Интернет-журнал «Отходы и ресурсы» https://resources.today
Russian Journal of Resources, Conservation and Recycling

2022, Том 9, № 4 / 2022, Vol 9, No 4 https://resources.today/issue-4-2022.html

URL статьи: https://resources.today/PDF/39ECOR422.pdf

DOI: 10.15862/39ECOR422 (https://doi.org/10.15862/39ECOR422)

Ссылка для цитирования этой статьи:
Лебедев, И. А. Этическая трансформация и правовые границы экономической разведки / И. А. Лебедев, В. И. Прасолов // Отходы и ресурсы. — 2022. — Т. 9. — № 4. — URL: https://resources.today/PDF/39ECOR422.pdf DOI: 10.15862/39ECOR422

For citation:
Lebedev I.A., Prasolov V.I. Ethical transformation and legal boundaries of economic intelligence. *Russian Journal of Resources, Conservation and Recycling*. 2022; 9(4): 39ECOR422. Available at: https://resources.today/PDF/39ECOR422.pdf. (In Russ., abstract in Eng.) DOI: 10.15862/39ECOR422

УДК 338

Лебедев Игорь Александрович
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Руководитель и доцент Департамента экономической безопасности и управления рисками
Кандидат экономических наук, доцент
E-mail: ILebedev@fa.ru

Прасолов Валерий Иванович
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Доцент Департамента экономической безопасности и управления рисками
Кандидат политических наук, доцент
E-mail: VIPrasolov@fa.ru

Этическая трансформация и правовые границы экономической разведки

Аннотация. В рамках данной статьи авторами рассмотрен вопрос, касающийся осуществления экономической разведки в современных условиях. На фоне экономического противостояния западных стран и России становится очевидным, что понятие экономической разведки изменяется, проявляя себя в нескольких плоскостях одновременно, а корпоративное противостояние переходит на уровень защиты национальных интересов. По мнению авторов, изменениям подвержены факторы, влияющие на восприятие методов корпоративного противостояния. Исходя из предположения о том, что методы и тактические приемы экономической разведки не являются статичными, авторы в данном исследовании ставят перед собой задачу определения факторов, оказывающих влияние на их этическое восприятие. В исследовании приводится мнение о том, что трансформации подходов к пониманию этичного поведения и самому определению этичного поведения в экономической разведке напрямую связаны с технологическим аспектом, переходом многих бизнес-процессов в цифровую плоскость. Авторы акцентируют внимание на том, что в условиях киберпространства существенно меняется психологическое восприятие противоправных действий. Приверженность этичному поведению может закономерно снизиться вследствие отсутствия личного контакта между агентом воздействия и источником. В то же время на практике граница, разделяющая этичные и неэтичные методы ведения конкурентной разведки, остается весьма нечеткой, что создает дополнительные трудности в вопросах противодействия таким методам. В заключительной части статьи авторы формулируют вывод относительно наиболее

распространенных угроз, которым подвержены корпоративные данные, а также роли экономической разведки в обеспечении безопасности организации.

Ключевые слова: конкурентная разведка; корпоративный шпионаж; этика; утечка информации; электронные средства связи; экономическая безопасность; этичное поведение; методы корпоративного противостояния; цифровизация экономики; бизнес-процессы

Введение

Актуальность темы экономической разведки на протяжении истории никогда не снижалась. В широком смысле понятие «разведка» принято определять, как деятельность, связанную со сбором сведений о противнике или конкуренте в целях обеспечения собственной безопасности и получения преимуществ в сферах осуществления общей деятельности, конкуренции [1]. Эволюция разведывательной деятельности, уходящей корнями глубоко в историю, пошла по двум направлениям. В первом случае речь идет о государственной разведке и контрразведке, во втором второе — о частной разведывательной деятельности, деловой разведке [2]. Несмотря на современную критику взглядов Маркса в определении экономики и политики как «базиса-надстройки», нельзя не согласиться с тем, что экономика лежит в основе общественного развития, следовательно, вопросы устойчивости экономики, экономической безопасности на любом уровне имеют характер стратегических [3].

В большинстве случаев конкурентную разведку отождествляют с промышленным шпионажем, однако в отличие от последнего практика конкурентной разведки основывается на этичности и законности исследований и сбора информации [4]. Этикой в условиях конкурентной разведки принято называть добровольно взятые на себя обязательства со стороны участников рынка по использованию таких форм и методов работы, которые, не предполагают нанесения умышленного непосредственного вреда конкурентам, создания угроз общественной безопасности. Предполагается, что субъект экономической разведки будет добиваться нужного результата, не выходя за рамки действующего правового регулирования и не создавая объективных оснований для обвинений со стороны других участников рынка конкурентной разведки, государства и общества [5].

Четвертая технологическая революция в значительной мере меняет общественный уклад большинства стран мира. На фоне научно-технического прогресса трансформация экономики происходит практически на всех уровнях. В то же время технологии, упрощающие процессы управления компаниями, создают новые вызовы, два из которых, на наш взгляд, являются ключевыми. В первую очередь, это проблема защищенности электронных ресурсов и технологий, и вторая — кадровая проблема. Если во втором случае, когда речь идет об изменение обязанностей сотрудников и исчезновение некоторых профессий в связи с информатизацией, проблема в большей степени имеет характер потенциальной, то с первой предприятия имеют дело уже сегодня. В условиях, когда доступность и оперативность обмена информацией усиливается, защита данных приобретает особую актуальность. Интернет, обеспечивающий удобство и скорость при обмене информацией, лишает людей анонимности. Такие достижения информационно коммуникативных технологий в сфере трудовых отношений как виртуальные рабочие места, удаленный доступ к хранилищам данных для работников повышают риск корпоративного шпионажа. С каждым годом инструментарий киберпреступности пополняется, поэтому важно, чтобы меры противодействия информационным преступлениям развивалась интенсивнее [6]. Необходимо противодействовать потребителям, желающим сэкономить путем установки нелицензионного программного обеспечения, в результате чего такие потребители нередко становится жертвой киберпреступников. Возможности корпоративной разведки также расширяются: к примеру,

еще 15 лет назад понятие аналитики социальных сетей было малоизвестным, а доступ к онлайн-реестрам по таким направлениям как информация об арестованном имуществе фирм во многих странах отсутствует по сей день [7].

Возрастание потребностей в получении инсайдерской информации пропорционально увеличивает значение этических норм, ставя субъектов экономической разведки перед известным компромиссом в плоскости «цель-средства». При возникновении проблем с получением конфиденциальных данных у специалистов деловой разведки могут проявиться побуждающие мотивы к нарушению этических ограничений. Поскольку бизнес в широком понимании термина непрерывно развивается и становится все более изощренным, а его коммерческие секреты меняются, компании предстают перед необходимостью периодически пересматривать свои меры защиты, чтобы попытаться обеспечить их соответствие и соразмерность возникающим угрозам [8].

В этом отношении возникает вопрос о том, в чем преимущества соблюдения этических норм. Приверженность соблюдению этических норм является не только правильной с моральной точки зрения, но и, в широком понимании несет экономическую выгоду. Помимо репутационных издержек следование этическим нормам способно уберечь предприятие от судебного разбирательства и связанных с ним затрат.

В последние годы, на фоне усиливающегося противостояния hi-tech гигантов, вопрос об этико-правовых границах в экономической разведке приобрел особую актуальность. Особый резонанс приобрело дело, касающееся обвинений в корпоративном шпионаже в адрес китайского телекоммуникационного гиганта Huawei. Компании были предъявлены федеральные обвинения США в связи с тем, что прокуратура называет многолетним заговором с целью кражи коммерческих секретов. В 2020 году Министерство юстиции США предъявило Huawei обвинительное заключение по 16 пунктам обвинения, которое включало обвинения в соответствии с Законом о коррумпированных и находящихся под влиянием рэкетиров организациях (RICO). В обвинительном заключении утверждается, что еще в 2000 году Huawei украла коммерческую тайну как минимум шести американских компаний. Названия компаний не называются, однако предыдущие иски Cisco и Motorola против китайской компании отражены в обвинительном заключении [9]. Как видно, на сегодняшний день экономическая разведка не только не ограничивается корпоративной сферой, но имеет межгосударственный характер плотно пересекаясь со сферой государственной безопасности, государственных интересов. При этом складывается ситуация, когда государственная экономическая контрразведка сталкивается не с «симметричной» экономической разведкой стран-соперниц на уровне правительственных агентств (органов), а с разведывательными мерами корпоративного сектора.

Современные исследования в сфере этико-правовых аспектов экономической разведки посвящены таким вопросам как влияние промышленного шпионажа на процессы слияния и поглощения, роль аналитики социальных сетей в обеспечении конкурентной разведки, роль экономической разведки в вопросах формирования корпоративных стратегий, системный анализ корпоративной разведки, изучение перспектив развития сферы экономической разведки и промышленного шпионажа, меры противодействия промышленному шпионажу. Принимая во внимание изменения методов и тактических приемов экономической разведки, исследование ставит своей задачей определить факторы, влияющие на их этическое восприятие.

Цель данного исследования предполагает изучение трансформации подходов к пониманию этичного поведения в экономической разведке в условиях существующих правовых ограничений.

Объект исследования — расширение этико-правовых границ экономической разведки.

Предметом выступают подходы к пониманию этичного поведения в экономической разведке в современных условиях.

1. Методы и материалы

Для достижения поставленной цели был поставлен ряд задач:

- раскрыть сущность экономической безопасности;
- проанализировать принципы экономической разведки;
- выявить особенности промышленного шпионажа в современных условиях;
- рассмотреть взаимосвязь экономической разведки с мерами контрразведки на примере крупных компаний.

Данное исследование основывается на изучении и анализе международных и национальных законодательных актов в сфере противодействия недобросовестной конкуренции и промышленному шпионажу, включая Парижскую конвенцию по охране промышленной собственности, Закон США об экономическом шпионаже (EEA, 1996), Единый закон о коммерческой тайне («UTSA», 1979), Директива Европейского Парламента и Совета Европейского Союза 2016/943 от 08.06.2016 о защите конфиденциальных ноу-хау и деловой информации (коммерческой тайны) от незаконного приобретения, использования и раскрытия, а также аналитических материалов в данной сфере (Консультационный документ о неправомерном использовании коммерческих секретов Комиссии по законодательству Великобритании, 1997 г.).

Так как объект исследования находится на пересечении криминологии, этики, корпоративного и уголовного права данное исследование носит междисциплинарный характер. При помощи метода содержательного контент-анализа, а также историко-правового подхода в исследовании рассмотрен генезис и развитие понятия экономической разведки с точки зрения теоретических взглядов и с позиции практического применения в современной корпоративной отрасли. В работе рассматриваются факторы, влияющие на изменение представлений об этичности мер, предпринимаемых в рамках экономической разведки. Исследование ограничено рассмотрением экономической разведки в корпоративной сфере.

Особое внимание в рамках написания работы уделялось теоретическим положениям, разработанным отечественными авторами, в частности, Малеванкиной А.Д. [10], Иляковой И.Е. [11], Красовских О.П. [12] и другими.

2. Результаты и обсуждения

Политика экономической безопасности заключается в реализации мер по прогнозированию и предотвращению всех вероятных ситуаций, которые могут нарушить «жизнедеятельность» государств или частных компаний. Понятие экономической безопасности привлекает частное и общественное внимание, несмотря на трудности с ее определением. Дать определение экономической безопасности непросто, поскольку оно затрагивает множество вопросов, которые имеют большую или меньшую степень важности, в зависимости от ситуации, сопутствующего контекста, среды осуществления экономической деятельности и пр.

Исходя из сущности понятия «безопасность», как состояния отсутствия угроз не подлежит противоречиям тезис о том, что состояние безопасности в наибольшей степени обусловлено возможностью и способностью предусмотреть опасность и оградить себя от нее,

предоставив возможность экономическому субъекту устойчиво развиваться в настоящее время и в перспективе. Это, в свою очередь, требует осуществления сбора и анализа информации о существующих и потенциальных угрозах — разведывательной деятельности. Способность создать условия для защиты от угроз экономики (экономических интересов) — задача экономической разведки. В современных исследованиях наряду с термином «экономическая разведка» используются термины «конкурентная разведка», «корпоративная разведка» «бизнес-разведка», далее эти термины будут обобщены в ЭР — экономическую разведку.

Экономическая разведка представляет собой часть корпоративной культуры осуществления современной предпринимательской деятельности. В условиях конкурентной борьбы наибольшее значение играет разведка намерений конкурентов. Отсутствие информации о деятельности и намерениях соперника существенно снижает шансы на успех в конкурентной борьбе. Напротив, информированность о действиях конкурента может дать не только краткосрочный тактический перевес, но и открывает возможности одержать верх над конкурентами в долгосрочной перспективе. Неудивительно, что во все времена экономическая разведка являлась преобладающим инструментом исследования рынка и конкурентной среды. ЭР, означает понимание и изучение того, что происходит за пределами собственного бизнеса, с целью сделать его максимально конкурентоспособным. Процесс сбора и анализа информации способствует предприятию в разработке собственной стратегии или выявлению недостатков, которые могут стать преградой для формирования конкурентных преимуществ [13].

В современных исследованиях подход к определению ЭР как правило схож. При этом ЭР принято соотносить с понятием конкурентной разведки. Несмотря на то, что ЭР иногда описывается как более широкое понятие (поскольку ЭР может подразумевать и другие цели — технические, связанные с коммерческим ноу-хау и пр.), тем не менее, преимущественно эти понятия отождествляются. Это в свою очередь обусловлено тем, что в коммерческой среде конечной и непосредственной целью выступает именно получение финансовой прибыли, обусловливающей причины и суть конкуренции. В частности, конкурентная разведка определяется как систематический процесс сбора, классификации, анализа и распространения информации о конкурентах, рынках и отрасли. ЭР защищена этическими и юридическими практиками и интегрирован в процесс принятия стратегических решений.

В настоящее время экономическая разведка признана профессиональным инструментом стратегии и управления для государств и компаний на фоне глобализации. Его реализация основана на трех основных принципах (столпах):

- сбор, обработка и анализ стратегически-значимой информации, с целью изучения «внешнего окружения» и предвидеть возможности воздействия на бизнес извне; этот принцип ассоциируют с наблюдением. Он составляет основу для двух других принципов;
- обеспечение экономической безопасности (подразумевает защитный характер, направлена на защиту экономических активов, особенно нематериальных);
- влияние (воздействие) — активное или наступательное — что означает быть в авангарде поиска возможностей и инноваций и иметь возможность воздействовать на свое окружение (правила, нормы, имидж), а не только пассивно зависеть от него.

Несмотря на то, что эти три принципа (столпа) в данном теоретическом разрезе рассматриваются отдельно, фактически они взаимозависимы и на практике, как правило, используются в рамках единой стратегии.

Под ЭР в современном корпоративном секторе понимается целенаправленный сбор и анализ данных о конкурентах и партнерах, основная цель которого состоит в выявлении объективной ситуации в компаниях, определении сильных и слабых стороны ведения предпринимательской деятельности, определении их целей и намерений. Ключевым различием между понятиями экономической разведки и промышленного шпионажа является то, что первая осуществляется в пределах правовой плоскости, а ее результаты становятся доступными благодаря анализу открытых (общедоступных) информационных источников. В то же время, вполне очевидно, что грань между этичными и неэтичными методами ведения конкурентной разведки может оставаться очень размытой, хотя в обоих случаях предполагается соблюдение правовых норм.

Рассматривая ЭР с точки зрения необходимости развития ее методов на предприятиях, в современных исследованиях утверждается, что наибольшая отдача от инвестиций, получаемая от эффективной ЭР, — это способность компании быстро адаптироваться к меняющимся рыночным условиям. Это способствует улучшению конкурентных позиций фирмы на рынке с точки зрения охвата профильного сегмента. Чтобы адаптироваться к меняющимся рыночным условиям, необходимо принимать естественные непрерывные процессы решений. Процесс принятия решений можно разделить на тактические и стратегические действия. Тактические действия включают в себя более мелкие решения, необходимые для ответа на вопросы операционного характера или возникающие проблемы, и поэтому связаны с более краткосрочной целью организации. Стратегические действия касаются решений, которые имеют более долгосрочное влияние на предприятие, что, разумеется, охватывает больший временной промежуток. Принятие стратегических, тактических решений и планирование могут быть улучшены за счет внедрения ЭР в организации.

ЭР, как правило, нацелена на применение различных инструментов в сфере анализа рынка (экономических, юридических и пр.) а также анализа и сравнения предприятия с его конкурентами с целью сделать последнее более конкурентоспособным и устойчивым к внешним потрясениям. В условиях глобализации конкуренции такие действия становятся особенно важными для бизнеса. Следует отметить, что понятия конкурентной разведки и шпионажа не являются тождественным, хотя, разумеется, конкурентная разведка и промышленный шпионаж имеют общие, связывающие их особенности. Как в первом, так и во втором случае, задачей является содействие в выработке решений и достижении конкурентных преимуществ. При этом основное различие в обоих случаях составляют их методы. В случае шпионажа — методы ориентированы на применение всего инструментария доступных средств для получения требуемой информации. К таковым может относиться и прямое нарушение законов (кража, хищение), и неэтичные методы (подкуп сотрудников, компромат). Методы ЭР исключают применение противозаконных (в частности, уголовно наказуемых) средств, а также ориентированы на соблюдение этических стандартов исходя из общепринятых подходов к определению термина «этика». Говоря о последнем, следует отметить, что вопрос о выработке подходов к вопросу определения этики (в частности этики в бизнесе) остается дискуссионным. Несмотря на то, что понятие этики является в преимущественной степени субъективным, в современных исследованиях разделяется мнение о том, что задача деловой этики заключается в повышении этического качества принятия решений и действий на всех уровнях бизнеса: на личном (микро-), организационном (мезо-) и системном (макро-). Столкнувшись со сложными проблемами, деловая этика должна использовать многоуровневый подход и учитывать свободы и ограничения на каждом из этих уровней, а также взаимосвязь между этими уровнями. Следовательно, КР должна осуществляться не только законно, но и этично. Однако, в практическом отношении граница, разделяющая этичные и неэтичные методы осуществления КР остается весьма нечеткой. Вместе с тем, следует учитывать различия, в понимании этики в

разных обществах, странах, регионах. То, что может восприниматься в качестве неприемлемого в одном государстве или профессиональной группе, в другом — может быть принято, как устоявшаяся норма. Сообразно возрастанию потребностей в получении ценной деловой информации возрастает роль этических норм и стандартов. В случае возникновении проблем с получением требуемой информации могут возникнуть стимулы, побуждающие к нарушению этических норм. Иногда инициативы, касающиеся нарушения этики могут прямо исходить от руководства компании. В таких случаях ответственность пропорционально ложится не только на исполнителя (сотрудника), но и на побудившего его к таким действиям руководителя.

Для выяснения вопроса о том, что можно отнести к определяющим особенностям при разграничении понятий экономической разведки и экономического шпионажа следует обратиться к существующим подходам к определению последнего. Как и в случае с определением термина «экономической разведки» промышленный шпионаж (далее ПШ) также не имеет стандартных определений. Термин по-разному определяется разными теоретиками и практиками с учетом различных факторов. Как правило именно законность и этику принято рассматривать в качестве двух определяющих факторов, отделяющими понятие экономического шпионажа от экономической разведки. Незаконный сбор разведывательной информации охватывается общим термином ПШ, в то время как юридические и этические аспекты подпадают под общий термин ЭР. В современных тематических исследованиях присутствуют такие определения как слежка одной компании за другой с целью кражи коммерческой тайны или другой конфиденциальной информации; систематическая деятельность по сбору, анализу и управлению внешней информацией, которая способствует процессу стратегического управления на предприятиях. С правовой точки зрения, пожалуй, наиболее содержательное определение дает Интерпол, характеризуя ПШ как «приобретение любым обманным путем интеллектуальной собственности, принадлежащей какому-либо юридическому лицу, которая была создана или законно приобретена этим юридическим лицом с целью произвести что-то, что имеет или может иметь промышленную ценность и, в более широком плане, ценность для национальной экономики» [14].

Одним из знаковых событий последних лет, связанных с промышленным шпионажем, стал суд над главным инженером-исследователем, обвиняемой в краже коммерческой тайны у нескольких компаний, включая Coca-Cola, начавшимся в апреле 2021 года в Восточном округе шт. Теннесси в Гринвилле. Инженер была обвинена в краже коммерческой тайны, заговоре с целью совершения кражи коммерческой тайны и мошенничестве с использованием электронных средств связи. Коммерческие тайны были оценены более чем в 119 миллионов долларов. В августе 2020 года в заменяющее обвинительное заключение были добавлены дополнительные обвинения, связанные с экономическим шпионажем [12].

Так как компании США являются одними из наиболее значительных объектов атак конкурентов из-за рубежа, в упомянутом контексте необходимо обратиться к вопросам о законодательном регулировании в сфере противодействия корпоративному шпионажу в стране. Так, на сегодняшний день в США действует Единый закон о коммерческой тайне («UTSA», 1979). В то время как большинство штатов приняли UTSA в той или иной форме, защита коммерческой тайны, предоставляемая в каждом штате, далеко не одинакова по сравнению с другими штатами. Это часто приводит к тому, что возможность взыскания за кражу коммерческой тайны становится вопросом выбора закона или толкования договора. Отмечая важность защиты интеллектуальной собственности и коммерческих секретов для экономического здоровья и безопасности страны в 1996 г. Конгресс Соединенных Штатов принял Закон об экономическом шпионаже (EEA). EEA содержит два отдельных положения, устанавливающих уголовную ответственность за кражу или незаконное присвоение коммерческой тайны. Также акт содержит положения о компенсации потерпевшим, которые позволяют правительству конфисковать любое имущество, использованное для совершения

преступления, а также доходы, полученные незаконным путем. Закон предусматривает механизмы компенсации ущерба потерпевшей стороне. Функции по возмещению ущерба потерпевшим, в тех случаях, когда это возможно, возложены на Министерство юстиции. EEA предоставляет потерпевшим приоритет при распределении конфискованного имущества. При этом с ответчика удерживаются штрафы в пользу государства, в связи с чем нетрудно представить себе случай, когда крупные штрафы могут привести к ответчика к обеднению, сделав невозможным возмещение ущерба, а потерпевший бизнес — оставить без компенсации. По той же причине штрафы могут стать причиной гражданского судебного разбирательства [15].

Как можно отметить, ЭР не ограничивается «симметричными» плоскостями (коммерция-коммерция, государство-государство), и может применяться в нескольких измерениях, переходя из коммерческой юрисдикции в административную. К субъектам в настоящее время относят: представители частного бизнеса (компании, банки), профессиональные ассоциации; глобальные или региональные организации; негосударственные организации в различном организационно-правовом статусе (среди которых НПО, институты, аналитические центры и пр.); государства. Более того, международный баланс сил меняется каждый день между «развитыми» и «развивающимися» странами, причем последним в большинстве случаев сильно помогают независимые фонды. Однако, в последнем случае речь идет лишь о легальном взаимодействии, поскольку, кроме того, незаконные и преступные группы, ассоциации, сети, а иногда и государства, помимо прочего, также ведут «жесткую игру» на международном уровне.

Принципиальным отличием КР от экономического шпионажа является то, что в первом случае сбор информации о конкурентах производится в рамках действующего законодательства и с учетом соблюдения этических норм. Это означает, что источники данных о деятельности конкурента должны находиться в открытом доступе. Исходя из данных современных исследований, связанных с КР, уровень общедоступности необходимой информации касательно позиции конкурента на рынке и его намерений способен практически в полной мере удовлетворять запросам заинтересованной стороны. Это, в свою очередь, делает применение незаконных и неэтичных методов получения информации излишним.

Не противоречащие закону методы КР могут быть направлены на получение как первичных, так и вторичных данных. Во втором случае речь идет об информации, предварительно собранной для целей, прямо не связанных с конкуренцией. Сбор информации может проводиться как наружно — без непосредственного контакта с представителями конкурентов, так и через взаимодействие с представителями компании-конкурента. К методам получения первичных данных принято относить сбор сведений от бывших сотрудников фирмы-конкурента, соискателей на должности, других конкурентов, опросы общих поставщиков и клиентов, метод «тайного покупателя», посещение профильных выставок и конференций и пр. Для получения т.н. «вторичной информации» применяю методы desk research (кабинетных исследовании) при помощи изучения данных из открытых источников. К методам desk research относятся сбор и анализ финансовых и маркетинговых отчетов, анализ рекламных активностей и открытых публикаций в СМИ, анализ учредительных и документов фирм, находящихся в открытом доступе. Наличие большого массива информации обуславливает использование искусственного интеллекта для оценки финансового и информационного потенциала анализируемых в конкурентной разведке организаций.

В рамках обсуждения вопроса о трансформации подходов к пониманию этичного поведения в условиях экономической разведки следует отметить, что в современных условиях эта трансформация в наибольшей степени обусловлена достижениями НТП и в определенном смысле повысившейся беспечностью пользователей всех технологических устройств.

Доступность и легкость пользования электронными средствами обмена информации (в частности, корпоративной) зачастую тесно связана с отсутствием у персонала компаний необходимых знаний по вопросам кибербезопасности. Необходимо отметить, что существенную угрозу для корпоративных данных нередко представляют сами сотрудники компаний, на которых приходится до половины так называемых «случайных утечек», происходящих из-за халатности или незнания внутренних инструкций. Нередко сотрудники забирают электронные носители, содержащие корпоративную информацию домой с целью поработать удаленно, сообщают коллегам пароли от рабочих аккаунтов, не уничтожают должным образом печатные документы, подлежащие уничтожению и содержащие данные разной степени важности о деятельности фирмы. Зачастую субъекты или агенты утечки (сотрудники) непреднамеренно подвергают своих работодателей риску из-за халатности, а не вследствие злонамеренного умысла. Сотрудники могут создать риск без намерения причинить вред из-за плохой деловой практики, незнания внутренней политики, слабого ее соблюдения, готовности обойти меры безопасности для более эффективного выполнения задания и просто вследствие человеческой ошибки. В современных исследованиях выделяю 4 категории инцидентов, связанных с непреднамеренными внутренними угрозами: случайное раскрытие, вредоносный код, введенный с помощью социальной инженерии, кража или ненадлежащее удаление записей и потеря портативных электронного устройства с корпоративными данными.

Следует отметить, что понятие анонимности в сети, до определенной степени, нивелировало социальные факторы, которые ранее влияли на приверженность правомерному поведению в общем, и в корпоративной сфере, в частности. В последнем случае момент, когда информация попадает в распоряжение конкурента ставит его перед моральным выбором, определяющим его последующие действия. Следует отметить, что в упомянутом отношении вопрос о трансформации подходов к пониманию этичного поведения и самому определению этичного поведения напрямую связан с технологическим аспектом. Разумеется, схожая ситуация может иметь место и в «аналоговом мире», однако современные средства передачи данных (не требующих, к примеру, физического присутствия в том или ином месте для совершения противозаконных или неэтичных действий) существенно расширяют круг возможностей. Кроме того, приверженность этичному поведению может закономерно снизиться вследствие отсутствия личного контакта между агентом/агентами воздействия и субъектом -источником сведений. Помимо этого, утечка информации в виде электронных данных усложняет процесс доказывания, так как криминалистические методы в данном отношении имеют известные ограничения, помимо прочего связанные с трудностями определения агента (субъекта) утечки данных. Кроме того, они не одинаково развиты в разных странах. Это широко согласуется с современными исследованиями, касающиеся киберпреступности и девиантного поведения в сети. Развитие информационно коммуникационных технологий, анонимность, связанная с этим девиация в сети и ограниченные возможности традиционной криминалистики имеют непосредственную связь с трансформацией взглядов на этичность распоряжения электронной информацией. Данные изменения создают новые вызовы, среди прочего, для криминологии, криминалистики, юридической психологии в расследовании киберпреступлений, связанные с отсутствием достаточного количества материальных следов преступника, широким охватом вероятных мотивов некоторых категорий киберпреступлений, проблемы, связанные с определением круга лиц, имевших возможность совершить преступление, а также значительный размер потенциального вреда, который может нанести киберпреступление, кража либо утечка данных.

Характерной чертой киберпреступлений является среда их совершения — киберпространство (или виртуальное пространство), образующееся электронным устройством и их сетями. В пределах виртуального пространства существенно меняется психологическое содержание взаимосвязей правонарушителя с предметом правонарушения (преступления), а

также правонарушителя с потерпевшим. В условиях виртуальной среды такие связи из прямых превращаются в опосредованные, следуя схеме: преступник (правонарушитель) — киберпространство — потерпевший (предмет преступления). Это, в свою очередь, ведет к устранению материальной составляющей как действий человека, так и социального взаимодействия. В описанном контексте «виртуальные» предметы с психологической точки зрения выглядят более доступными, в том числе для незаконного завладения ими. Характерным примером менее ответственного отношения к нематериальным, чем к материальным предметам является широко распространенные нарушения авторских прав, преступления в сфере интеллектуальной собственности.

Экономическая разведка тесно сопряжена с мерами контрразведки, включающих главным образом внутренние политики и зачастую имеющими жизненно важное значение для многих компаний, особенно в сфере высоких технологий [16]. Наряду с формальными политиками и мерами по противодействию утечкам действуют и негласные меры, так как формальные инструкции, ограниченные дисциплинарной ответственностью, могут не быть достаточно эффективной мерой для того, чтобы сохранить в секрете, к примеру, данные о выпуске нового продукта и пр., и уберечь компанию таким образом от многомиллионных убытков. Значение, которое многие фирмы (в особенности — hi-tech гиганты) уделяет вопросам сохранности коммерческой информации и кибербезопасности иногда приобретает беспрецедентные масштабы. По информации бывших сотрудников некоторых из таких компаний-гигантов находясь в сверхсекретных зонах, работники часто контролируются камерами наблюдения во время их работы. К примеру, в Apple по данным инсайдеров, меры предосторожности для сотрудников, работающих с наиболее чувствительными проектами, на фоне некоторых конкурентов являются беспрецедентными, включая работу в специализированных помещениях, множественные средства для сокрытия процесса работы над продуктом, включающим технологическое ноу-хау и пр.

Пример Apple в части работы с информацией, связанной с коммерческой тайной, может использоваться в качестве ориентира для других фирм. Рекомендации для малых предприятий в области противодействия внутренней киберпреступности среди прочего предполагают изменение мышления и культуры организации включая предоставление сотрудникам необходимого обучения для повышения уровня бдительности и осведомленности о возможных рисках и существующих угрозах. Отсутствие технических ресурсов может быть компенсировано определением квалифицированного внешнего специалиста, который может помочь провести оценку рисков, выявить киберугрозы для бизнеса, разработать план реагирования на инциденты и принять контрмеры для смягчения угроз высокой вероятности. Обеспечение безопасности данных станет намного сложнее, если среди уполномоченных сотрудников организации окажется хотя бы один злоумышленник.

Говоря о технической составляющей предупреждения утечки данных, следует отметить тот факт, что, как это ни очевидно, внутренние политики и инструкции, а также контроль за их исполнением, должны быть подкреплены необходимым техническим инструментарием. Случай с сотрудницей Coca-Cola наглядно демонстрирует, что средства предупреждения краж и утечек в реальном времени (например, предупреждение, которое может обнаруживать, когда внешний жесткий диск подключен к компьютеру компании), предназначенные для обнаружения внутренних угроз и предотвращения цифровой передачи данных компании, могут помочь предотвратить утечки и, в конечном итоге, использование секретов компании. Назначение специальных рабочих станций для доступа к информации, составляющей коммерческую тайну, и требование к сотрудникам, касающиеся ограничений в использовании корпоративных технических средств может быть полезным для защиты корпоративных секретов. Компаниям также следует стремиться ограничить использование личных и

неразрешенных устройств, включая смартфоны с камерами, в зонах ограниченного доступа, содержащих конфиденциальное оборудование или коммерческую тайну.

Выводы

На фоне научно-технического прогресса и усиления роли информационно коммуникационных технологий в рыночных отношениях трансформация экономики происходит практически на всех уровнях. Развитие информационно коммуникационных технологий, анонимность, связанная с этим девиация в сети и ограниченные возможности традиционной криминалистики имеют непосредственную связь с трансформацией взглядов на этичность распоряжения электронной информацией. Такие особенности современных бизнес-процессов как использование инфраструктуры виртуальных рабочих мест, удаленный доступ к репозиториям данных для сотрудников повышают риск корпоративного шпионажа. Исходя из результатов исследования есть все основания утверждать, что трансформация восприятии этичности мер ЭР также в большей степени связана с развитием информационно коммуникационных технологий. Исследование дает основание говорит о том, что восприятие мер ЭР агентом разведки (шпионажа) с точки зрения их этичности непосредственно связано с технической составляющей современных разведывательных методов. Исходя из криминально-правовой аналогии (субъект-объект преступления) психологическое содержание взаимосвязей «агент — объект разведки» в условиях использования информационно коммуникационных технологий из прямых трансформируются в опосредованные, что ведет к устранению материального компонента как действий человека, так и социального взаимодействия.

Помимо угрозы активных разведывательных мер извне, направленных на получение конкурентного преимущества, угрозу для корпоративных данных нередко представляют сами сотрудники компаний. Отсутствие у персонала компаний необходимых знаний по вопросам кибербезопасности создающих утечки корпоративных данных, или создающие предпосылки для них, также в определенной степени могут влиять на занижение «порога» этичности в принятии методов разведки конкурирующей компании и агентов ее влияния. Сотрудники могут создать риск без намерения причинить вред компании, а низкие навыки пользования информационно коммуникационных технологий могут существенно этому способствовать.

С развитием НТП меняются тактико-технические меры экономической разведки. На его фоне меняются факторы, влияющие на восприятие методов корпоративного противостояния. Предполагается, что последующие исследования должны быть посвящены вопросам изучения лучших корпоративных практик предотвращения утечек внутренних данных.

ЛИТЕРАТУРА

1. Щербакова Т.А., Архипов Э.Л. Модель обеспечения экономической безопасности компаний в рыночных условиях // Вестник Евразийской науки. — 2020 № 6. — URL: https://esj.today/PDF/76ECVN620.pdf.
2. Крохичева Г.Е., Архипов Э.Л., Лилеева Л.Р., Фуникова Е.А. Модель стратегии экономической безопасности в управлении производственным холдингом // Вестник Евразийской науки. — 2018 № 2. — URL: https://esj.today/PDF/81ECVN218.pdf.

3. Пантелеева Т.А. Систематизация кадровых рисков в контексте их влияния на экономическую безопасность хозяйствующих субъектов // Вестник Евразийской науки. — 2018 № 4. — URL: https://esj.today/PDF/60ECVN418.pdf.
4. Бегичев М.М., Потапов С.А., Власов А.В. Корпоративная разведка как инструмент конкурентной борьбы // Путеводитель предпринимателя. — 2021. — Т. 14. — № 4. — С. 136–141.
5. Трунцевский Ю.В., Есаян А.К. Конкурентная разведка как фактор предупреждения преступлений // Вестник Югорского государственного университета. — 2019. — № 1(52). — С. 23–30.
6. Аббазова А.Р., Сулейманова С.А. Промышленный шпионаж, конкурентная разведка // Академическая публицистика. — 2019. — №. 5. — С. 130–133.
7. Власов А.В., Бегичев М.М., Штепа Т.В. Конкурентная разведка в системе экономической безопасности предприятия // Ученые записки Российской академии предпринимательства. — 2020. — Т. 19. — № 3. — С. 8–18.
8. Болдырева Т.В. Конкурентная разведка как инструмент современного обеспечения экономической безопасности бизнеса // Система и механизмы обеспечения экономической безопасности государства. — 2020. — С. 4–9.
9. Коробейникова Л.С., Подлесных С.А. Роль бизнес-разведки в системе экономической безопасности организации // Апрельские научные чтения имени профессора ЛТ Гиляровской. — 2020. — С. 71–75.
10. Малеванкина А.Д. Конкурентная разведка как способ экономической безопасности компаний России // Теоретические и прикладные вопросы комплексной безопасности. — 2021. — С. 133–137.
11. Илякова И.Е., Сульдина О.В. Конкурентная разведка как инструмент минимизации экономических рисков предприятия // Ученые записки Российской академии предпринимательства. — 2019. — Т. 18. — № 3. — С. 78–88.
12. Красовских О.П., Красовских Е.О. Промышленный шпионаж как угроза экономической безопасности предприятия // Современная юриспруденция: актуальные вопросы, достижения и инновации. — 2019. — С. 90–93.
13. Башков В.В., Пономарев С.В. Промышленный шпионаж с использованием кибер-вооружения и методы борьбы с ним // Лучшая студенческая работа 2022. — 2022. — С. 113–116.
14. Одаховская Д.А., Санина Л.В., Пятак А.А. Промышленный шпионаж и защита интеллектуальной собственности в РФ // Развитие российского общества: вызовы современности. — 2021. — С. 154–166.
15. Плешакова М.В., Гонин А.А. Конкурентная разведка и промышленный шпионаж как источники информации предприятия // Экономика: теория и практика. — 2020. — № 4. — С. 65–71.
16. Миначева Э.Ф. Промышленный шпионаж как угроза экономической безопасности хозяйствующего субъекта // В мире научных открытий. — 2020. — С. 104–106.

Lebedev Igor Alexandrovich
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: ILebedev@fa.ru

Prasolov Valery Ivanovich
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: VIPrasolov@fa.ru

Ethical transformation and legal boundaries of economic intelligence

Abstract. Within the framework of this article, the authors considered the issue of economic intelligence in modern conditions. Against the backdrop of the economic confrontation between Western countries and Russia, it becomes obvious that the concept of economic intelligence is changing, manifesting itself in several planes at the same time, and corporate confrontation is moving to the level of protecting national interests. According to the authors, the factors affecting the perception of the methods of corporate confrontation are subject to change. Based on the assumption that the methods and tactics of economic intelligence are not static, the authors in this study set himself the task of determining the factors that influence their ethical perception. The study provides an opinion that the transformation of approaches to understanding ethical behavior and the very definition of ethical behavior in economic intelligence is directly related to the technological aspect, the transition of many business processes to the digital plane. The authors focus on the fact that in the conditions of cyberspace the psychological perception of illegal actions changes significantly. Commitment to ethical behavior may naturally decrease due to the lack of personal contact between the agent of influence and the source. At the same time, in practice, the boundary separating ethical and unethical methods of conducting competitive intelligence remains very unclear, which creates additional difficulties in countering such methods. In the final part of the article, the authors formulate a conclusion regarding the most common threats to which corporate data is exposed, as well as the role of economic intelligence in ensuring the security of an organization.

Keywords: competitive intelligence; corporate espionage; ethics; information leakage; electronic means of communication; economic security; ethical behavior; methods of corporate confrontation; digitalization of the economy; business processes