

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**Белова С.Е., студентка 3 курса экономического факультета,  
Научный руководитель – Климушкина Н. Е.,  
кандидат экономических наук, доцент  
ФГБОУ ВО Ульяновский ГАУ**

**Ключевые слова:** *информационно-коммуникационные технологии, информационная безопасность, экономическая безопасность, кибербезопасность.*

*В статье рассмотрено роль информационной безопасности в условиях развития глобальных информационных и телекоммуникационных систем.*

В современных условиях глобализации и развития глобальных информационных и телекоммуникационных систем проблема обеспечения экономического суверенитета страны приобретает новое содержание и смысл. Система экономической безопасности, по сути, является гарантом суверенитета и независимости страны в целом, поскольку национальная безопасность и оборона тесно связаны с экономической ситуацией. В связи с быстрым развитием ИКТ (информационно-коммуникационные технологии) информация стала одним из важнейших объектов защиты при обеспечении экономической безопасности страны. Ее существенное значение обусловлено тем, что она пронизывает все сферы нашей жизни [1].

Цифровая эпоха, в которой мы живем, облегчает реструктуризацию информационных систем и вызывает необходимость принимать новые стратегии, отвечающие требованиям информационной безопасности (ИБ). Помимо очевидных преимуществ, использование информационных технологий (ИТ) также сопряжено с проблемами (например, интернет-мошенничество, обработка больших объемов данных и др.). Киберпреступность, стала глобальной проблемой, сложной транснациональной угрозой, действующей в промышленных масштабах [2]. Под влиянием информационной

экономики технологии, связанные с экономической и конкурентной деятельностью, перешли из традиционного пространства в виртуальное. Так, за 7 лет количество информационных преступлений в РФ выросло в 7,5 раз, а их доля увеличилась с 15% до 40%. В 2024 году зарегистрировано 765,4 тыс. таких преступлений, увеличившись по сравнению с 2023 годом на 13,1%, из них тяжких и особо тяжких - на 7,8%. В 2024 году СК России расследовано более 23 787 преступлений, совершенных с применением современных цифровых средств, что на 9,6% больше, чем в 2023 году. Две трети из расследованных ведомством преступных деяний связаны с использованием интернет-ресурсов [3].

В наши дни бизнес широко использует информационную войну для создания рыночных преимуществ и ослабления своих противников. Как угроза экономической безопасности в информационной сфере, сама информационная война характеризуется поляризацией масштабов источника и объекта воздействия, латентным характером, необратимостью последствий, дальностью воздействия и невозможностью полной ликвидации [4].

Одной из форм информационной войны является создание и распространение мистификаций и разжигания ненависти. Это преднамеренная практика, направленная на продвижение определенных мотивов и интересов субъектов, стремящихся распространить обман и ненависть в цифровой экосистеме ради своих политических или экономических интересов. Разжигание ненависти в киберпространстве благодаря современным медиа-платформам фактически превращает свободу слова в свободу ненависти, которая используется для нападения на тех, кто выступает против. Распространение мистификаций и разжигания ненависти угрожает национальной безопасности и стабильности. Поэтому не только правительство и спецслужбы, но также бизнес и гражданское общество должны обратить серьезное внимание на риски, связанные с такими мистификациями.

Развитие ИКТ и их внедрение во все сферы государственного контроля и национальной экономики поднимают вопрос уязвимости критической информационной инфраструктуры (КИИ) на новый уровень. Без сомнения, серьезный сбой в КИИ будет иметь ужасные последствия как для общества, так и государства в целом [5].

Широкое применение ИКТ поднимает вопрос о том, как лучше всего определить стратегию кибербезопасности, которая бы эффективно работала на благо экономики и гражданского общества. Эффективная стратегия кибербезопасности должна сбалансировать принятые в стране нормы с возможностями, предоставляемыми Интернетом. С одной стороны, Интернет считается прорывной технологией, которая ставит под сомнение многие общепринятые нормы государственной политики, бизнеса и гражданского общества. Однако, с другой стороны, необходимо нивелировать эту опасность открытостью Интернета и свободным потоком информации. Хотя строгая политика безопасности обеспечивает стабильность, она также может снизить потенциальные выгоды от информационных технологий. На примере скандалов, связанных с использованием персональных данных физических и юридических лиц со стороны социальных сетей, непоследовательность властей дорого обходится потенциальным жертвам разного рода утечек персональных данных. Вопрос институционализации и надлежащего управления должен снова стать вопросом совершенствования судебной практики в отношении информационной безопасности, влияющей на общее благосостояние [6].

Таким образом, политика государства в отношении регулирования информационной повестки должна быть гибкой. Однако при проведении такой политики следует понимать, что обеспечение информационной безопасности экономической деятельности является сложной задачей и требует многих ресурсов для обеспечения стратегии реагирования на кризис.

#### **Библиографический список:**

1. Виды экономической безопасности. Их систематизация [Электронный ресурс]. – Режим доступа: <https://studopedia.ru>
2. Правильно настроенная система ИБ – это конкурентное преимущество для бизнеса [Электронный ресурс]. – Режим доступа: <https://www.comnews.ru>
3. Новости цифровой трансформации, телекоммуникаций, вещания и ИТ [Электронный ресурс]. – Режим доступа: <https://www.comnews.ru>

4. Климушкина, Н. Е. Определение основных факторов, влияющих на формирование высокого уровня финансовой безопасности предприятий / Н. Е. Климушкина, Н. Р. Александрова, А. А. Азизова // Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения: Материалы XIV Международной научно-практической конференции, Ульяновск, 25 июня 2024 года. – Ульяновск: Ульяновский государственный аграрный университет им. П.А. Столыпина, 2024. – С. 744-751. – EDN KVASCE.

5. Климушкина, Н. Е. Преступления коррупционной направленности в РФ / Н. Е. Климушкина, Е. А. Лешина // Аграрная наука и образование на современном этапе развития: Материалы XIII Международной научно-практической конференции, посвященной 80-летию Ульяновского ГАУ, Ульяновск, 23 июня 2023 года / Редколлегия: И.И. Богданов [и др.]. – Ульяновск: Ульяновский государственный аграрный университет им. П.А. Столыпина, 2023. – С. 774-779. – EDN GWJVVB.

6. Климушкина, Н. Е. Финансовая безопасность предприятия: системный подход: Монография / Н. Е. Климушкина, О. И. Хамзина, Н. Р. Александрова. – Ульяновск: Ульяновский государственный аграрный университет, 2024. – 182 с. – ISBN 978-5-605-23946-8. – EDN GZNVVD.

## SECURITY IN THE SOCIAL SPHERE

**Belova S.E.**

**Scientific supervisor – Klimushkina N. E.**

**Ulyanovsk SAU**

**Keywords:** *ICT, information security, cybersecurity, CII.*

*The article describes the problem of providing information. Security (IS) in the economic sphere is of particular relevance. Despite the abundance of research on information security, the impact of the information sphere on the country's economy and security has not yet been sufficiently studied.*