Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2022, 2: 18–24

DOI 10.26163/GIEF.2022.51.76.003
УДК 327.84:343.9.018

O.V. Kharchenko

COUNTERING INDUSTRIAL ESPIONAGE AS A THREAT TO ECONOMIC SECURITY: CRIMINOLOGICAL STUDY

Oleg Kharchenko – Professor, the Department of Criminal Law, State Institute of Economics, Finance, Law and Technology, PhD in Law, Professor, Gatchina; **e-mail: prof.o.v.kharchenko@gmail.com**.

The article discusses some problematic issues dealing with industrial espionage as a threat to economic security. Based on a comparative analysis of major statistical data on the state of crime in the sphere of entrepreneurial activity for the period 2020-2021 and judicial practice of 2017-2020 in Russia, the main problems arising in the prevention of crimes under Article 183 of the Criminal Code of the Russian Federation (Illegal receipt and disclosure of information constituting commercial, tax or banking secrets) are formulated. These problems include the high level of latency of this type of crimes; the use of modern technologies by criminals; the complexity of the investigation; insignificant judicial practice. The article concludes with the author's proposals for solving the problems under consideration: expanding the powers of law enforcement agencies that control and combat the illegal receipt and disclosure of information constituting commercial, tax or banking secrets; development of forensic techniques; generalization of investigative and judicial practice; holding scientific and practical conferences.

Keywords: *economic security; crimes in the sphere of economic activity; illegal receipt and disclosure of information constituting commercial; tax or banking secrets; industrial espionage; criminological analysis; judicial practice.*

О.В. Харченко

ПРОТИВОДЕЙСТВИЕ ПРОМЫШЛЕННОМУ ШПИОНАЖУ КАК УГРОЗЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ: КРИМИНОЛОГИЧЕСКОЕ ИССЛЕДОВАНИЕ

Олег Витальевич Харченко – профессор кафедры уголовно-правовых дисциплин, Государственный институт экономики, финансов, права и технологий, кандидат юридических наук, профессор, г. Гатчина; **e-mail: prof.o.v.kharchenko@gmail.com**.

Рассмотрены отдельные проблемы, связанные с промышленным шпионажем как угрозой экономической безопасности. На основе сравнительного анализа основных статистических данных о состоянии преступлений в сфере предпринимательской деятельности за 2020–2021 гг. и судебной практики 2017–2020 гг. в России сформулированы основные проблемы, возникающие при предупреждении преступлений, предусмотренных ст. 183 УК РФ («Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»). К числу данных проблем относятся: высокий уровень латентности данного вида преступлений; использование преступниками современных технологий; сложность расследования; незначительная судебная практика.

Даны авторские предложения по решению рассматриваемых проблем: расширение полномочий правоохранительных органов, осуществляющих контроль и борьбу с незаконным получением и разглашением сведений, составляющих коммерческую, налоговую или банковскую тайну; разработка криминалистических методик; обобщение следственной и судебной практики; проведение научно-практических конференций.

Ключевые слова: *экономическая безопасность; преступления в сфере экономической деятельности; незаконное получение и разглашении сведений; составляющих коммерче-*

скую, налоговую или банковскую тайну; промышленный шпионаж; криминологический анализ; судебная практика.

Одним из показателей состояния экономической безопасности является уровень преступности в сфере экономики, поэтому важное значение приобретают криминологические исследования преступлений в сфере экономики, и в частности, – в сфере экономической деятельности. Так, криминологический анализ динамики преступлений в сфере экономической деятельности за 2020–2021 гг. показывает стабильную тенденцию к увеличению числа выявляемых преступлений данного вида. В 2021 г. зарегистрировано 40 706 преступлений в сфере экономической деятельности, что на 2,8% больше, чем за 2020 г., а удельный вес этих преступлений в общем числе зарегистрированных преступлений экономической направленности увеличился до 34,6%. Предварительно расследовано 16 236 (+10,2%) уголовных дел о рассматриваемых преступлениях, из них направлены в суд – 10 150 (+27,1%), при этом выявлено лиц, уголовные дела о которых направлены в суд, – 8 329 (+33,1%) [15; 16]. Таким образом, следует отметить эффективную работу правоохранительных органов, которая привела к увеличению удельного веса уголовных дел и выявленных лиц, направляемых в суд за совершение преступлений в сфере экономической деятельности, что обеспечивает экономическую безопасность как государства, так и предприятий.

Одним из элементов экономической безопасности предприятий выступает система противодействия промышленному шпионажу. Угрозы могут исходить как из источников, лежащих за пределами влияния предприятия, так и со стороны элементов, на которые организация может оказывать прямое воздействие (это, прежде всего, сотрудники, уровень охраны материальных объектов и информации). Поэтому большинство исследователей при этом выделяет классификацию угроз экономической безопасности на внешние и внутренние.

Можно отдельно обозначить угрозы, характерные именно для промышленных предприятий, которые, в том числе, служат факторами возникновения промышленного шпионажа. Данные угрозы чаще всего возникают вследствие внутренней недостаточно корректно выстроенной системы взаимодействия с государственными органами, а также неэффективной кадровой политики.

Необходимо отметить, что существует ряд макроэкономических факторов, которые усиливают угрозы экономической безопасности и не поддаются прямому влиянию на уровне предприятия, однако являются обязательными к учету с целью наиболее эффективного управления экономической безопасностью. Указанные факторы являются следствием общеэкономических тенденций как в нашем государстве, так и в общемировом пространстве, они оказывают влияние на деятельность всех предприятий, занимающихся хозяйственной деятельностью.

Сегодня, как никогда, становится актуальным создание систем экономической безопасности, которые представляют собой комплекс мер (организационные, управленческие, технологические и т.д.), направленных на реализацию интересов предприятия, а также их защиты от внешних и внутренних угроз. Одной из таких угроз выступает промышленный шпионаж. В настоящее время у промышленного шпионажа нет легального толкования. В качестве доктринального толкования предлагаются различные определения.

Промышленный шпионаж – это добыча, кража секретной производственной информации у конкурентов с целью получения лучших результатов (в предпринимательской деятельности, при производстве того или иного товара) в своей деятельности и хорошей прибыли, превышающей в разы прибыль конкурента [5, с. 133].

Промышленный шпионаж – это тайный и в основном незаконный сбор информации о конкурентах с одной лишь целью – получить преимущество в предпринимательской деятельности (как правило, в одной промышленной области) и получить материальную выгоду [17, с. 94].

Промышленный шпионаж – это практика расследования деятельности конкурентов с целью получения преимущества в бизнесе [4, с. 112].

Промышленный шпионаж – это недобросовестная конкуренция, при которой происходит незаконное получение, использование, разглашение какой-либо информации, которая содержит экономическую (коммерческую), служебную тайну, с целью получения преимущества перед конкурентами и получения финансовой выгоды [6, с. 15].

Промышленный шпионаж рассматривают как незаконное завладение инновационными технологиями или любой информации, являющейся коммерческой тайной. Под коммерческой тайной стоит понимать любую информацию о деятельности предприятия или компании, обнародование которой (либо попадание к конкурентам) нанесет сильный финансовый урон. Как правило, речь идет об инновационных разработках, изобретениях, новых технологиях, революционных маркетинговых ходах и т.п. То есть, промышленный шпионаж – это воровство одной компанией секретов другой компании с целью победы в конкурентной борьбе.

Таким образом, промышленный шпионаж следует рассматривать как вид незаконной деятельности, подразумевающий завладение сведениями, составляющими коммерческую, налоговую или банковскую тайну, если это причинило ущерб обладателю.

На крупных предприятиях существуют отделы внутренней безопасности, они следят за правомерными действиями сотрудников и лиц, которые могут проникнуть на контролируемый объект. На таких предприятиях осуществляется пропускная система, и попасть туда достаточно сложно. Все сотрудники подписывают договоры о неразглашении, и им запрещено делиться производственной и конфиденциальной информацией.

Промышленный шпионаж присутствует во всех отраслях производства: в банках, медицине, на фирмах и в разного рода направлениях компаний. Экономический шпионаж – это не только кража важной информации из сейфа или с жесткого диска, но и похищение людей, владеющих этой информацией (конструкторы, биологи, химики, программисты), к примеру, тех, которые нужны в мире технологий или для изготовления новой таблетки. В промышленном шпионаже применяют все методы для добычи важной информации – это может быть шантаж, вербовка, подкуп и др.

Промышленному шпионажу чаще всего подвергаются индустрия информационных технологий (далее – IT), компьютерная, энергетическая, промышленная, аэрокосмическая и химическая отрасли. Также следует упомянуть широкое распространение промышленного шпионажа в области экономики и финансов как на уровне частных компаний, так и на государственном уровне.

Промышленный шпионаж позволяет сэкономить как время, так и средства, которые должен заплатить нечестный предприниматель, чтобы догнать и опередить своего конкурента, занимающего лидирующие позиции. То есть, если у конкурента идет развитие, и у него имеется новейшая технологическая разработка, которая дает свои плоды, то другая организация может не утруждать себя в создании такой же технологии, а может незаконным путем похитить разработки своего конкурента и выйти на новые для себя рынки.

Данное деяние влечет уголовную ответственность, виновный привлекается по ст. 183 Уголовного кодекса Российской Федерации (далее – УК РФ) за незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну [1].

Криминологический анализ судебной практики по данному составу преступления показывает, что на этапе предварительного расследования существуют определенные проблемы. Так, в России по ст. 183 УК РФ осуждено (по основной статье): в 2017 г. – 37, в 2018 г. – 22, а в 2019 – 43 человека [10; 11; 12]. В 2020 г. осуждено по основной статье (ст. 183 УК РФ) – 35 человек, а по дополнительной квалификации – 25, при этом число лиц, в отношении которых уголовные дела прекращены по иным основаниям по основной статье, – 47 и по допол-

нительной квалификации – 15 [13].

Криминологический анализ личности показывает, что среди осужденных в 2020 г. (по основной статье 35 человек): женщины составили 7 человек (20%); по возрастным группам: 18–24 года – 15 чел. (42,9%), 30–49 лет – 12 (34,2%) и 25–29 лет – 8 чел. (22,9%); по образованию: высшее образование – 21 чел. (60%), среднее профессиональное – 8 (22,9%), среднее общее – 5 (14,3%); лица, осуществляющие предпринимательскую деятельность, – 10 чел. (28,6%). Таким образом, можно составить криминологический портрет лица, осужденного за промышленный шпионаж: мужчина (80%), возраст – 18–29 лет (65,8%).

Цель промышленного шпионажа заключается в опережении своего конкурента в рыночных позициях, в экономии денежных средств на приобретении ценных технологий, в привлечении большего числа покупателей своего продукта [7, с. 262].

Выделяют также узкие задачи, которые решают с помощью промышленного шпионажа:

- устранение конкурентов;
- добыча клиентской базы компании-конкурента и переманивание клиентов;
- подделка товаров;
- подготовка ответа на различные маркетинговые ходы конкурентов;
- выдерживание ценовой конкуренции, заранее зная о ценовой политике компаний-конкурентов;
- разработка новых инновационных продуктов;
- разведка торговых секретов;
- получение информации о клиенте и др.

Данные конкурентов, включая их финансовую информацию, могут быть использованы для кражи бизнеса или утечки, чтобы повредить репутацию компании. Финансовая информация о компании может быть использована для того, чтобы рекомендовать лучшие предложения клиентам и партнерам, выигрывать предложения и даже делать лучшие предложения ценным сотрудникам. Получение маркетинговой информации позволяет конкурентам подготовить своевременный ответ для маркетинговых кампаний, что, в свою очередь, может сделать их неэффективными.

Вместе с тем существует несколько видов промышленного шпионажа [9, с. 263]:

- государственный шпионаж – это кража, изъятие информации, являющейся экономической и военной тайной с целью передачи зарубежным организациям;
- экономический шпионаж – это сбор информации о состоянии организации с помощью подкупных лиц, взлома базы данных с последующим массовым оглашением ее обществу;
- шпионаж в Интернете – это сбор конфиденциальной информации об интернет-пользователях с помощью специальных программ;
- мобильный шпионаж – это установка в смартфоны специальных программ, устройств, которые могут определить, где находится человек, с кем он разговаривает и переписывается.

Существует и разрешенный мобильный шпионаж – применяется в том случае, когда потерялся человек.

К методам промышленного шпионажа можно отнести следующие [14, с. 34]:

- подкуп лица, который имеет доступ к необходимой информации;
- шантаж лиц, которые также имеют доступ к необходимой информации;
- внедрение своего человека на предприятие конкурента, который все разведает и соберет необходимую информацию или получит доступ к продукции, интересующей организацию;
- прослушивание телефонов, проникновение в компьютерные сети и т.д.;
- наружное наблюдение;
- техническое наблюдение, к примеру, при помощи беспилотников;
- слежка за объектом, включая видео- и фотонаблюдение, а также прослушивание;
- хакерские атаки на сайт компании;
- кража флеш-накопителей или жестких дисков с данными;
- и др.

Промышленный шпионаж (он же экономический шпионаж, или корпоративный шпионаж) определяется как случай, когда одна компания крадет секреты другой ком-

пании, с которой она конкурирует. Эта форма шпионажа не является вопросом национальной безопасности.

Несмотря на явно значительные потери предприятий в результате промышленного шпионажа, пострадавшие чаще не афишируют такие ситуации.

Причины, из-за которых большинство компаний не сообщает о случаях промышленного шпионажа:

1. Промышленный шпионаж доказать сложно. Часто он осуществляется инсайдерами, которые уже имеют доступ к конфиденциальным данным. Шпионская деятельность почти неотличима от обычной повседневной деятельности, поэтому ее трудно обнаружить и еще труднее доказать в суде.

2. Трудно привлечь виновных к ответственности. Поскольку законы о коммерческой тайне и промышленном шпионаже повсюду различны, может оказаться очень трудным привлечь к ответственности иностранные компании и правительства. Даже если преступник находится внутри страны, они могут продлить судебные процедуры до такой степени, что компания, подавшая иск, не сможет продолжить рассмотрение дела.

3. Это может негативно повлиять на акции компаний. Стоимость их может упасть, если станет известно, что ее безопасность была нарушена. Это может подорвать доверие инвесторов и клиентов.

4. Это можно рассматривать как разглашение информации. Компания несет ответственность за обеспечение безопасности конфиденциальных данных своих клиентов. В некоторых странах и отраслях, если эти данные будут утеряны или украдены промышленными шпионами, компания будет оштрафована.

В 2021 г., в сравнении с 2012 г., количество зарегистрированных преступлений, которые были совершенны с использованием информационно-телекоммуникационных технологий или в компьютерной сфере, увеличилось более чем в 50 раз (в 2012 г. – 10,2 тыс., в 2021 г. – 517,7 тыс.), а их удельный вес возрос до 25,8% (2020 г. – 25,8%). Подавляющее большинство всех «киберпреступлений» носило имущественный характер. Свыше трех четвертей (78,4%) совершается путем кражи или мошенничества – 406,0 тыс. [16].

В результате принятых в 2021 г. мер раскрыто 118 920 преступлений рассматриваемой категории (+25,3%), в суд направлено 111 125 уголовных дел (+33,9%), выявлено 86 696 лиц, совершивших указанные преступления (+32,0%). Раскрыто 21,6 тыс. из 249,2 тыс. IT-мошенничеств (-0,1%) и 41,9 тыс. IT-краж (+60,2%) [16].

В целях противодействия IT-преступлениям МВД России совершенствует законодательную и ведомственную нормативные базы, позволяющие выстраивать оптимальные алгоритмы их выявления, раскрытия и расследования с учетом появляющихся новых форм и методов подготовки, совершения и сокрытия таких деяний.

Так, с 1 июля 2020 г. вступили в силу внесенные в национальное законодательство изменения, ужесточающие требования к порядку выдачи электронной цифровой подписи и ее использования при подписании документов различными субъектами. Федеральным законом «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 г. № 259-ФЗ установлены правила выпуска цифровых финансовых активов, оборота цифровой валюты (криптовалюты), а также запрет на прием цифровой валюты в качестве оплаты товаров, работ и услуг [2].

Важность проблемы обусловила ее рассмотрение также на оперативных совещаниях Совета Безопасности Российской Федерации, где Президентом Российской Федерации даны поручения ведомствам по вопросам борьбы с киберпреступностью по усилению противодействия имущественным преступлениям, в том числе мошенничествам и продажам фальсифицированных лекарств, а также по расширению соответствующей социальной рекламы в сети «Интернет», ориентированной на профилактику преступлений.

Во исполнение Указа Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» и на-

циональной программы «Цифровая экономика Российской Федерации» проводятся мероприятия по созданию системы центров обработки данных МВД России [3; 8].

В рамках цифровой трансформации государственного управления и государственных услуг разработана ведомственная программа цифровой трансформации МВД России на 2021–2023 гг. В целях информационного обеспечения органов внутренних дел проводится совершенствование общесистемных и прикладных сервисов единой системы информационно-аналитического обеспечения деятельности МВД России, функционирующих в интересах служб и подразделений органов внутренних дел, к которой посредством проводных, спутниковых и беспроводных каналов связи подключены пользователи. Обеспечивается информационная безопасность технологической инфраструктуры органов внутренних дел, развивается электронное взаимодействие с органами государственной власти и организациями.

Защита в области промышленного шпионажа с целью обеспечения информационной безопасности для предприятий промышленного комплекса является необходимой и актуальной. Экономическая безопасность представляет собой совокупность отдельных ее элементов, каждый из которых связан с определенным аспектом деятельности предприятия, который может подвергаться воздействию конкретных угроз. Важнейшим элементом является информационная безопасность, которая подразумевает необходимость защиты конфиденциальной информации и цифровых данных предприятия.

Как отмечено выше, промышленный шпионаж – это вид незаконной деятельности, подразумевающий завладение сведениями, составляющими коммерческую, налоговую или банковскую тайну, если это причинило ущерб обладателю. Также промышленный шпионаж следует рассматривать как один из видов недобросовестной конкуренции, осуществляемый с целью похищения секретной информации относительно новой продукции, способов ее изготовления, либо др. элементов деятельности предприятия.

Промышленный шпионаж преследует следующие основные цели:

- устранение конкурента;
- завоевание рынка;
- получение материальной выгоды.

Влияние промышленного шпионажа на деятельность предприятий весьма негативно, поскольку возможна как утечка данных и построение на этом системы повышения конкурентоспособности у конкурентов, так и вывод из строя основных информационных систем и баз предприятия, которое не позволит ему нормально функционировать. Данный вопрос приобрел очень важное масштабное значение в рамках государства, в последние годы на высшем законодательном уровне ему уделяется большое внимание, вследствие чего принимаются соответствующие нормативно-правовые акты.

С целью эффективной борьбы с незаконным получением и разглашением сведений, составляющих коммерческую, налоговую или банковскую тайну, необходимо внедрение следующих мероприятий:

- повышение «цифровой грамотности» населения на различных уровнях (в высших учебных заведениях), для чего необходимо включение в программу дисциплины или темы, направленной против преступлений в сфере экономической деятельности;
- развитие более эффективного взаимодействия правоохранительных органов, осуществляющих борьбу с незаконным получением и разглашением сведений, составляющих коммерческую, налоговую или банковскую тайну;
- разработка криминалистических методик расследования преступлений о незаконном получении и разглашении сведений, составляющих коммерческую, налоговую или банковскую тайну;
- обобщение следственной и судебной практики, проведение научно-практических конференций.

ЛИТЕРАТУРА

1. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru/ (дата

обращения: 29.03.2022).

2. Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 г. № 259-ФЗ // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru/ (дата обращения: 29.03.2022).

3. Указ Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Официальный интернет-портал правовой информации. – URL:http://pravo.gov.ru/ (дата обращения: 29.03.2022).

4. *Грунин О.А.* Экономическая безопасность организации / О.А. Грунин, С.О. Грунин. – СПб.: Питер, 2002. – 160 с.

5. *Джилад Б.* Конкурентная разведка. Как распознать внешние риски и управлять ситуацией / Б. Джилад. – СПб: Питер, 2010. – 320с.

6. *Каторин Ю.Ф.* Большая энциклопедия промышленного шпионажа / Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко. – СПб.: Полигон, 2000. – 885 с.

7. *Манохина Н.В.* Экономическая безопасность / под ред. Н.В. Манохиной. – М.: ИНФРА–М, 2017. – 320 с.

8. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 г. № 7). Доступ из справ.-правовой системы «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_328854/ (дата обращения 13.03.2022).

9. *Одинцов А.А.* Экономическая и информационная безопасность предпринимательства / А.А. Одинцов. – М.: Академия, 2008. – 333 с.

10. Отчет о числе осужденных по всем составам преступлений УК РФ и иных лиц, в отношении которых вынесены судебные акты по уголовным делам за 12 месяцев 2017 г. (Форма № 10-а) // Судебный департамент при Верховном Суде Российской Федерации: [сайт]. – URL: http://www.cdep.ru/index.php?id=79&item=5669 (дата обращения: 30.03.2022).

11. Отчет о числе осужденных по всем составам преступлений УК РФ и иных лиц, в отношении которых вынесены судебные акты по уголовным делам за 12 месяцев 2018 г. (Форма № 10-а) // Судебный департамент при Верховном Суде Российской Федерации: [сайт]. – URL: http://www.cdep.ru/index.php?id=79&item=5669 (дата обращения: 30.03.2022).

12. Отчет о числе осужденных по всем составам преступлений УК РФ и иных лиц, в отношении которых вынесены судебные акты по уголовным делам за 12 месяцев 2019 г. (Форма № 10-а) // Судебный департамент при Верховном Суде Российской Федерации: [сайт]. – URL: http://www.cdep.ru/index.php?id=79&item=5669 (дата обращения: 30.03.2022).

13. Отчет о числе осужденных по всем составам преступлений УК РФ и иных лиц, в отношении которых вынесены судебные акты по уголовным делам за 12 месяцев 2020 г. (Форма № 10-а) // Судебный департамент при Верховном Суде Российской Федерации: [сайт]. – URL: http://www.cdep.ru/index.php?id=79&item=5669 (дата обращения: 30.03.2022).

14. *Роберт С. Кэмп.* Легальный промышленный шпионаж. Бенчмаркинг бизнес-процессов: технологии поиска и внедрение лучших методов работы ваших конкурентов / Роберт С. Кэмп. – М.: Баланс–Клуб, 2004. – 416 с.

15. Состояние преступности в Российской Федерации за январь–декабрь 2020 года // Министерство внутренних дел Российской Федерации: [сайт]. – URL: https://мвд.рф (дата обращения: 30.03.2022).

16. Состояние преступности в Российской Федерации за январь–декабрь 2021 года // Министерство внутренних дел Российской Федерации: [сайт]. – URL: https://мвд.рф (дата обращения: 30.03.2022).

17. *Ярочкин В.И.* Технические каналы утечки информации / В.И. Ярочкин. – М.: ИПКИР, 1994. – 105 с.