Научная статья
УДК 330.1

УГРОЗЫ И РИСКИ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ: КИБЕРБЕЗОПАСНОСТЬ

Раздобарова Марина Николаевна[1], Раздобаров Артем Михайлович[2]

[1] ***ФГБОУ ВО «Саратовский государственный университет генетики, биотехнологии и инженерии имени Н.И. Вавилова», Саратов, Россия***
mar-razdobarova2009@yandex.ru,
https://orcid.org/0000-0003-1257-8443
[2] ***Саратовский государственный технический университет им. Ю.А. Гагарина, Саратов, Россия,***
vanderbullet122177@gmail.com

Аннотация. *В статье исследуется эволюция концепции безопасности в постхолодновоенный период с акцентом на её экономические и цифровые аспекты. Актуальность работы обусловлена трансформацией понимания безопасности: от традиционно военно-политической трактовки к многомерной системе, включающей экономические, социальные, экологические и кибернетические компоненты.*

Цель исследования — проанализировать новые формы угроз и разработать подходы к обеспечению экономической безопасности в условиях цифровизации. В рамках работы систематизированы современные формы безопасности, изучены взаимосвязи традиционных и новых угроз, выявлена специфика киберпреступности как ключевого вызова XXI века, предложена многоуровневая модель угроз (от индивидуального до глобального уровня).

Методология включает системный, сравнительно-правовой и структурно-функциональный анализ. Эмпирическую базу составили правовые акты, кейсы кибератак, данные правоохранительных органов и исследования в области киберправа.

Основные выводы: концепция безопасности стала многомерной; экономическая безопасность — ключевой элемент национальной устойчивости; киберпреступность требует международного сотрудничества и технологической модернизации.

Предложены направления укрепления экономической безопасности: развитие систем раннего предупреждения, повышение цифровой грамотности, создание межгосударственных платформ и инвестирование в киберзащиту критической инфраструктуры.

Ключевые слова: *безопасность, экономическая безопасность, кибербезопасность, угрозы, риски*

Для цитирования: Раздобарова Марина Николаевна, Раздобаров Артем Михайлович УГРОЗЫ И РИСКИ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ: КИБЕРБЕЗОПАСНОСТЬ / Марина Николаевна Раздобарова, Артем Михайлович Раздобаров // Агрофорсайт. 2025. № 6— Саратов: ООО «ЦеСАин»,2025. – 1 электрон. опт. диск (CD-ROM). – Загл. с этикетки диска.

Финансирование: исследование проводилось за счет собственных средств.

THREATS AND RISKS TO ECONOMIC ACTIVITIES: CYBERSECURITY

Marina N. Razdobarova[1] ,Artem M. Razdobarov[2]

[1]***Saratov State University of Genetics, Biotechnology and Engineering named after N.I. Vavilov, Saratov, Russia,***
mar-razdobarova2009@yandex.ru,
https://orcid.org/0000-0003-1257-8443
2Saratov State Technical University named after Yu.A. Gagarin, Saratov, Russia, vanderbullet122177@gmail.com

Abstract. This article examines the evolution of the concept of security in the post-Cold War period, focusing on its economic and digital aspects. The relevance of this work stems from the transformation of the understanding of security: from a traditional military-political interpretation to a multidimensional system incorporating economic, social, environmental, and cybernetic components.

The aim of the study is to analyze new forms of threats and develop approaches to ensuring economic security in the context of digitalization. This work systematizes modern forms of security, examines the interrelations between traditional and new threats, identifies the specifics of cybercrime as a key challenge of the 21st century, and proposes a multi-level threat model (from the individual to the global level).

The methodology includes systemic, comparative legal, and structural-functional analysis. The empirical base consists of legal acts, cyberattack cases, law enforcement data, and research in the field of cyberlaw.

Key findings: the concept of security has become multidimensional; economic security is a key element of national resilience; cybercrime requires international cooperation and technological modernization. Proposed areas for strengthening economic security include developing early warning systems, increasing digital literacy, creating interstate platforms, and investing in the cyber defense of critical infrastructure.

Keywords: security, economic security, cybersecurity, threats, risks

Введение

Актуальность темы обусловлена фундаментальными изменениями в понимании и практиках обеспечения безопасности в современном мире. Традиционная трактовка безопасности как исключительно военно-политической категории уступает место многомерной концепции, охватывающей экономические, социальные, экологические и цифровые аспекты.

В условиях глобализации и цифровой трансформации возникают новые угрозы — от киберпреступности до экономических потрясений, затрагивающих целые регионы. Это требует переосмысления: структуры уровней безопасности (от индивидуального до глобального); механизмов защиты экономических интересов; способов противодействия транснациональным угрозам.

Особую значимость приобретает анализ экономической безопасности, поскольку: экономические факторы напрямую влияют на национальную устойчивость; киберпреступность создаёт системные риски для финансовой инфраструктуры; глобализация усиливает взаимозависимость государств, делая локальные кризисы глобальными.

Научная новизна исследования заключается в:

1. Систематизации современных форм безопасности с учётом постхолодновоенного контекста.
2. Комплексном анализе взаимосвязи между традиционными (военно-политическими) и новыми (цифровыми, экономическими) угрозами.
3. Выявлении специфики киберпреступности как ключевого вызова экономической безопасности в XXI веке.
4. Предложении многоуровневой модели угроз, учитывающей взаимовлияние индивидуального, национального и глобального уровней.

Целью исследования является анализ эволюции концепции безопасности в постхолодновоенный период, выявление новых форм угроз и разработка подходов к обеспечению экономической безопасности в условиях цифровизации.

Задачи исследования:

1. Определить основные трактовки термина «безопасность» в различных сферах (политика, экономика, IT).

2. Выявить уровни безопасности и их специфические угрозы (от индивидуального до глобального).
3. Проанализировать понятие экономической безопасности и её ключевые компоненты.
4. Исследовать феномен киберпреступности как новой формы экономических угроз.
5. Классифицировать виды киберпреступлений и их влияние на экономическую стабильность.
6. Предложить направления укрепления экономической безопасности в цифровой среде.

Материалы и методы исследования

В качестве основных методов исследования применены: системный анализ — для изучения взаимосвязей между уровнями безопасности и типами угроз; сравнительно-правовой метод — при сопоставлении нормативных подходов к регулированию киберпреступности; структурно-функциональный анализ — для выявления роли институтов безопасности в разных странах;

В качестве материалов исследования выступают данные о правовых механизмах противодействия цифровым угрозам (законодательство разных стран); случаях крупных кибератак и их последствиях для экономики.

В рамках исследования угроз и рисков экономической деятельности в сфере кибербезопасности проанализирован ряд ключевых источников. M. Abdullayeva и S. Tokhirova [1] акцентируют внимание на возрастающей значимости кибербезопасности в цифровую эпоху, подчёркивая необходимость защиты данных и ИТ-инфраструктуры для устойчивого экономического развития. A. V. Vinogradova [2] изучает международный опыт противодействия кибертерроризму, детально разбирая стратегию кибербезопасности Великобритании как образец системного подхода к минимизации угроз. В работе В. А. Ермаковой [3] исследуется взаимосвязь информационной безопасности и экономической устойчивости предприятия, предлагаются конкретные механизмы защиты управленческих систем экономического объекта. V. V. Kornienko и T. A. Pavlova [4] анализируют взаимосвязь бизнеса и кибербезопасности в условиях цифровизации экономики, выявляя ключевые риски и методы их снижения для коммерческих структур. И. М. Левкин [5] раскрывает понятие информационно-экономической безопасности как неотъемлемого элемента общей экономической безопасности, обозначая основные угрозы и способы их нейтрализации. D. R. Misinev и O. V. Karchava [6] фокусируются на психологическом аспекте кибербезопасности, изучая поведенческие уязвимости пользователей и методы профилактики человеческого фактора в киберинцидентах. A. Orazgeldiyev и J. Shohradova [7] обобщают современные вызовы кибербезопасности, формулируют стратегические направления защиты в цифровой среде и намечают перспективы развития отрасли. Коллективная монография под редакцией Е. В. Алексеевой и др. [8] предлагает комплексный анализ угроз экономической безопасности, включая киберриски, и рассматривает сценарии реагирования на вызовы новой экономической реальности. M. N. Razdobarova, A. A. Kryukov и E. S. Moroz [9] исследуют тенденции цифровизации и автоматизации экономики, выявляя сопутствующие риски и пути их снижения в контексте экономической деятельности. А. П. Плотников, В. В. Бехер, О. А. Мызрова и др. [10] в

учебном пособии систематизируют методы управления экономической безопасностью в различных сферах, включая киберпространство, и дают практические рекомендации для организаций. H. Bertel и K. Bertel [11] в энциклопедическом обзоре затрагивают вопросы международной безопасности, в том числе аспекты кибербезопасности в глобальном контексте. Cambridge English Business Dictionary [12] предоставляет базовые определения ключевых терминов («безопасность», «кибербезопасность») в бизнес-контексте, что важно для уточнения понятийного аппарата исследования.

Основная часть. Результаты исследования.

Рассмотрены различные информационные источники: международные договоры и соглашения по кибербезопасности; научные публикации по теории безопасности и экономике; данные национальных правоохранительных органов; кейсы из судебной практики по делам о киберпреступлениях; исследования в области цифровой экономики и киберправа.

Безопасность как концепция и как явление в конце холодной войны приобрела новые формы. Появились новые повестки дня в области безопасности, новые проявления безопасности и новые подходы к решению вопросов безопасности.

Безопасность — это общеупотребительное слово, используемое в отношении широкого спектра личных и коллективных действий и условий. Рассмотрим основные определения этого термина.

Безопасность – это:

- состояние отсутствия опасности или угрозы;
- защищенность государства или организации от преступной деятельности, такой как терроризм, кража или шпионаж;
- процедуры или меры, принимаемые для обеспечения безопасности государства или организации;
- состояние ощущения безопасности, стабильности и отсутствия страха или тревоги.

Различают безопасность в обычной повседневной жизни (работа, экономика, транспорт, питание), безопасность в позитивных, желаемых условиях (демократия, свобода, процветание, развитие, хорошая жизнь) и безопасность от негативных условий (война, загрязнение окружающей среды, преступность, все виды угроз).

Кембриджский бизнес-словарь также даёт определения термину безопасность в различных сферах:

1. Финансы. Финансовый или инвестиционный инструмент, выпущенный компанией или государственным учреждением, который подтверждает право собственности и подтверждает наличие долга, право на долю в прибыли эмитента или право на распределение имущества. Ценные бумаги включают облигации, долговые обязательства, векселя, опционы, акции и варранты, но не страховые полисы, и могут торговаться на финансовых рынках, таких как фондовые биржи.

2. Банковские операции. Актив, заложенный в качестве гарантии погашения кредита, исполнения обязательства или в соответствии с соглашением. Его обеспечение предоставляет кредитору законное право доступа к заложенному активу и право на вступление в его владение и право собственности в случае невыполнения обязательств по продаже заложенного имущества.

3. Вычислительная техника. Степень защиты компьютерной системы от повреждения, уничтожения, перехвата, потери или несанкционированного доступа к данным.

4. Предотвращение и защита от нападения, повреждения, пожара, мошенничества, нарушения конфиденциальности, кражи, незаконного проникновения и других подобных действий [12].

В политической сфере термин «безопасность» используется как политический инструмент, например, для придания определённому явлению особого приоритета, помещая его в сферу высокой политики. Наконец, «безопасность» может использоваться как аналитическое понятие для определения, описания, понимания, объяснения или даже прогнозирования явлений в общей социальной сфере; таких как «политика безопасности», «взаимодействие политики безопасности» или «институты и структуры безопасности».

Существенным изменением в политическом использовании термина «безопасность» стало введение концепции политики безопасности.

В 1947 году администрация США создала Совет национальной безопасности, что повлекло за собой введение нового понятия – «политика безопасности». Политика безопасности охватывала внутреннюю безопасность, политику экономического развития и политику влияния на международную систему с целью создания мирной обстановки как на региональном, так и на глобальном уровне, включая иностранную помощь развивающимся странам.

Политика безопасности стала важным инструментом для отдельных государств в продвижении своих национальных интересов путем воздействия на международную систему. Политическое понятие безопасности расширилось, отражая, не только преимущественно такие вопросы как предотвращение военной агрессии, но и решение экономических, политических и социальных вопросов, как внутренних, так и международных [11].

Чтобы сформировать представление о концепции безопасности, следует указать шесть её уровней, каждый из которых определяется субъектами безопасности и которые одновременно являются жертвами угроз безопасности на своём уровне:

1. Индивидуальная безопасность. Для отдельного человека жизненно важной угрозой, является то, что угрожает его физическому и экономическому выживанию. Она проявляется через принуждение и насилие, как физическое, так и экономическое.

2. Безопасность социальной группы, сообщества, нации или организованной национальной или этнической общности. Для национального общества жизненно важным элементом является идентичность, составляющая саму основу общества. Без идентичности нет общества.

3. Безопасность государства или нации (национальная безопасность).

Для государства жизненно важной угрозой является то, что угрожает его суверенитету. Без суверенитета социально-политическое образование не может быть признано государством.

4. Региональная безопасность, то есть целостный регион безопасности, не обязательно основанный на географической близости. Для региона важнейшими факторами являются стабильность и согласованность.

5. Безопасность международного сообщества, которое включает большинство государств мира. Для мира, рассматриваемого как субъект безопасности, устойчивость воспринимается как наиболее уязвимый жизненно важный фактор для угроз.[1]

6. Глобальная безопасность, то есть всей планеты. Глобальная безопасность может принимать различные формы, включая экономическую, экологическую, личную и информационную. Каждая из них имеет решающее значение для поддержания международных политических и экономических отношений.

Обратимся к понятию экономической безопасности. Экономическая безопасность подразумевает защиту систем производства и обмена, экономических ресурсов и корпоративных интересов. Глобализация экономических отношений и рост транснациональных корпораций (ТНК) и международных финансовых рынков создали новые вызовы для глобальной экономической безопасности [8,10].

Экономическая безопасность — это сложное понятие, которое в широком смысле охватывает три проблемы:

1. страны должны поддерживать достаточно прочную экономическую базу для покрытия своих военных расходов;

2. страны должны защищать своих граждан от международных экономических потрясений и обеспечивать доступ к необходимым ресурсам и технологиям;

3. страны должны обеспечивать достойный уровень жизни для своих граждан, что может подразумевать поддержание внутреннего производства в стратегических отраслях.

Первое определение экономической безопасности тесно связано с традиционной политикой национальной безопасности. Располагаемый доход государства, зависящий от налоговых поступлений от производительной экономики, всегда определял уровень военного потенциала, который они могли бы приобрести. Страны, у которых заканчиваются деньги на военные расходы, проигрывают войны; страны, у которых не хватает экономических ресурсов для поддержания уровня военных расходов мирного времени, часто терпят внутренний крах.

Второе определение экономической безопасности фокусируется на внешних факторах, которые могут периодически влиять на процветание, так же как военная безопасность фокусируется на защите от войн, которые периодически угрожают территориальной целостности страны.

Экономическая безопасность, с этой точки зрения, определяется невосприимчивостью к внешним экономическим потрясениям и иностранному экономическому принуждению.

Третье определение экономической безопасности рассматривает долгосрочное процветание страны как базовый показатель её экономического роста, а не как вариацию уровня благосостояния, рассматриваемую во втором определении.

Экономическая преступность постоянно развивается и представляет собой всё более сложную проблему для организаций и экономики.

За последние годы экономическая преступность претерпела изменения, принимая различные формы в разных отраслях. Одной из самых распространённых форм экономической преступности является киберпреступность.

Киберпреступность, также известная как компьютерное преступление, подразумевает использование информационных технологий в качестве инструмента для незаконных целей, таких как мошенничество, торговля интеллектуальной собственностью, кража личных данных или вторжение в частную жизнь. Киберпреступность, особенно совершаемая через интернет, приобретает всё большую значимость благодаря центральной роли информационных технологий во всех сферах жизнедеятельности, особенно в торговле, индустрии развлечений и государственном управлении.

Киберпреступность охватывает широкий спектр деятельности. С одной стороны, совершаются преступления, представляющие собой грубые нарушения неприкосновенности частной жизни, будь то личной или профессиональной, такие как посягательства на целостность цифровой информации и использование незаконно полученной цифровой информации для шантажа компании или отдельного лица. Сюда также относится растущее число преступлений, связанных с кражей личных данных. В середине спектра находятся транзакционные преступления, такие как мошенничество, взлом, отмывание денег и подделка документов. Это конкретные преступления, направленные на конкретных лиц, но преступник скрывается благодаря относительной анонимности, предоставляемой интернетом.

Другой аспект этого вида преступлений связан с лицами, работающими в компаниях или государственных учреждениях, которые намеренно изменяют данные ради прибыли или политической выгоды. Также следует отметить преступления, направленные на нарушение функционирования интернета. Они варьируются от спама, взлома и атак типа «отказ в обслуживании» на определенные веб-сайты до актов кибертерроризма, то есть использования интернета для создания общественных беспорядков или даже гибели людей. Кибертерроризм сосредоточен на использовании интернета негосударственными субъектами для воздействия на экономическую и технологическую инфраструктуру страны [4,5,7].

В настоящее время существует множество видов киберпреступности:

-хакеры-любители. До относительно недавнего времени большинство онлайн-атак совершали хакеры-любители, которые портили веб-сайты и создавали вредоносное ПО ради собственного удовольствия. Некоторые из них были самоучками в области компьютерных наук, как, например, Кевин Митник (2011), которые искали доступ к внутренним данным, чтобы добиться престижа или проверить пределы своих возможностей. Другие были хакерами низкого уровня, которые эксплуатировали уязвимости безопасности ради небольшой выгоды, например, увеличения времени интернет-соединения от провайдера;

- крэкеры, пираты и спекулянты совершают относительно распространённые и малоэффективные правонарушения. Этот вид пиратства, пожалуй, один из самых ранних и распространённых. Программные пираты (или крэкеры) стремятся обойти защиту авторских прав на программное обеспечение или другой контент, защищённый системой управления цифровыми правами, чтобы использовать его бесплатно. Спекулянты — это те, кто несправедливо наживается на работе крэкеров и пиратов, используя пиратский контент, свободно распространяемый в интернете. Иногда спекулянты помогают

продлить срок действия этого контента, выступая в качестве источников в одноранговых сетях;

- киберпреступники, которые представляют наиболее серьёзную экономическую угрозу. Эти преступники выбирают своих жертв — отдельных лиц, организации и правительства — и пытаются обмануть, вымогать, украсть их интеллектуальную собственность или помешать им получать доход. Каждая атака состоит из четырёх этапов: выявление уязвимости, разработка эксплойта, его реализация и монетизация данных;

- профессиональные разработчики вредоносных программ и скрипт-кидди. После того, как разработчики вредоносных программ обнаружили уязвимость, они создают инструменты для её эксплуатации. Эти инструменты могут представлять собой программное обеспечение, предназначенное для компрометации целевой системы. Например, вредоносное ПО может включить машину в ботнет, который затем может быть использован для запуска распределённой атаки типа «отказ в обслуживании», распространения вредоносного ПО или генерации спама. Разработчики этих платформ обычно не используют их лично; вместо этого они продают программное обеспечение или взломанные компьютеры (боты) лицам, которые их используют. Их часто уничижительно называют «скрипт-кидди», поскольку им приходится покупать эти инструменты, а не разрабатывать их самостоятельно;

- подпольные кардеры. В случае утечки данных следующим шагом является монетизация украденных данных. Монетизацию посредством манипуляции данными для получения доступа к связанным аккаунтам практикуют лица, известные как «кардеры» (термин, происходящий от практики использования украденных учетных данных для создания поддельных кредитных карт);

- вымогатели также присутствуют в интернете. Они используют ботнеты и вредоносное ПО для осуществления своих мошеннических действий. Это могут быть мошенники, разрабатывающие и использующие вредоносное ПО, или младшие разработчики, которые его покупают и запускают;

- фишинг, заключающийся в использовании спам-писем, чтобы обманным путем заставить жертв раскрыть конфиденциальную информацию или установить вредоносное ПО на свои устройства, — широко известная проблема среди интернет-пользователей;

-мошенники, использующие чёрный метод. Помимо уже упомянутых видов мошенничества, существует ряд других, которые можно отнести к «чёрному методу» — то есть к неприемлемым, неэтичным или несанкционированным приёмам, используемым для обхода существующих систем, например, используемых играми или рекламными платформами.

Сектор онлайн-игр и ставок также генерирует значительные доходы, что делает его благодатной почвой для мошеннической деятельности.

- кликфродисты. Кликфрод — это метод «чёрной шляпы», предназначенный для увеличения дохода от кликов или просмотров рекламы. Это можно осуществить с помощью бота или обманным путём, заставляя людей вручную кликать по рекламным объявлениям.

Экономическая безопасность является важнейшим аспектом стабильности как отдельной страны и её граждан, так и всего мира. Вопрос экономической безопасности

требует комплексного и многогранного подхода в контексте преодоления угроз и вызовов, с которыми она сталкивается. Понимая ключевые компоненты экономической безопасности, выявляя угрозы и уязвимые места и реализуя стратегии по укреплению экономической безопасности, мы можем способствовать созданию более стабильной и процветающей экономики.

Выводы и предложения

1. Концепция безопасности претерпела кардинальную трансформацию: от военно-политического фокуса к многомерной системе, включающей экономические, цифровые и социальные аспекты.

2. Выделены шесть уровней безопасности (индивидуальный, групповой, национальный, региональный, международный, глобальный), каждый из которых имеет специфические угрозы и механизмы защиты.

Экономическая безопасность стала ключевым элементом национальной устойчивости, охватывающим: защиту экономической базы государства; противодействие внешним экономическим потрясениям; обеспечение достойного уровня жизни граждан.

Киберпреступность представляет собой системную угрозу, требующую: международного сотрудничества в расследовании; модернизации законодательства; внедрения передовых технологий защиты данных.

Для укрепления экономической безопасности необходимо: развивать системы раннего предупреждения о киберугрозах; повышать цифровую грамотность населения и бизнеса; создавать межгосударственные платформы для обмена информацией о преступлениях; инвестировать в киберзащиту критической инфраструктуры; гармонизировать правовые нормы разных стран в сфере киберпреступности.

3. Перспективным направлением является формирование глобальной архитектуры кибербезопасности, объединяющей усилия государств, частного сектора и гражданского общества.

Список источников

1.Abdullayeva, M. The importance of cybersecurity in a digital age / M. Abdullayeva, S. Tokhirova // Universum: технические науки. – 2024. – No. 6-6(123). – P. 4-6. – EDN GNSVFS.

2.Vinogradova, A. V. International experience in combating cyberterrorism and the UK cybersecurity strategy / A. V. Vinogradova // , 24–27 апреля 2023 года, 2023. – P. 342-347. – EDN PKMTJY.

3.Ермакова, В. А. Информационная безопасность системы управления экономическим объектом как элемент обеспечения экономической безопасности предприятия / В. А. Ермакова // Управление развитием социально-экономических систем: глобализация, предпринимательство, устойчивый экономический рост : Материалы XXV Международной научной конференции молодых учёных и студентов, Донецк, 05 декабря 2024 года. – Донецк: Донецкий национальный университет, 2025. – С. 34-37. – EDN DEIXDA.

4.Kornienko, V. V. Relationship of business and cyber security in conditions of economy digitalization / V. V. Kornienko, T. A. Pavlova // Научный альманах. – 2022. – No. 12-2(98). – P. 42-45. – EDN QRFVIU.

5.Левкин, И. М. Информационно-экономическая безопасность как специфический элемент экономической безопасности / И. М. Левкин // Технологии информационно-экономической безопасности. – Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2016. – С. 79-89. – EDN XFZLIR.

6.Misinev, D. R. The psychology of cybersecurity and its application to the protection of Internet users / D. R. Misinev, O. V. Karchava // Молодежь. Общество. Современная наука, техника и инновации. – 2024. – No. 23. – P. 43-44. – EDN OSOXQU.

7.Orazgeldiyev, A. Cybersecurity in the digital age: challenges, strategies, and future directions / A. Orazgeldiyev, J. Shohradova // Матрица научного познания. – 2024. – No. 10-2. – P. 82-85. – EDN PQNFMG.

8.Проблемы экономической безопасности: вызовы новой реальности / Е. В. Алексеева, В. В. Бехер, Т. А. Верезубова [и др.]. – Челябинск : Южно-Уральский государственный университет (национальный исследовательский университет), 2023. – 732 с. – ISBN 978-5-696-05372-1. – EDN JGEVFM.

9.Razdobarova, M. N. Digitalization and automation in the economy: trends and challenges / M. N. Razdobarova, A. A. Kryukov, E. S. Moroz // , 10 февраля – 14 2025 года, 2025. – P. 507-510. – EDN FAEPTN.

10.Экономическая безопасность: управление в различных сферах : учебник / А. П. Плотников, В. В. Бехер, О. А. Мызрова [и др.]. – Саратов : Вузовское образование, 2025. – 490 c. – ISBN 978-5-4487-1009-4. – EDN VEAJAS.

11. Bertel H., Bertel K. International Relations. Vol.II – International Security – Encyclopedia of Life Support Systems (EOLSS).

12. Cambridge English Business Dictionary // Cambridge press.- Текст : электронный URL: http://www.businessdictionary.com/definition/security.html. (дата обращения 10.10.2025)

References

1. Abdullayeva, M. The importance of cybersecurity in a digital age / M. Abdullayeva, S. Tokhirova // Universum: technical sciences. - 2024. - No. 6-6 (123). - P. 4-6. - EDN GNSVFS.

2. Vinogradova, A. V. International experience in combating cyberterrorism and the UK cybersecurity strategy / A. V. Vinogradova // , April 24-27, 2023, 2023. - P. 342-347. - EDN PKMTJY.

3. Ermakova, V. A. Information security of the management system of an economic entity as an element of ensuring the economic security of an enterprise / V. A. Ermakova // Managing the development of socio-economic systems: globalization, entrepreneurship, sustainable economic growth: Proceedings of the XXV International Scientific Conference of Young Scientists and Students, Donetsk, December 5, 2024. - Donetsk: Donetsk National University, 2025. - P. 34-37. - EDN DEIXDA.

4. Kornienko, V. V. Relationship of business and cyber security in conditions of economy digitalization / V. V. Kornienko, T. A. Pavlova // Scientific almanac. - 2022. - No. 12-2 (98). - P. 42-45. - EDN QRFVIU.

5. Levkin, I. M. Information and economic security as a specific element of economic security / I. M. Levkin // Technologies of information and economic security. - St. Petersburg: St. Petersburg State University of Economics, 2016. - P. 79-89. - EDN XFZLIR.

6. Misinev, D. R. The psychology of cybersecurity and its application to the protection of Internet users / D. R. Misinev, O. V. Karchava // Youth. Society. Modern Science, Technology and Innovation. - 2024. - No. 23. - P. 43-44. - EDN OSOXQU.

7. Orazgeldiyev, A. Cybersecurity in the digital age: challenges, strategies, and future directions / A. Orazgeldiyev, J. Shohradova // Matrix of scientific knowledge. - 2024. - No. 10-2. – P. 82-85. – EDN PQNFMG.

8. Problems of Economic Security: Challenges of the New Reality / E. V. Alekseeva, V. V. Bekher, T. A. Verezubova [et al.]. – Chelyabinsk: South Ural State University (National Research University), 2023. – 732 p. – ISBN 978-5-696-05372-1. – EDN JGEVFM.

9. Razdobarova, M. N. Digitalization and automation in the economy: trends and challenges / M. N. Razdobarova, A. A. Kryukov, E. S. Moroz //, February 10–14, 2025, 2025. – P. 507-510. – EDN FAEPTN.

10. Economic Security: Management in Various Spheres: Textbook / A. P. Plotnikov, V. V. Bekher, O. A. Myzrova [et al.]. – Saratov: Vuzovskoe obrazovanie, 2025. – 490 p. – ISBN 978-5-4487-1009-4. – EDN VEAJAS.

11. Bertel H., Bertel K. International Relations. Vol. II – International Security – Encyclopedia of Life Support Systems (EOLSS).

12. Cambridge English Business Dictionary // Cambridge press. – Text: electronic URL: http://www.businessdictionary.com/definition/security.html. (accessed date 10.10.2025)