Экономика

УДК 346.7

П.Б. Акмаров, В.Ю. Войтович, О.П. Князева

НЕКОТОРЫЕ АСПЕКТЫ ЗАЩИТЫ ЭКОНОМИЧЕСКОЙ ИНФОРМАЦИИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Рассматриваются вопросы защиты экономической информации от неправомерного использования в условиях расширения сферы применения информационных технологий. Показаны уязвимые места в потоках и каналах циркулирующей информации с точки зрения правовой защиты коммерческих сведений. Приведен обзор правоприменительной практики в сфере получения и использования экономической информации. При этом выделены юридические аспекты решения проблемы с точки зрения российского и зарубежного законодательства. Проведен анализ информационного обеспечения законности в государственном муниципальном управлении. Рассмотрены входы и выходы и внутреннее движение управленческой информации по подсистемам органов, распределение информации между руководителями и исполнительным персоналом. Показан режим доступа к информации различных категорий государственных и муниципальных служащих и другие моменты, фиксирующие и характеризующие законность управленческих решений и действий. На основе анализа причин возникновения угроз выявлены тенденции и структура утечек информации за последние годы. Отмечено, что все должно осуществляться в правовых рамках со строгим соблюдением правового статуса управленческих публичных органов и действующих должностных инструкций. Показана динамика возникновения угроз и применения средств защиты информации от несанкционированного использования. Также проанализированы наиболее значимые направления совершенствования систем защиты информации, включая правовую, техническую и кадровую стороны решения вопроса.

Ключевые слова: коммерческая тайна, правовая защита информации, утечка, техническая защита информации, криптография, инновационное развитие, цифровая трансформация.

DOI: 10.35634/2412-9593-2020-30-4-469-478

В демократическом государстве, зафиксированном ст. 1 Конституции РФ, любая деятельность человека невозможна без получения и использования различного рода информации. При этом рыночная система требует учитывать, что сейчас информация является товаром, имеющим определенную ценность. В экономической среде наибольшую ценность представляет информация, используемая для получения определенной выгоды организации, связанной, как правило, с применением инновационных технологий. Разглашение этой информации ставит под угрозу возможности реализации поставленной цели и задач. Конечно, не каждая информация при её оглашении провоцирует появление угроз, однако наиболее ценная информация нуждается в особой защите, которую должны предоставить субъекты, владеющие ей, чтобы обезопасить себя и соответствующий орган [1].

Необходимо отметить, что защита информации становится наиболее актуальной в условиях цифровой трансформации не только производственной, но и социальной, общественной сферы. Это определяется большим объемом передаваемой информации, которая часто подвержена целенаправленным или случайным угрозам и может не только ухудшить экономические показатели отдельных организаций, но и поставить под сомнение стабильность общественного развития государства. Поэтому данная проблема должна решаться с учетом технических, программных, юридических и кадровых сторон вопросов.

В научной литературе под защитой информации понимается режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [2]. Информацией же, составляющей коммерческую тайну, считаются сведения производственного, технического, экономического, организационного и т. п. характера. Она включает результаты интеллектуальной деятельности в различных сферах жизни общества. Также сведения об алгоритмах и способах осуществления предпринимательской деятельности, имеющие реальную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к

которым у них на законном основании нет свободного доступа и в отношении которых обладателем таких сведений применяется режим коммерческой тайны [1].

Информация ограниченного пользования для коммерческой организации может представлять ценность различного вида, поэтому ее разглашение может повлечь финансовые потери за счет возникновения угроз экономической безопасности различной степени тяжести. Отсюда нам представляется, что все ее виды предварительно необходимо разделить на следующие группы:

1) информация открытого пользования в различных формах;

2) информация ограниченного доступа, предназначенная только для работников, имеющих соответствующий доступ;

3) информация только для руководителей государственных и муниципальных организаций.

Методы защиты информации не могут быть общеизвестными и общедоступными, так как открытое их использование зачастую влечет угрозы экономической безопасности не только организации, но и обществу, государству, личности. В связи с этим управленцам должно быть выгодно осуществлять меры по сохранению ее конфиденциальности и защите от несанкционированного использования.

Экономическую информацию ограниченного доступа принято называть коммерческой тайной, которая должна выражаться в установленном порядке конфиденциальности, что позволит ее обладателю при определенных условиях увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке услуг или получить иную коммерческую выгоду.

Стоит отметить, что не ко всей информации, возникающей и передаваемой в рамках организации, может быть присвоен статус коммерческой тайны. В Российской Федерации официально утвержден перечень данных, которые не могут составлять коммерческую тайну. Они общеизвестны и законодательно определены. Это учредительные документы; документы, предоставляющие право для занятия предпринимательской деятельностью; сведения по установленным формам отчетности о финансово - хозяйственной деятельности; документы о платежеспособности; документы об уплате налогов и обязательных платежей и т. п. [4]. Однако необходимо отметить, что даже эти сведения не имеют статуса открытого доступа для любого желающего. Например, данные о заработной плате работников организации, финансовая отчетность предоставляются исключительно по требованию органов власти, управления, контролирующих и правоохранительных органов, а также других юридических лиц, имеющих на это право в соответствии с законодательством России. Однако в то же время клиенты коммерческой организации вправе ознакомиться с ее уставом, свидетельством о регистрации, лицензиями, сертификатами и патентами [5].

Получение информации, не предназначенной для внешних пользователей с нарушением действующего законодательства и приводящее к прямым экономическим потерям организации, либо к упущенной выгоде, относится к незаконному способу.

Сегодня существует множество незаконных способов получения информации, которые могут привести к существенным экономическим угрозам для субъектов предпринимательства. Количество и перечень этих способов имеет тенденцию к возрастанию. Это связано в немалой степени с развитием информационных технологий, основанных на электронных способах получения, преобразования и перемещения информации. Цифровизация экономики и общественной сферы деятельности государства подняли на очень высокий уровень потребности современных технологий связи. Развитию информатизации способствует научно-техническая база, созданная за последние годы, а также технологическая основа новых технологий обработки информации. Одновременно существенно возрастают риски безопасного перемещения информации через информационные каналы. Эти риски могут иметь объективный и субъективный характер, быть случайными или преднамеренными. Но, с точки зрения бизнеса, наибольшую важность представляет защита информации от неправомерного использования с точки зрения законодательства. Это особенно актуально в современных условиях, когда информация становится не только источником для решения вопросов управления, но и средством производства. Определенный опечаток на процессы обработки информации накладывают также глобализация и демократизация общества, увеличивая возможности несанкционированного применения информации.

Так, по данным аналитического центра InfoWatch, в 2018 г. основную долю утечек конфиденциальной информации составляли компьютерные сети, в первую очередь Интернет. Также значительный объем утечек приходится на такие каналы, как кражи и потери оборудования, электронная почта [6]. Распределение утечек конфиденциальной информации по каналам за 2017–2018 гг. представлено на рис. 1.

Рис. 1. Распределение утечек информации по источникам

Для получения интересующей их информации конкуренты сегодня прибегают, как правило, к открытым источникам, таким как компьютерные сети, в первую очередь Интернет, газеты, специальные журналы, информация с выставок и т.д. Из этих источников можно получить до 90 % необходимых сведений. Для этого многие фирмы даже создают специальные аналитические подразделения, целью которых является изучение открытой информации для извлечения и формирования нужных сведений.

Исследование данных InfoWatch в первом полугодии 2018 г. аналитическим центром InfoWatch была отмечена регистрация 840 случаев утечки коммерческой тайны. Эта цифра на 16 % больше, чем за аналогичный период предыдущего 2017 г. В 2016 г. процентное увеличение количества утечек коммерческой тайны составляло 10 % (рис. 2). Это при том, что 99 % случаев утечки коммерческой тайны остаются за «кадром», однако собранная информация позволяет судить о конкретных фактах в данной области и делать соответствующие выводы.

Для предпринимателя ценность информации определяется ее значимостью, которая определяется, по мнению специалистов, полезностью, своевременностью, достоверностью и полнотой. Понятие «Коммерческая тайна» появилось в российском законодательстве с принятием в 1991 г. закона «О предприятиях и предпринимательской деятельности». В законе коммерческая тайна предприятия была определена как не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью организации, разглашение (передача, утечка) которых может нанести ущерб ее интересам.

Анализируя защиту экономической информации в зарубежных странах, необходимо отметить, что она основывается на разных принципах. Так, в США сохранение и защита экономической информации отданы на откуп законодательной власти штатов. Однако местные законы штатов опираются на единый рамочный законодательный акт. В соответствии с данным актом коммерческая тайна определяется как информация или технология, которая обладает самостоятельной экономической ценностью (действительной или потенциальной) и недоступна для других лиц, которые могли бы извлечь экономическую выгоду из ее использования или разглашения.

В Великобритании система регулирования в сфере защиты экономической информации основывается на договорах между работодателем и наемными работниками, либо между контрагентами. При этом существует отдельная категория лиц, чьи профессии могут быть связаны с получением коммерческих тайн: полицейские, медицинские работники, налоговые инспекторы и так далее. Они должны подписывать договор о неразглашении конфиденциальной информации и придерживаться его в повседневной службе. Такая же схема регулирования защиты коммерческой тайны используется в странах, которые ранее были колониями Великобритании.

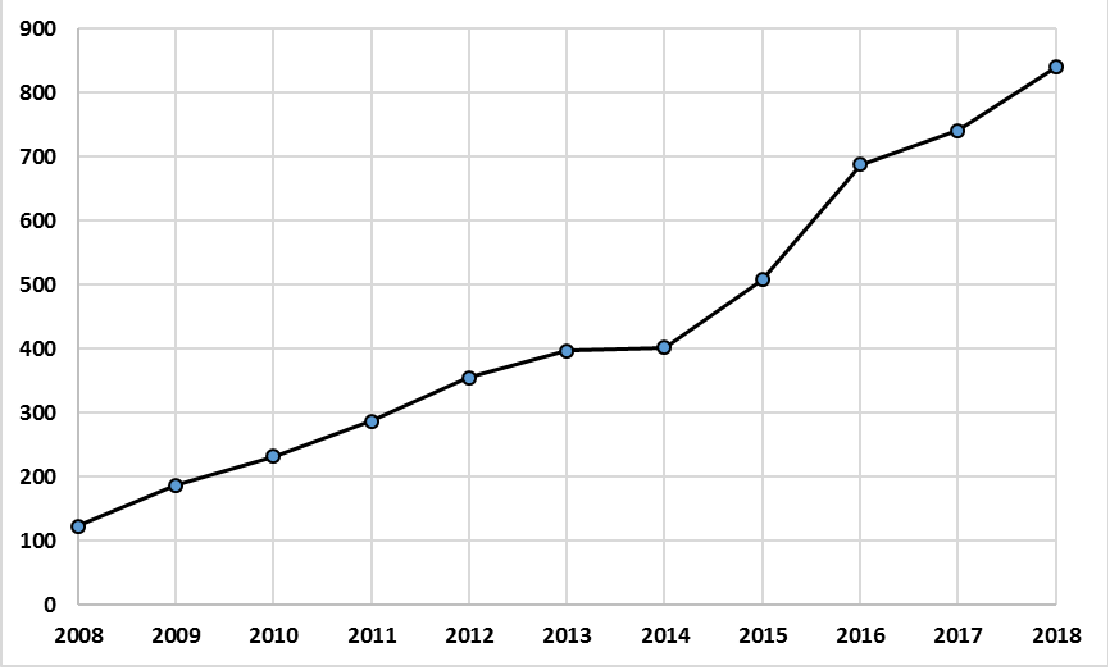

Рис. 2. Рост утечек коммерческой тайны в России за 2008–2018 гг.

В Германии применительно к защите коммерческой тайны используется термин «ноу-хау», значение которого отличается от общеизвестного технического. Если в технической сфере «ноу-хау» обозначает какие-либо расчеты, формулы, чертежи или модели, неизвестные до настоящего момента, то в коммерческой это списки поставщиков и клиентов, картотека связанных между собой организаций, а также сведения о методах и средствах работы с товаром [7].

По немецкому законодательству тайной считается любая информация, отвечающая принципам секретности, при условии, что обладатель этой информации заинтересован в ее сохранении и защите от передачи третьим лицам.

Подобная система защиты экономической информации применяется и в Австрийском законодательстве. Но там нет специального акта, регулирующего защиту коммерческой тайны, к тому же в Австрии вместо коммерческой тайны применяется термин «закрытая информация». Таким образом, защита информации регулируется отдельными нормами права, представленными, к примеру, в Австрийском торговом кодексе от 1938 г. и ряде других актов.

Итальянское право регулирует защиту коммерческой тайны посредством контролирования взаимоотношений «работодатель-работник», чаще всего пункты о неразглашении включаются в трудовой договор. Закон в свою очередь запрещает работникам передавать тайную информацию третьим лицам, а также предавать ее огласке, публиковать или конкурировать с работодателем, особенностью которого является то, что сроки неразглашения тайны и соблюдения «обещания верности» никак не устанавливаются, а значит работник не имеет права разглашать коммерческую тайну, даже если перестает работать в организации [8].

В Китае, так же как и в Австрии, нет специальных нормативно-правовых актов, посвященных урегулированию вопросов юридической защиты коммерческой информации. Вместо этого есть, например, положение о коммерческих службах безопасности, в которой рассмотрены некоторые вопросы защиты коммерческой тайны. В частности, любые документы, оформленные на бумаге или ином материальном носителе, автоматически получают юридическую защиту. Китайское законодательство запрещает разглашение и передачу данных, полученных незаконным путем, либо нарушающих договоренности о неразглашении и могущих принести ущерб организации [9].

Законодательство ряда европейских государств, таких как Франция, Швейцария, Финляндия предусматривает использование в сфере защиты информации норм общего права. Их анализ позволяет определить следующие направления в сфере защиты коммерческой тайны:

- ответственность за сохранение конфиденциальности информации «работник-работодатель» возлагается на работника;

– по прекращению совместной деятельности работник не вправе конкурировать с работодателем;

– за передачу работником конфиденциальных данных третьим лицам предусмотрена гражданско-правовая ответственность;

– за разглашение конфиденциальной информации предусмотрена уголовно-правовая ответственность для государственных служащих и должностных лиц контролирующих органов.

В Японии нет отдельных законов и положений, которые описывают сохранение и защиту коммерческой тайны. На каждом отдельном предприятии защита информации регулируется специальным нормативным актом. При этом в крупных компаниях существует «департамент кадров», в чьи обязанности входит регулирование конфликтов разглашения коммерческой тайны. Местные нормативные акты регулируют не только юридическую сторону отношения работника и работодателя, но также и морально-этические аспекты поведения служащих на работе в данной компании. Они включают в себя ряд принципов, которых должен придерживаться сотрудник компании, а именно: запрет на разглашение конфиденциальных сведений, составляющих коммерческую тайну; запрет на работу по совместительству, либо конкуренцию с руководителем.

В Японии конфликты с разглашением коммерческой тайны происходят гораздо реже, чем в других странах, что объясняется традиционной системой пожизненного найма сотрудников, а также преданностью работников своей компании [7]. Однако современное законодательство разрешает переход работникам в другие компании с сохранением карьерного роста, в связи с этим встанет необходимость защиты информации, дабы не принести экономический ущерб организации.

В Тайланде принят специальный закон о коммерческой тайне, регулирующий все вопросы, связанные с защитой экономической информации. В законе описывается не только ответственность за разглашение и передачу третьим лицам защищенной информации, но и порядок судебной защиты, применимый к коммерческой тайне и порядок установления размера возмещения убытков.

Приведенные данные выше проанализированных стран дают основание сделать вывод о том, что коммерческой тайной можно считать любые формы и виды научной, финансовой, технической и другой информации, в том числе формулы, модели, чертежи, рисунки, записи. При условии, что законный владелец этой информации уже предпринял меры по ее сохранению и защите, тем самым ограничив доступ к ней других людей и придав ей экономическую ценность.

Следующим принципом, по которому информацию можно считать коммерческой тайной, является ее неочевидное для конкурентов содержание. Таким образом, общеизвестная информация не может быть официально признана коммерческой тайной. Однако, если какая-либо переданная общественности информация может раскрывать суть коммерческой тайны только с помощью специально проведенных исследований, она тем не менее будет считаться незаконной и в данном случае подлежит юридической защите.

Владелец тайны должен самостоятельно оценить, насколько значима эта информация и какой будет ущерб от ее утраты. Это необходимо для того, чтобы определить степень усиления мер защиты, которые могут приниматься в отношении коммерческой тайны. При этом в случае судебного разбирательства будут учтены все предпринятые меры защиты, а также используемые технические средства и способы защиты. Кроме того, важную роль будет играть сама политика конфиденциальности обладателя коммерческой тайны.

В настоящее время в российском законодательстве вопросы, связанные с коммерческой тайной предприятий, отражены в Гражданском кодексе Российской Федерации, в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [10]. Информация официально считается охраняемой, если руководитель той или иной организации подписывает приказ, в котором излагаются причины необходимости ее защиты.

Наиболее частыми вопросами защиты коммерческой тайны становятся конфликты интересов предприятий и государства в лице контрольных органов. В связи с этим наибольшее внимание при составлении нормативных актов должно уделяться урегулированию вышеописанных отношений. Тем не менее, учитывая современные тенденции, мы полагаем, что важнейшими вопросами в этой сфере станут вопросы урегулирования отношений «работник-работодатель» и конкурирующих предприятий [11]. В законодательстве России коммерческой тайной считается какой-либо факт о работе конкретного предприятия, который по своей сути известен только ограниченному кругу лиц и в отношении которого документально подтверждена воля владельца информации по ее сохранению и защите.

При этом вид информации, подлежащей защите, может быть, как техническим, так и коммерческим. Защита экономической информации рассматривается только в неразрывной связи с предприятием и вне организации существовать не может, чем отличается от принятого в некоторых странах понятия «ноу-хау».

Законодательно защита коммерческой тайны обеспечивается только от неправомерного действия третьих лиц, однако в случае получения данными лицами закрытой информации самостоятельно и на правомерной основе, например, с помощью полученных знаний и проведенных исследований, эта тайна не будет подлежать юридической защите. В связи с этим, защита обеспечивает не конкретное авторство и сохранение определенных сведений, а нормативное функционирование владельца коммерческой тайны. Подтверждением тому является возможность одновременного существования одной и той же информации, составляющей коммерческую тайну в различных сферах или даже в конкурирующих предприятиях.

Защищаемая экономическая информация представляет собой преимущество одной компании перед другой в экономическом смысле. Обладатель коммерческой тайны способен сам выбирать, будет ли он использовать конфиденциальные сведения как преимущество перед конкурирующими предприятиями, либо запатентует, обозначив свои юридические права на эти данные, потеряв при этом возможность обладания уникальными сведениями. Сохранение информации в качестве коммерческой тайны применяется также при невозможности патентовать особенные сведения, либо под влиянием каких-либо других технических причин [12].

Развитие информационных технологий в современном мире и, особенно, интернет-технологий, ставит перед пользователями информации новые проблемы, а именно: нуждается в особой системе регулирования информации, циркулирующей в социальных сетях, размещенная на сайтах, передаваемая по компьютерным сетям с помощью других сервисов интернета. Основы для такого регулирования заложены в федеральном законодательстве России, в частности в законе «Об информации, информационных технологиях и о защите информации». В нем зафиксировано, что доступ к информации может быть ограничен в целях защиты основ Конституции, нравственности, здоровья, прав и законных интересов граждан, а также обеспечения обороны страны и безопасности государства [13]. Однако необходимо отметить, что этот закон никак не защищает интересы организаций – юридических лиц, видимо законодатель полагал, что эти вопросы должны рассматриваться отдельными законодательными актами.

В реальной действительности условия доступа к некоторым видам защищаемой информации устанавливаются различными федеральными законами. Так, ими регулируется отнесение информации к сведениям, составляющим коммерческую тайну, служебную и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение. В то же время необходимо учитывать, что порядок разделения информации по степени доступности, способы регулирования информационных потоков, а также меры предупреждения несанкционированного использования информации устанавливаются федеральным органом – Роскомнадзором. Однако учитывая, что объемы преступлений в информационной сфере растут в геометрической прогрессии, мы считаем, что некоторые вопросы защиты информации, включая вопросы защиты от умышленного искажения или хищения, должны отражаться в федеральных законах.

В современных отношениях значительная доля умышленных противоправных действий с применением цифровых технологий происходит из-за утечки персональных данных граждан, которые можно получить разными способами. Это и недобросовестность работников, обязанных соблюдать меры защиты информации и неосторожность самих граждан, допускающих раскрытие персональных сведений. В то же время большой объем незаконного оборота информации возникает из-за несовершенства технической и технологической защиты баз данных и систем управления этими базами. В табл. 1 приведена динамика неправомерного пользования информацией, которая создает угрозы информационной безопасности страны и ее граждан.

Наибольшую долю здесь представляют спам-рассылки по компьютерным сетям и по каналам сотовой связи, причем эту динамику не удается сократить даже за счет применения специальных фильтров. Наибольшую угрозу представляют факты незаконного доступа к информации, включая персональные данные. И, хотя их доля сравнительно невелика, но ущерб от таких преступлений огромный.

Таблица 1

Динамика возникновения угроз информационной безопасности
(% от всех наблюдений)

Вид угрозы	Годы				
	2015	2016	2017	2018	2019
Несанкционированное распространение информации	19,1	18,4	18,5	19,6	19,7
Рассылка вредоносных программ (вирусов)	17,1	13,3	11,4	8,9	8,5
Несанкционированный доступ к информационным ресурсам	1,9	1,4	1,8	1,4	1,6

Поэтому необходимо уделять повышенное внимание криптографическим методам защиты, алгоритмы которых практически не подвластны умышленному воздействию человека с целью завладения закрытыми сведениями. В этой сфере правовое регулирование должно быть направлено не только на наказание за совершенные факты умышленного завладения или порчи информации, но, прежде всего, на предупреждение неправомерных действий со стороны юридических и физических лиц.

В последнее время значительно расширился арсенал программно-технических средств защиты информации. Помимо антивирусных программ, которые сегодня использует практически каждый пользователь, организации и граждане начинают устанавливать спам-фильтры, средства шифрования. Наиболее «продвинутые» пользователи применяют биометрические средства аутентификации личности (табл. 2).

Безусловно, все современные средства и методы защиты не могут в полной мере исключить влияние человеческого фактора на информационную безопасность. Это особо касается простых работников, не обремененных, как правило, дополнительными обязательствами по защите информации.

Таблица 2

Использование средств защиты информации в организациях, %

Вид защиты	2015 год	2019 год
Антивирусные программы	85	89
Средства цифровой подписи	82	85
Логины, пароли	64	66
Спам-фильтры	52	59
Средства шифрования	46	51
Средства обнаружения постороннего вмешательства	31	36
Биометрические средства аутентификации	2	6

Интересам сторон наиболее полно отвечает самостоятельное определение характера последоговорных отношений, поэтому законодательное регулирование подобных отношений не имеет особого практического смысла, достаточно того, что закон допускает их оформление и применение.

На перспективы мы предлагаем компромиссный вариант, когда работник сам сознательно ограничивает свой профессиональный рост, а владелец тайны несет дополнительные расходы, которые, однако, значительно меньше тех, которые бы возникли у него в случае нарушения тайны. В современных условиях для России возможность такого рода соглашений может явиться наиболее действенным способом зашиты коммерческой тайны после завершения трудовых отношений с работником.

Сегодня имеется множество различных способов, с помощью которых конкурент может получить сведения, составляющие коммерческую тайну, либо попытаться это сделать. Эти действия могут быть предприняты как самим конкурентом, так и при помощи третьих лиц. Примерами таких действий являются: проникновение на предприятие конкурента; маскировка под клиента данного предприятия и другие действия, которые могут быть отнесены к промышленному шпионажу как проявлению недобросовестной конкуренции. Наиболее часто используемым и простым способом завладения коммерческой тайной конкурента является привлечение действующих или бывших работников. Недобросовестными действиями в таком случае признаются: дача взятки, подстрекательство работника к разглашению тайны, склонение к нарушению условий договора, шантаж работника, вплоть до физического насилия.

В то же время информация может быть получена заинтересованными лицами и с применением законных способов, включая аналитические способности и опыт этих лиц. В этом случае необходимо разграничить информацию, полученную законным способом от незаконно полученной информации. Это задача достаточно сложная, поэтому в российском законе на этот случай сделана оговорка: неправомерными являются любые способы получения сведений, составляющие коммерческую тайну, без официального согласия владельца информации.

С другой стороны, защитные меры не должны препятствовать развитию бизнеса, поэтому, на наш взгляд, правовое регулирование не является абсолютной защитой владельца информации против любых ее нарушений. Данную защиту закон может предоставить ему лишь только в отношении неправомерных нарушений при использовании коммерческой тайны. В связи с этим защита коммерческой тайны выступает как одна из гарантий свободы осуществления предпринимательской деятельности и невмешательства в нее извне.

Вопросы защиты информации играют очень важную роль не только в коммерческой деятельности организаций, но и в плане реализации государственной политики обеспечения доступности государственных услуг. В соответствии со стратегией информатизации российского общества доля таких услуг, оказываемых с помощью современных информационно-коммуникационных технологий, должна расти.

Необходимо отметить, что законодательное обеспечение указанной стратегии в плане сохранности информации осуществляется по нескольким направлениям в зависимости от уровня циркулирования информации. Во-первых, это защита от неправомерного разглашения или использования коммерческой тайны или части подобных сведений государственными органами и должностными лицами, имеющими доступ к таким сведениям, полагаясь на прямое указание законодательства. Во-вторых, это защита от нарушения обязательств по сохранению конфиденциальности информации работниками, владеющими информацией, составляющей коммерческую тайну. В-третьих, защита от неправомерных деяний посторонних лиц, нарушивших режим сохранности коммерческой тайны [14].

Однако и сегодня одним из основных препятствий для расширенного использования информационных технологий является неуверенность населения и коммерческих структур в защищенности каналов связи, в первую очередь сети Интернет. Приведем результаты исследований, проведенных высшей школой экономики, которые выявили основные причины отказа от применения информационных технологий при получении государственных услуг (табл. 3) [15].

Как видим, доля людей, опасающихся утечки информации, в последние годы возрастает. С этим связана и другая проблема, которая вызывает необходимость представления дополнительных документов при передаче цифровой информации. А для этого снова необходимо обращаться с личным визитом. Из таблицы видно, что остальные причины имеют тенденцию к снижению. Эта же тенденция складывается и в отношении оборота коммерческой информации.

Таблица 3

Причины отказа от применения информационных технологий при получении государственных услуг, % от опрошенных

Причина отказа	Год	
	2017	2018
Предпочитают личный визит	52,1	51,1
Вынуждены обращаться к помощи других лиц	18,2	17,2
Недостаточно навыков работы	12,3	13,2
Необходимость представления дополнительных документов	12,3	12,7
Есть опасения по поводу защиты информации	2,4	3,3
Услуга недоступна в электронном виде	2	1,9
Проблемы с цифровой подписью	0,7	0,6

Полученные результаты еще раз дают основание сделать вывод о том, что необходимо усилить не только программно-техническую защиту информации в сетях, но и пересмотреть правовое регулирование этой сферы деятельности нашего общества.

Сегодня в зарубежных странах сложилась тенденция законодательного регулирования, в соответствии с которой защита информации возложена на отраслевое право, а именно гражданское, администт-

ративное и даже уголовное право. В современной российской действительности такого рода защита осуществляется лишь в рамках законов, регулирующих конкуренцию и ограничение монопольной деятельности. В связи с быстрым развитием цифровой экономики и усилением роли информационных технологий российское законодательство нуждается в более четкой и эффективной системе защиты экономической информации. Создание такой системы целесообразно провести в ходе работы над совершенствованием законодательства. Одновременно с этим следует продолжать работы по повышению качества программно-технических средств защиты, включая криптографические методы.

В любом случае, даже самое совершенное законодательство и современные технологии защиты не могут гарантировать достаточный уровень безопасной работы с информацией без учета человеческого фактора. Граждане страны должны не только обладать широкими знаниями в сфере информационных технологий, но и осознавать социальную ответственность за свои действия. Это задача достаточно сложная и требует системной работы на всех уровнях управления и воспитания человека, начиная с детского возраста.

СПИСОК ЛИТЕРАТУРЫ

1. Валюженич Н. Коммерческая тайна: предпринимательство и лояльность персонала. М.: КноРус, 2018. 779 с.
2. Езангина И.А. Проблемы и тенденции развития инфраструктуры кредитных рынков в России // Экономическая безопасность России и стратегии развития ее регионов в современных условиях. М., 2017. С. 67-70.
3. Хачатурян Г.Ю. Институциональные основы экономической безопасности банковской деятельности в современной экономике // Вестн. ун-та (государственный университет управления). 2015. № 21. С. 15-22.
4. Сазонов С.П., Езангина И.А., Евсеев Р.С. Экономическая безопасность кредитной организации: факторы, угрозы, направления укрепления // Финансовая аналитика: проблемы и решения. 2016. № 31 (313). С. 42-56.
5. Экономическая безопасность предприятия. Объективные причины появления коммерческой тайны. URL: http://www.dvgu.ru/doc.
6. Методика RiskWatch. URL: http: //www.intuit.ru/studies/courses/531/387/lecture/8996.
7. Graham Stuart J.H., Robert P. Merges, Pam Samuelson, Ted Sichelman. High Technology Entrepreneurs and the Patent System: Results of the 2008 Berkeley Patent Survey // Berkeley Tech. L.J. 2009. № 4. С. 1255-1328.
8. Дашков Л.П., Брызгалин А.В. Коммерческий договор от заключения до исполнения. М.: Маркетинг, 2016. 324 с.
9. Bombard, Gregory S. Three Key Distinctions between the Uniform Trade Secrets Act and the Common Law // Commercial & Business Litigation. 2016. № 2. С. 23-27.
10. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: http://base.garant.ru/12148555/.
11. Валюженич Н. Коммерческая тайна: способы доступа и защиты. М.: КноРус, 2016. 484 с.
12. Клебанов Л.Р. Незаконное получение сведений, составляющих коммерческую, налоговую или банковскую тайну: особенности квалификации // Вестн. Омского ун-та. Серия: Право. 2014. №2 (39). С. 137-140.
13. Акмаров П.Б., Войтович В.Ю., Третьякова Е.С. Повышение эффективности государственного управления в условиях развития информационного общества // Наука Удмуртии. 2019. № 1 (87). С. 11-18.
14. Войтович В.Ю. Проблемы государственного и муниципального управления в условиях построения демократического правового государства // Государственное и муниципальное управление: теория, история, практика: сб.ст. науч.-практ. конф. Ижевск: УдГУ, 2015. С. 6-11.
15. Индикаторы цифровой экономики: 2019. Статистический сборник. М.: НИУ ВШЭ, 2019. 248 с.

Поступила в редакцию 10.07.2020

Акмаров Петр Борисович, кандидат экономических наук, профессор,
заведующий кафедрой экономической кибернетики и информационных технологий
ФГБОУ ВО «Ижевская ГСХА»
426069, Россия, г. Ижевск, ул. Студенческая, 11
E-mail: izgsha_ur@mail.ru

Войтович Валерий Юрьевич, доктор юридических наук, профессор
ФГБОУ ВО «Удмуртский государственный университет»
426034, Россия, г. Ижевск, ул. Университетская, 1
E-mail: gimu4282@inem.uni.udm.ru

Князева Ольга Петровна, кандидат экономических наук, доцент
ФГБОУ ВО «Ижевская ГСХА»
426069, Россия, г. Ижевск, ул. Студенческая, 11
E-mail: izgsha_ur@mail.ru

P.B. Akmarov, V.Yu. Voitovich, O.P. Knyazeva

SOME ASPECTS OF PROTECTION OF ECONOMIC INFORMATION IN MODERN CONDITIONS

DOI: 10.35634/2412-9593-2020-30-4-469-478

Issues of protection of economic information from a misuse in the conditions of expansion of scope of application of information technology are considered. It is necessary to understand more deeply streams and channels of the circulating information to give to all Russian society necessary controllability on a legal basis. The review of legal experience in the sphere of receiving and using economic information is given. Legal aspects of solving the problem in terms of Russian and foreign legislation are allocated. The analysis of information support of legality in the state municipal management is carried out. Entries and exits and internal movement of the administrative information on subsystems of bodies, information distribution between heads and executive personnel are considered. The regime of access to the information of different categories of state and municipal employees and other aspects that fix and characterize the legality of managerial decisions and actions are shown. Trends and structure of information leaks in recent years have been revealed on the basis of analysis of reasons for threats. It is noted that everything should be carried out within the legal framework with strict observance of the legal status of administrative public bodies and existing job descriptions. Dynamics of occurrence of threats and application of protection frames of the information against unauthorized use is shown. Also the most significant directions of perfection of the systems of information protection, including legal, technical and personnel parties of resolution of the issue are analyzed.

Keywords: trade secret, information legal protection, information, information leakage, technical protection of information, cryptography, innovative development, digital transformation.

Received 10.07.2020

Akmarov P.B., Candidate of Economics, Professor, Head of Department
Izhevsk State Agriculture Academy
Studencheskaya st., 11, Izhevsk, Russia, 426069
E-mail: izgsha_ur@mail.ru

Voitovich V.Yu., Doctor of Law, Professor
Udmurt State University
Universitetskaya st., 1, Izhevsk, Russia, 426034
E-mail: gimu4282@inem.uni.udm.ru

Knyazeva O.P., Candidate of Economics, Senior lecturer
Izhevsk State Agriculture Academy
Studencheskaya st., 11, Izhevsk, Russia, 426069
E-mail: izgsha_ur@mail.ru