	Влияние элементов системы экономической безопасности на деятельности организации Козлова Е.А., Старовойтова Д.А.	66
14	Внедрение технологий искусственного интеллекта в российскую экономику и их влияния на национальную безопасность Кукульян А.А., Шаронина Л.В.	72
15	Теоретико-методологические подходы к трактовке экономической безопасности организаций промышленности как экономической категории Картель С.А.	76
16	Влияние современных информационных технологий на обеспечение экономической безопасности Козлова Е.А., Васильченко К.В.	83
17	Проблема информационной безопасности в условиях цифровизации общества Магомедов А.А.	88
18	Актуальность инклюзивной занятости в экономике Беларуси Маковская Н.В.	92
19	Проблема формирования ценовых индикаторов на традиционных цифровых	

	рынках РФ и РБ, Мелешкина А.И.	95
20	Эффективная организация бухгалтерского учета как основа обеспечения экономической безопасности субъектов малого бизнеса транспортного сегмента, Мельник А.Г.	100
21	Занятость в реализации цифровых инициатив, Миренкова И.В.	106
22	Риск мониторинг реализации стратегии роста, Миренков А.А.	110
23	Международное сотрудничество в области кибербезопасности проблемы и перспективы, Потеряев В.А.	116
24	Мошенничество с банковскими картами, Пильдунча А.А., Шаронина Л.В.	122
25	Формирование предпринимательских и профессиональных компетенций у специалистов инженерно-экономического и технического профиля при преподавании социально-гуманитарных дисциплин, Пушкин И.А.	127
26	Профилактика и предупреждение экономических преступлений, Серпионов К.С.	132
27	Подходы к оценке продовольственной независимости регионов, Стельмах Е.В.	138
28	Проблемы правового регулирования искусственного интеллекта в судебной системе Российской Федерации для безопасности прав граждан, Точасов.Я.В.	144