УДК 339.9
JEL F52
DOI: http://doi.org/10.25728/econbull.2024.1.1-tulunbasova

ВЛИЯНИЕ ЭКОНОМИЧЕСКОГО ШПИОНАЖА В ИНТЕРНЕТЕ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ И РАЗВИТИЕ НАЦИОНАЛЬНЫХ ЭКОНОМИК (ОПЫТ США И КНР)

Тулунбасова Надежда Андреевна
Российский университет дружбы народов, Москва, Россия,
e-mail:tulunbasova.n.a@mail.ru; SPIN-код: отсутствует; ORCID: отсутствует

Аннотация: Эволюция интернета оказала двойственное воздействие на общество: с одной стороны, она стимулировала прогресс, а с другой – создала плодотворную почву для киберпреступности, в последнее время многие страны все чаще сталкиваются с киберугрозами. Целью данной работы является рассмотрение такого явления, как экономический кибершпионаж и его влияния на экономическую безопасность национальных экономик. В статье анализируется определение понятия «экономический шпионаж» в законодательстве США и КНР, уделяется внимание росту напряженности между этими странами из-за применения ними механизмов экономического шпионажа. В работе рассмотрены позитивные и негативные стороны экономического шпионажа с точки зрения воздействия на национальные экономики и безопасность стран. По результатам анализа сделан вывод, что экономический шпионаж, безусловно, угрожает конкурентоспособности, инновационной деятельности, экономике и национальной безопасности, однако он имеет и позитивные стороны: способствует распространению и развитию новых технологий, мотивирует улучшать кибербезопасность, а также стимулирует международное сотрудничество в этой области.

Ключевые слова: экономический шпионаж, кибершпионаж, киберпреступность, экономическая безопасность, кибербезопасность, национальная безопасность

THE IMPACT OF ECONOMIC CYBER ESPIONAGE ON THE ECONOMIC SECURITY AND DEVELOPMENT OF NATIONAL ECONOMIES (THE EXPERIENCE OF THE USA AND CHINA)

Tulunbasova Nadezhda Andreevna
RUDN University, Moscow, Russia,
e-mail: tulunbasova.n.a@mail.ru; SPIN code: none; ORCID: none

Abstract: The evolution of the Internet has had a dual impact on society: on the one hand, it has stimulated progress, and on the other, it has created fertile ground for cybercrime, and recently countries have increasingly faced cyber threats. The purpose of this article was to consider such a concept as economic cyber espionage and its impact on economic security of national economies. The article analyzes the definition of "economic espionage" in the legislation of the United States and China, and focuses to the growing tensions between these countries due to the use of economic espionage mechanisms. The article examines the positive and negative sides of

economic espionage in terms of its impact on national economies and countries security. The analysis concluded that economic espionage undoubtedly threatens competitiveness, innovation, the economy and national security, but it also has a positive side: it promotes diffusion and development of new technologies, motivates to improve cybersecurity, and stimulates international cooperation in the field of cybersecurity.

Keywords: economic espionage, cyber espionage, cybercrime, economic security, cybersecurity, national security

Введение. Технологический прорыв 1970-х годов XX века, и последовавшее внедрение интернета, привели к глобальным изменениям во всех областях жизни общества и государства. Информационно-коммуникационные технологии играют ключевую роль в быстро развивающемся глобальном информационном обществе. Сегодня в мире насчитывается 5,16 миллиардов пользователей интернета, то есть 64,4% мирового населения имеют доступ в интернет. Общество уже не может представить свою жизнь без постоянного доступа к онлайн-ресурсам, цифровой коммуникации и интернет-услугам. Это явление привело к тому, что все больше областей деятельности активно переходят в онлайн пространство, изменяя привычные нам процессы и взаимодействия. Можно с уверенностью сказать, что в настоящее время практически всё имеет выход в Интернет, и всё, что имеет выход в Интернет, может быть «взломано».

Эксперты Центра исследования компьютерных преступлений сообщили, что «потери мировой экономики от киберугроз выросли за последние 4 года более чем втрое и составили оценочно не менее $8 трлн за 2022 год», также они опубликовали прогноз, согласно которому «ущерб от киберпреступлений по всему миру достигнет в следующем году $12 трлн, а к 2030 году – $90 трлн» [3]. Мировое сообщество вступает в бесконечную борьбу с киберугрозами, которые постоянно совершенствуются. Очевидно, что сегодня страны становятся более уязвимыми в информационном пространстве. При этом, в условиях широкой сетевой интеграции, возрастает взаимосвязь и взаимозависимость информационных пространств государств. Вопросы противодействия угрозам в информационной сфере уже получают глобальное измерение [2].

Понятие экономического шпионажа в законодательстве США и КНР. В Соединенных Штатах Америки термин «экономический шпионаж» употребляется в «Законе об экономическом шпионаже», принятом в 1996 году, и соответствующих комментариев к нему [7]. Этот закон устанавливает уголовную ответственность за незаконное присвоение коммерческой тайны и предоставляет правительству возможность рассматривать такие дела в судах. Наказание за нарушение данного закона – штраф или лишение свободы на срок не более 10 лет. Под экономическим шпионажем в данном законе понимается сознательное совершение субъектом, намеревающимся или знающим, что совершенное преступление принесет пользу какому-либо иностранному правительству, иностранной организации или иностранному агенту, следующих действий:

1) кража, незаконное присвоение, сокрытие, получение путем обмана или мошенничества информации, составляющей коммерческую тайну;
2) копирование, дублирование, воспроизведение, уничтожение, скачивание, рассылка, оглашение и передача информации, составляющей коммерческую тайну;

3) получение, покупка или обладание информацией, составляющей коммерческую тайну, с осознанием того, что она была украдена, присвоена или преобразована без соответствующего разрешения [7].

Федеральное бюро расследований (ФБР) определяет экономический шпионаж как «спонсируемую или скоординированную иностранными державами разведывательную деятельность, направленную против правительства США или американских корпораций, учреждений или частных лиц, направленную на незаконное или подпольное влияние на важные решения в области экономической политики или на незаконное получение конфиденциальной финансовой, торговой или экономической политической информации; частной экономической информации; или критических технологий. Эта кража, осуществляемая открытыми и подпольными методами, может предоставить иностранным организациям жизненно важную конфиденциальную экономическую информацию за небольшую часть истинной стоимости ее исследований и разработок, что приводит к значительным экономическим потерям» [9].

Если рассмотреть законодательство КНР в области экономического шпионажа, можно выделить «Закон о борьбе со шпионажем», впервые принятый в 2014 году и ставший первым законом, специально направленным против шпионской деятельности. Стоит отметить, что в апреле 2023 года Постоянный комитет Всекитайского собрания народных представителей принял решение о реформировании системы контрразведки Китая и одобрил пересмотренный «Закон о борьбе со шпионажем» [4]. Эти последние изменения в законодательстве отражают серьезный поворот в стратегии Китая по укреплению своего аппарата национальной безопасности. Пересмотренный закон уточняет масштабы шпионского поведения. Согласно ему, «акт шпионажа» относится к любому из следующих действий:

1) деятельность, ставящая под угрозу национальную безопасность КНР, которая осуществляется, побуждается или финансируется шпионской организацией и ее агентами или осуществляется агентствами, органами, частными лицами или другими коллаборационистами внутри страны или за пределами границ КНР;
2) участие в шпионской организации или принятие заданий от шпионской организации и ее агентов, или стремление присоединиться к шпионской организации и ее агентам;
3) деятельность, осуществляемая, подстрекаемая или финансируемая иностранными учреждениями, организациями и частными лицами, отличными от шпионских организаций и их представителей, или в рамках которой национальные учреждения, организации или частные лица вступают в сговор с целью кражи, проникновения в чужие дела, приобретения или незаконного предоставления государственных секретов, разведывательных данных и других документов, данных, материалов, или предметы, связанные с национальной безопасностью, или в которых государственных служащих подстрекают, соблазняют, принуждают или подкупают, чтобы они стали предателями.
4) сетевые атаки, вторжения, препятствия, контроль или сбои в работе, нацеленные на государственные органы, подразделения, связанные с секретами, или критически важную информационную инфраструктуру, которые осуществляются, побуждаются или финансируются шпионской организацией и ее агентами, или осуществляются агентствами, органами,

частными лицами или другими коллаборационистами внутри страны или за пределами границ КНР;

5) указание любой цели для врага.
6) другая шпионская деятельность [5].

Таким образом, рассмотрев трактовку понятий «экономический шпионаж» в нормативных документах Китая и США, можно прийти к общему выводу, что «экономический шпионаж в интернете» – это процесс получения конфиденциальной информации о деятельности компании с целью использования этой информации в собственных интересах или для нанесения ущерба конкурентам. Эта информация, как правило, включает в себя коммерческие тайны и сопутствующую информацию, под угрозу могут попасть такие ценные сведения, как: новые разработки кампании, документация, финансовые отчеты, транзакции, доступ к банковским счетам, уникальные схемы, методы, стратегии ведения бизнес-процессов, организационная структура и штат кампании и другие. И в КНР, и в США данному термину уделяется большое внимание, созданы специальные законодательные акты, определяющие конкретные действия, относящиеся к экономическому шпионажу. Также примечательно, что в обеих странах экономический шпионаж неразрывно связан с иностранными правительствами, иностранными организациями или иностранными агентами.

Вопросы экономического шпионажа в американско-китайском взаимодействии. Сейчас экономическим шпионажем пользуются практически все развитые страны для тех или иных целей, однако есть две страны, которые используют методы экономического шпионажа в целях подрыва национальной безопасности и экономической стабильности наиболее часто: речь идет о США и КНР.

С ростом увеличения могущества Китая, его возросшей экономической мощью, стремлением влиять на международные процессы и стать глобальным лидером на международной арене, возросла обеспокоенность США, китайско-американские отношения начали значительно ухудшаться, появилась тенденция к секьюритизации внешней политики обеих стран, все больше характеризуя их отношения с точки зрения конкуренции и являясь препятствием для их дальнейшего диалога [1]. С начала 2017 года к власти в США приходит республиканская партия во главе с Дональдом Трампом, и начинается открытая политика сдерживания Китая, вызванная усилением беспокойства по поводу его растущего экономического влияния и усиления военной мощи. Новый конфронтационный подход администрации США к Китаю был озвучен в речи вице-президента Америки Майка Пенса. В 2018 году он произнес заявление, в котором обвинял Китай в нанесении ущерба национальным интересам США в таких областях, как экономика, политика и безопасность, а также отметил отход от сотрудничества в сторону конкуренции [6]. Этот переход мы можем заметить в последующих действиях администрации Д. Трампа, и Д. Байдена, а именно в крупномасштабной торговой и информационной войне и последующими обвинениями Китая в стремлении завоевать лидирующие позиции в экономике и политике XXI века, сформировать новую систему международных отношений путем нанесения ударов по основам либерального демократического порядка.

В американских источниках можно найти множество обвинений КНР в экономическом шпионаже, предлагаем рассмотреть их статистику более подробно. Китайская Народная Республика и ее Министерство государственной безопасности

были замешаны в множестве обвинений в краже коммерческой тайны в Соединенных Штатах и во всем мире. В период с 1996 по 2019 год Китай выиграл 66 (32%) из 206 федеральных дел США, связанных с обвинениями, связанными с «Законом об экономическом шпионаже 1996 года». Экономический эффект также значителен: по состоянию на 2018 год на китайскую экономическую шпионскую деятельность приходилось 320 миллиардов долларов убытков в год, или 80% от общей стоимости кражи интеллектуальной собственности в США, которая оценивается в 400 миллиардов долларов в год [8]. Нынешнюю волну экономического шпионажа под руководством Китая, нацеленного на Соединенные Штаты, остановить еще труднее, поскольку стратегически важные торговые связи между двумя странами облегчают поток информации и делают контрразведывательную политику чрезвычайно дорогостоящей.

Однако наряду с обвинениями КНР в экономическом шпионаже, появляются и обвинения США в кибершпионаже. Институты кибербезопасности Китая периодически публикуют отчеты, в которых раскрываются многолетние кибератаки правительства США против Китая. Пекин регулярно отчитывается о раскрытии очередных фактов шпионажа в пользу США. В очередной раз об этом в октябре сообщило Министерство государственной безопасности Китая. По его данным, спецслужбы китайской провинции Сычуань выявили случай передачи секретной информации с одного из оборонных предприятий КНР компетентным органам Соединенных Штатов. Шпионажем занимался гражданин Китая, который прежде проходил стажировку в США. В 2010-2012 годы в КНР вскрывали агентов, работающих на ЦРУ. Около двух десятков лиц, предоставлявших информацию США, были казнены или заключены в тюрьму, в их числе были высокопоставленные китайские чиновники [10].

Негативное влияние экономического шпионажа в интернете на экономическую безопасность и развитие национальных экономик. Рассмотрев взаимоотношения Китая и Америки в аспекте экономического шпионажа, можно убедиться, что он несет за собой значительные отрицательные последствия для обеих стран. Говоря о негативном влиянии экономического шпионажа в интернете на экономическую безопасность и развитие национальных экономик, можно отметить такие ключевые аспекты, как:

1. ***Потеря конкурентного преимущества***. Конкуренты могут получать доступ к конфиденциальным данным о новых технологиях, стратегиях или исследованиях, что позволяет им адаптировать свои собственные практики и оставаться на шаг впереди. Это приводит к снижению прибыли и утрате рыночной доли у компаний, что в конечном итоге отрицательно сказывается на экономике страны.

2. ***Ущерб инновационной деятельности.*** Экономический шпионаж может подорвать инновационную деятельность компаний, угрожая целым отраслям экономики. Компании неохотно делиться своими идеями и технологиями из-за опасений по поводу их кражи или использования против них, что замедляет темпы инноваций и развития новых продуктов и услуг и в конечном итоге может привести к отставанию от других стран в технологической гонке.

3. ***Разрушение доверия и репутации между странами***. Успешные случаи экономического шпионажа могут нанести серьезный ущерб доверию к компаниям и правительствам. Когда конфиденциальные данные становятся доступными для посторонних, это может привести к потере доверия со стороны клиентов,

партнеров и инвесторов. Повреждение репутации компании или страны может привести к потере бизнеса, инвестиций и уменьшению международного влияния;

4. ***Экономические потери***. Потери от экономического шпионажа могут быть огромными как для частных компаний, так и для государственных структур. Утечка конфиденциальных данных может привести к финансовым убыткам, включая потерю интеллектуальной собственности, штрафы и судебные издержки. В целом, экономические потери от экономического шпионажа могут быть колоссальными и оказать серьезное воздействие на национальную экономику.

5. ***Угроза национальной безопасности***. Наконец, экономический шпионаж представляет угрозу для национальной безопасности страны. Кража важной информации о научных исследованиях, военных технологиях или критической инфраструктуре может иметь далеко идущие последствия для безопасности и суверенитета государства.

Позитивное влияние экономического шпионажа в интернете на экономическую безопасность и развитие национальных экономик. После рассмотрения негативного влияние экономического шпионажа, и его масштабов, может показаться, что этот термин несет за собой лишь угрозу безопасности и стабильности, но нельзя не отметить, что экономический шпионаж может иметь и положительные последствия для национальной экономики, при этом можно отметить несколько аспектов:

1. ***Повышение конкурентоспособности***. Путем сбора информации о стратегиях и технологиях конкурентов, компании могут адаптировать свои собственные практики и инновации, чтобы оставаться впереди. Это способствует стимулированию инноваций и развитию новых продуктов и услуг, что в конечном итоге способствует экономическому росту страны;

2. ***Улучшение национальной безопасности***. Парадоксально, но сам факт существования экономического шпионажа мотивирует компании и правительства улучшить свою собственную систему безопасности. Чем более активно происходит кибершпионаж, тем сильнее становится необходимость в разработке и внедрении новых методов защиты данных и информационных ресурсов. Это приводит к развитию индустрии кибербезопасности и укрепляет оборонную стратегию страны от цифровых угроз.

3. ***Содействие в выявлении уязвимостей***. Часто экономический шпионаж выявляет уязвимости в системах и инфраструктуре компаний и правительств. Обнаружение этих слабых мест позволяет предпринять меры по их устранению, что в итоге способствует улучшению кибербезопасности в целом. Это также помогает предотвратить возможные атаки со стороны злоумышленников и других государств.

4. ***Содействие международному сотрудничеству***. Феномен экономического шпионажа заставляет государства сотрудничать в сфере кибербезопасности и обмене информацией. Это помогает создать более безопасное киберпространство не только внутри страны, но и на международном уровне. Совместные усилия по борьбе с киберугрозами способствуют укреплению международных отношений и сотрудничеству в различных областях.

5. ***Стимулирование иннова***ций. Экономический шпионаж также может стимулировать инновационную деятельность в компаниях и правительственных организациях. Необходимость защиты собственной информации заставляет

разрабатывать новые технологии и методы, что способствует росту инноваций и улучшению технологического потенциала страны.

Выводы. Рассмотрев понятие экономического шпионажа в интернете, можно сказать, что экономический шпионаж оказывает серьезное негативное влияние на экономическую безопасность и развитие национальных экономик. Он угрожает конкурентоспособности компаний, инновационной деятельности, доверию к бизнесу и государству, причиняет экономические потери и представляет угрозу для национальной безопасности. Поэтому необходимо уделять повышенное внимание борьбе с этим явлением и развитию соответствующих стратегий и политик для защиты экономики от киберугроз. Однако не следует забывать и о его позитивном влиянии на экономическое развитие: он мотивирует компании и правительства улучшать свою кибербезопасность, способствует инновациям и развитию новых технологий, а также стимулирует международное сотрудничество в области кибербезопасности. Понимание этих позитивных аспектов позволяет лучше оценивать роль экономического шпионажа в современном цифровом мире и использовать его потенциал в интересах национального развития. Стоит также отметить, что технологии постоянно развиваются, создавая все новые формы киберугроз, в связи с чем странам необходимо постоянно обновлять законодательство и совершенствовать структуру по борьбе с киберпреступностью, а также усилить международное взаимодействие по данным вопросам.

Литература

1. Актуальные кибергурозы для стран Азии: 2022–2023 год. – Текст: электронный // Positive Technologies [сайт]. – 2021. – 12 сен. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/asia-cybersecurity-threatscape-2022-2023/ (дата обращения: 01.04.2024).
2. Тышова А.С. Международный опыт в сфере противодействия экономическим преступлениям, совершаемым в киберпространстве // Трансформация национальной социально-экономической системы России: Материалы V Международной научно-практической конференции, Москва, 02 декабря 2022 года. – Москва: Российский государственный университет правосудия, 2023. – С. 321-326. – EDN FGUEAY.
3. Chin K. The Impact of Cybercrime on the Economy // UpGuard [website]. – 2023. – May 18. – URL: https://www.upguard.com/blog/the-impact-of-cybercrime-on-the-economy (mode of access: 02.04.2024).
4. Counter-espionage Law of the People's Republic of China // China law translate: [website]. – 2023. – Apr. 26. – URL: https://www.chinalawtranslate.com/en/counter-espionage-law-2023/ (mode of access: 02.04.2024).
5. Gong J. What You Need to Know about China’s Counter-Espionage Law/ J. Gong // The Bird&Bird: [website]. – 2023. – Nov. 8. – URL: https://www.twobirds.com/en/insights/2023/china/what-you-need-to-know-about-chinas-counter-espionage-law/ (mode of access: 02.04.2024).
6. Dingding C. 3 Types of Chinese Reactions to Mike Pence’s China Speech // The Diplomat: [website]. – 2018. – Oct. 7. – URL: https://thediplomat.com/2018/10/3-types-of-chinese-reactions-to-mike-pences-china-speech/ (mode of access: 02.04.2024).

7. Economic Espionage Act of 1996. // Congress [website]. – 1996. – Oct. 11. – URL: https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf (mode of access: 02.04.2024).
8. Eftimiades N. The impact of Chinese espionage on the United States // The Diplomat [website]. – 2018. –Dec. 4. – URL: https://thediplomat.com/2018/12/the-impact-of-chinese-espionage-on-the-united-states/ (mode of access: 02.04.2024).
9. Federal Bureau of Investigation: official website. – URL: https://www.fbi.gov/about/faqs/what-is-economic-espionage/ (mode of access: 02.04.2024). – Text: electronic.
10. West B. Understanding Economic Espionage: The Present // Stratfor [website]. – 2021. – Feb. 23. – URL: https://worldview.stratfor.com/article/understanding-economic-espionage-present (mode of access: 02.04.2024).

References

1. Current cyber threats for Asian countries: 2022-2023. – Text: electronic //Positive Technologies [website]. – 2021. – 12 Sep. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/asia-cybersecurity-threatscape-2022-2023/ (mode of access: 02.04.2024).
2. Tyshova A.S. International experience in countering economic crimes committed in cyberspace // Transformation of the national socio-economic system of Russia: Materials of the V International Scientific and Practical Conference, Moscow, December 02, 2022. – Moscow: Russian State University of Justice, 2023. – Pp. 321-326. – EDN FGUEAY.
3. Chin K. The Impact of Cybercrime on the Economy // UpGuard [website]. – 2023. – May 18. – URL: https://www.upguard.com/blog/the-impact-of-cybercrime-on-the-economy (mode of access: 02.04.2024).
4. Counter-espionage Law of the People's Republic of China // China law translate: [website]. – 2023. – Apr. 26. – URL: https://www.chinalawtranslate.com/en/counter-espionage-law-2023/ (mode of access: 02.04.2024).
5. Gong J. What You Need to Know about China’s Counter-Espionage Law/ J. Gong // The Bird&Bird: [website]. – 2023. – Nov. 8. – URL: https://www.twobirds.com/en/insights/2023/china/what-you-need-to-know-about-chinas-counter-espionage-law/ (mode of access: 02.04.2024).
6. Dingding C. 3 Types of Chinese Reactions to Mike Pence’s China Speech // The Diplomat: [website]. – 2018. – Oct. 7. – URL: https://thediplomat.com/2018/10/3-types-of-chinese-reactions-to-mike-pences-china-speech/ (mode of access: 02.04.2024).
7. Economic Espionage Act of 1996. // Congress [website]. – 1996. –Oct. 11. – URL: https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf (mode of access: 02.04.2024).
8. Eftimiades N. The impact of Chinese espionage on the United States // The Diplomat [website]. – 2018. –Dec. 4. – URL: https://thediplomat.com/2018/12/the-impact-of-chinese-espionage-on-the-united-states/ (mode of access: 02.04.2024).
9. Federal Bureau of Investigation: official website. – URL: https://www.fbi.gov/about/faqs/what-is-economic-espionage/ (mode of access: 02.04.2024). – Text: electronic.

10. West B. Understanding Economic Espionage: The Present // Stratfor [website]. – 2021. – Feb. 23. – URL: https://worldview.stratfor.com/article/understanding-economic-espionage-present (mode of access: 02.04.2024).

Поступила в редакцию 5 апреля 2024 г.