DOI 10.12737/2073-0462-2020-133-138
УДК 346.7

ПРОБЛЕМЫ ЗАЩИТЫ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Акмаров П.Б., Газетдинов М.Х., Третьякова Е.С.

Реферат. В условиях глобальной информатизации общества многократно возрастают угрозы неправомерного распространения информации, включая умышленное незаконное получение коммерческих сведений. Изучение поставленной проблемы проводили с использованием статистического инструментария, методов анализа и прогнозирования. Объемы несанкционированного применения информации в последние годы возрастают. За период с 2008 г. по 2018 г. число случаев утечки сведений, представляющих коммерческую тайну увеличилось в 8 раз, в основном этот рост обусловлен использованием информационных технологий, прежде всего, компьютерных сетей. Такое положение наносит существенный ущерб экономике страны и отдельных организаций, а также повышает риски незаконного изъятия и искажения информации в системах электронного документооборота и при использовании электронных платежных систем гражданами. Наибольшую опасность представляют несанкционированное распространение информации и незаконный доступ к информационным ресурсам. Применение программных и технических способов защиты компьютеров снижает экономические последствия от распространения вредоносных программ. Однако население все еще настороженно относится к преимуществам, которые дает информатизация. Большинство людей предпочитают личное общение при решении возникающих вопросов как в сфере государственных услуг, так и в коммерческой деятельности. Недоверие к информационным технологиям обусловлено разными причинами, включая несовершенство компьютерных программ и технических средств связи, а также недостатками в сфере правовой защиты информации. Необходимо усиление не только программно-технической защиты информации в сетях, но и пересмотр правового регулирования этой сферы деятельности. В связи с быстрым развитием цифровой экономики возникает объективная необходимость совершенствования российского законодательства с точки зрения повышения эффективности системы защиты экономической информации. Одновременно следует продолжить работу по повышению качества программно-технических средств защиты, включая криптографические методы.

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

Введение. На современном этапе развития экономики страны происходит становление качественно новой стратегии производства, базирующейся на различных цифровых технологиях. В этих условиях многократно возрастают риски неправомерного использования данных персонального характера или сведений, составляющих коммерческую тайну. При этом рыночная система требует учитывать тот факт, что информация сейчас – это товар, имеющий определенную стоимость. Соответственно, по мнению специалистов, этот процесс сталкивается с необходимостью решения различных правовых вопросов [1]. В экономической среде наибольшую ценность представляет информация, используемая для получения определенной выгоды, связанной, как правило, с применением инновационных технологий. Разглашение таких сведений ставит под угрозу возможности реализации поставленных целей и задач, наиболее ценная часть информации нуждается в особой защите, которую должны предоставить субъекты, владеющие этой информацией, чтобы обезопасить себя и соответствующий орган [2].

Цель исследования – анализ существующих методов и способов защиты информации, снижающих риски неправомерного ее использования для получения преимущества над конкурентами, выбор средств повышения эффективности системы защиты экономической информации.

Условия, материалы и методы исследований. Проблема защиты информации становится наиболее актуальной в условиях цифровой трансформации производственной, социальной и общественной сферы. Это определяется большими объемами передаваемых данных, которые часто подвержены целенаправленным или случайным угрозам, что может не только ухудшить экономические показатели отдельных организаций, но и поставить под сомнение стабильность общественного развития государства. Поэтому рассматриваемая проблема должна решаться по определенной методике с учетом технических, программных, юридических и кадровых аспектов, регламентирующих технологию и организацию цифровизации [3].

Материалы исследований были получены из статистических источников, публикаций отечественных и зарубежных авторов, докладов профильных министерств и ведомств. При их обработке использовали статистические и графические методы, методы сравнений и прогнозирования.

Анализ и обсуждение результатов исследований. С научной точки зрения защита информации предполагает конфиденциальность той ее части, которая в определенных обстоятельствах предоставляет обладателю возможности увеличения доходов, сохранения положения на рынке или получения иной коммерческой выгоды [4]. Представляющая коммерческую тайну информация может носить производственный, технический, экономический и другой характер. Чаще всего это результаты интеллектуальной деятельности в самых разных областях. Даже алгоритмы и способы ведения пред-

принимательства могут иметь определенную ценность, поскольку неизвестны третьим лицам и стало быть могут составлять коммерческую тайну [5].

Информация ограниченного пользования для коммерческой организации может представлять ценность различного вида, поэтому ее разглашение может повлечь финансовые потери из -за возникновения угроз экономической безопасности различной степени тяжести. Исходя из этого целесообразно предварительно разделить все ее виды на следующие группы:

1) открытого пользования в различных формах;

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

3) только для руководителей государственных и муниципальных организаций.

Методы защиты информации не могут быть общеизвестными и общедоступными, так как открытое их использование зачастую влечет угрозу экономической безопасности не только организации, но и обществу, государству, личности, именно поэтому руководители непосредственно заинтересованы в осуществлении мер по сохранению ее конфиденциальности и защите от несанкционированного использования.

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

Стоит отметить, что не любой информации, возникающей и передаваемой в рамках организации, может быть присвоен статус коммерческой тайны. В Российской Федерации официально утвержден перечень данных, которые не могут относится к этой категории. К ним относятся учредительные документы, документы о праве на ведение предпринимательства, формы хозяйственной отчетности, документы о платежеспособности, документы об уплате налогов и обязательных платежей и др. [6].

Однако необходимо отметить, что даже эти сведения не полностью открыты для любого желающего. Например, данные о заработной плате работников организации, финансовая отчетность предоставляются исключительно в соответствии с требованиями контролирующих органов, которые обладают таким правом по законодательству Российской Федерации. В то же время устав коммерческой организации, свидетельство о регистрации, лицензии и патенты открыты для клиентов [7].

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

Сегодня существует множество незаконных способов получения информации, которая может привести к существенным экономическим угрозам для субъектов предпринимательства. Причем их количество постоянно растет. Это в немалой степени связано с развитием информационных технологий, основанных на электронных способах получения, преобразования и перемещения информации. Цифровизация экономики и общественной сферы деятельности государства подняли потребности современных технологий связи на очень высокий уровень. Развитию информатизации способствует научно-техническая база, созданная за последние годы, а также технологическая основа новых способов обработки информации [8].

Одновременно возрастают риски для безопасного перемещения информации через информационные каналы. Они могут иметь объективный и субъективный характер, быть случайными или преднамеренными. Но, с точки зрения бизнеса, наибольшую важность представляет защита информации от неправомерного использования с целью получения преимущества над конкурентами. Это особенно актуально в современных условиях, когда информация становится не только источником для решения вопросов управления, но и средством производства. Определенный отпечаток на процессы обработки информации, увеличивая возможности ее несанкционированного использования, накладывают также глобализация и демократизация общества.

В российском законодательстве вопросы, связанные с коммерческой тайной предприятий, отражены в Гражданском кодексе Российской Федерации и Федеральном законе от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [9]. Информация официально считается охраняемой, если руководитель той или иной организации подписывает приказ, в котором излагаются причины необходимости ее защиты.

Наиболее часто вопросы защиты коммерческой тайны возникают в результате конфликтов интересов организаций и государства. В связи с этим наибольшее внимание при составлении нормативных актов уделяется урегулированию таких отношений. Тем не менее, в соответствии с современными тенденциями можно предположить, что важнейшими вопросами в этой сфере станут вопросы урегулирования отношений «работник-работодатель» и конкурирующих предприятий [10]. 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 этими лицами закрытой информации самостоятельно и на правомерной основе, например, в результате проведенных исследований, она не

будет подлежать юридической защите. В связи с этим защита обеспечивает не конкретное авторство и сохранение определенных сведений, а норму сохранения коммерческой тайны. Подтверждением тому служит 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 конкурентами, либо запатентует, обозначив свои юридические права, но потеряв при этом возможность обладания уникальными сведениями. Сохранение информации в качестве коммерческой тайны используют также при невозможности запатентовать особенные сведения, либо под влиянием каких-либо других технических причин [11].

Развитие информационных, особенно, интернет-технологий в современном мире ставит перед пользователями информации новые задачи. А именно, возникает потребность в особой системе регулирования информации, циркулирующей в социальных сетях, размещенной на сайтах, передаваемой по компьютерным сетям с помощью других сервисов интернета [12]. 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.

При этом условия доступа к некоторым видам защищаемой информации устанавливают различные федеральные законы. В них определен статус тех или иных сведений (коммерческая тайна, служебная и др.), режим соблюдения её конфиденциальности и ответственность за сохранность. Порядок разделения информации по степени доступности, способы регулирования информационных потоков, а также меры предупреждения несанкционированного использования информации устанавливает федеральный орган – Роскомнадзор. Однако, на наш взгляд, с учетом постоянного роста преступлений в информационной сфере целесообразно некоторые вопросы защиты информации, в том числе от умышленного искажения или хищения, должны быть отражены в специальных федеральных законах.

В современных условиях значительная часть умышленных противоправных действий с использованием цифровых технологий происходит из-за утечки персональных данных граждан, которые происходят по разным причинам. Среди них могут быть, как недобросовестность работников, обязанных соблюдать меры защиты информации, так и неосторожность самих граждан, допускающих раскрытие персональных сведений. В то же время большой объем незаконного оборота информации связан с несовершенством технической и технологической защиты баз данных и систем управления такими базами. В результате обработки материалов социологических исследований научно-исследовательского института Высшей школы экономики [14] и собственных выборочных обследований удалось выделить основные угрозы информационной безопасности для организаций России.

Среди угроз информационной безопасности страны и ее граждан наибольшая доля приходится на спам-рассылки по компьютерным сетям и по каналам сотовой связи (табл. 1). Самую высокую угрозу представляет несанкционированный доступ к информации, включая персональные данные. И, хотя ее доля сравнительно невелика, ущерб от таких преступлений огромен. Поэтому необходимо уделять повышенное внимание криптографическим методам защиты, обойти алгоритмы которых с целью завладения закрытыми сведениями практически не возможно. В этой сфере правовое регулирование должно быть направлено не только на наказание за совершенные факты умышленного завладения или порчи информации, но и, прежде всего, на предупреждение неправомерных действий со стороны юридических и физических лиц.

В последние годы арсенал программно-технических средств защиты информации значительно расширился. 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. Динамика изменения применяемых организациями средств защиты информации, установленная по результатам обобщения данных аналитического центра InfoWatch [8] и материалов исследований научно-исследовательского института Высшей школы экономики [14], пока-

Таблица 1 – Динамика возникновения угроз информационной безопасности, % от общего числа

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
Прочие	61,9	66,9	68,3	70,1	70,2

Таблица 2 – Использование средств защиты информации в организациях, %

Вид защиты	2015 г.	2019 г.
Антивирусная программа	85	89
Цифровая подпись	82	85
Логин, пароль	64	66
Спам-фильтр	52	59
Средства шифрования	46	51
Средства обнаружения постороннего вмешательства	31	36
Биометрические средства аутентификации	2	6

зывает усиление внимания к этим вопросам (табл. 2).

Конечно, все современные средства и методы защиты не могут в полной мере исключить влияния на информационную безопасность человеческого фактора. Это особенно касается рядовых сотрудников, как правило, не обремененных дополнительными обязательствами по защите информации. В таких случаях вопросы защиты коммерческой информации достаточно отразить в трудовых договорах, тем более, что законодательно это допускается.

Попытки получения доступа к тайной информации могут быть связаны, например, с проникновением непосредственно на предприятие, в том числе в виде клиента. Однако наиболее часто используемый и простой способ завладения коммерческой тайной конкурента – привлечение действующих или бывших работников. Кроме того, незаконными признаются подкуп работника, содействие нарушению работником условий трудового контракта по соблюдению тайны организации с использованием различных мер вплоть до физических угроз [15].

В то же время информация может стать доступной заинтересованным лицами и законными способами, включая их собственные аналитические способности и опыт. В таком случае необходимо ее разграничение с информацией, полученной незаконным способом. Это достаточно сложная задача, в частности в российском законодательстве неправомерны любые способы получения информации, связанной с коммерческой тайной, без согласия её владельца.

С другой стороны, защитные меры не должны препятствовать развитию бизнеса, поэтому, на наш взгляд, правовое регулирование не может быть абсолютной защитой владельца информации против сторонних лиц действующих в рамках закона. Такую защиту закон может предоставить только в отношении неправомерного использования коммерческой тайны. В связи с этим ее защиту можно рассматривать в качестве меры, гарантирующей свободу предпринимательской деятельности без внешнего вмешательства.

Вопросы защиты информации играют очень важную роль не только в коммерческой деятельности организаций, но и в плане реализации 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 к ним доступ. 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, пытающихся нарушить режим сохранности коммерческой тайны.

Одно из основных препятствий для расширенного использования информационных технологий – неуверенность населения и коммерческих структур в защищенности каналов связи, в первую очередь сети Интернет. По результатам исследований, проведенных НИУ ВШЭ с целью определения основных причин отказа от применения информационных технологий при получении государственных услуг, доля людей, опасающихся утечки информации в последние годы растет (табл. 3) [16]. С этим связана и другая проблема, вызванная необходимостью предоставления дополнительных документов при передаче цифровой информации, для чего нужен личный визит. Остальные причины име-

Таблица 3 – Причины отказа от применения информационных технологий при получении государственных услуг, % от опрошенных

Причина отказа	Год	
	2018	2019
Предпочтение личного визита	52,1	51,1
Необходимость обращения за помощью к другим лицам	18,2	17,2
Недостаток навыков работы	12,3	13,2
Необходимость представления дополнительных документов	12,3	12,7
Опасения по поводу защиты информации	2,4	3,3
Отсутствие доступа к услуге в электронном виде	2	1,9
Проблемы с цифровой подписью	0,7	0,6

ют тенденцию к снижению. Аналогичная ситуация складывается в отношении оборота коммерческой информации.

Выводы. Полученные результаты позволяют сделать вывод о необходимости усиления не только программно-технической защиты информации в сетях, но и пересмотра правового регулирования этой сферы деятельности. В связи с быстрым развитием цифровой экономики и увеличением роли информационных технологий возникает объективная необходимость совершенствования российского законодательства с точки зрения повышения эффективности системы защиты экономической информации. Одновременно следует продолжить работу по повышению качества программно-технических средств защиты, включая криптографические методы.

Литература

1. Ганиева И.А., Бобров Н.Е. Цифровые платформы в сельском хозяйстве России: правовой аспект внедрения // Достижения науки и техники АПК. 2019. Т. 33. № 9. С. 83-86.

2. Валюженич Н. Коммерческая тайна: предпринимательство и лояльность персонала. М.: КноРус, 2018. 779 с.

3. Газетдинов М.Х. Методические вопросы перехода к цифровой экономике в сельском хозяйстве // Развитие АПК и сельских территорий в условиях модернизации экономики: материалы I Международной научно-практической конференции, посвященной 90-летию со дня рождения д.э.н., профессора Н.С. Каткова. Казань: Издательство Казанского ГАУ, 2018. – С. 56-59.

4. Езангина И.А. Проблемы и тенденции развития инфраструктуры кредитных рынков в России // Экономическая безопасность России и стратегии развития ее регионов в современных условиях: Сборник научных трудов Международной научно-практической конференции / Волгоград: Волгоградский государственный технический университет, 2015. С. 67-70.

5. Хачатурян Г.Ю. Институциональные основы экономической безопасности банковской деятельности в современной экономике // Вестник университета (государственный университет управления). 2015. №21. С.15-22.

6. 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.

7. Экономическая безопасность предприятия. Объективные причины появления коммерческой тайны. URL: http://pmn.narod.ru/secur/jgurnal/kt/oppkt.htm (дата обращения: 27.05.2020).

8. Акмаров П.Б., Газетдинов М.Х., Князева О.П. Состояние и основные направления развития цифровой экономики в сельском хозяйстве России // Вестник Казанского ГАУ. 2019. №1 (52). С. 107-112.

9. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации» URL: http://base.garant.ru/12148555/ (дата обращения: 27.05.2020).

10. Koshkina I., Sharamko M. Economic Security and Internal Control of the Academic Research Projects // Procedia - Social and Behavioral Sciences. 2015. No 214. pp. 858 - 865.

11. Клебанов Л.Р. Незаконное получение сведений, составляющих коммерческую, налоговую или банковскую тайну: особенности квалификации // Вестник Омского Университета. Серия: Право. 2014. №2 (39). С. 137 -140.

12. Зиганшин Б.Г. Газетдинов Ш.М. О некоторых методологических аспектах создания и развития цифровой экономики // Развитие АПК и сельских территорий в условиях модернизации экономики: материалы I Международной научно-практической конференции, посвященной 90-летию со дня рождения д.э.н., профессора Н.С. Каткова. Казань: Издательство Казанского ГАУ, 2018. С. 9-11.

13. High Technology Entrepreneurs and the Patent System: Results of the 2008 Berkeley Patent Survey / S.J.H. Graham, R.P. Merges, P. Samuelson, et al. // Berkeley Tech. L.J. 2009. №. 4. С. 1255–1328.

14. Индикаторы цифровой экономики: статистический сборник. М.: НИУ ВШЭ, 2019. 248 с.

15. Bombard G.S. Three Key Distinctions between the Uniform Trade Secrets Act and the Common Law // Commercial & Business Litigation. 2016. No.2. С. 23-27.

16. 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.

Сведения об авторах:

Акмаров Петр Борисович – кандидат экономических наук, профессор кафедры экономической кибернетики и информационных технологий, e-mail: izgsha_ur@mail.ru
ФГБОУ ВО «Ижевская государственная сельскохозяйственная академия», г. Ижевск, Россия.
Газетдинов Миршарип Хасанович – доктор экономических наук, профессор кафедры экономики и информационных технологий, e-mail: mirsharip@yandex.ru
ФГБОУ ВО «Казанский государственный аграрный университет», г. Казань, Россия.
Третьякова Екатерина Сергеевна – кандидат экономических наук, доцент кафедры экономической кибернетики и информационных технологий, e-mail: katiu83@yandex.ru
ФГБОУ ВО «Ижевская государственная сельскохозяйственная академия», г. Ижевск, Россия.

PROBLEMS OF PROTECTION OF COMMERCIAL INFORMATION IN THE CONDITIONS OF ECONOMY DIGITALIZATION

Akmarov P.B., Gazetdinov M.Kh., Tretyakova E.S.

Abstract. In the context of the global informatization of society, the threats of illegal dissemination of information, including deliberate illegal obtaining of commercial information, are increasing many times over. The study of the problem was carried out using statistical tools, methods of analysis and forecasting. The volume of unauthorized use of information has been increasing in recent years. During the period from 2008 to 2018, the number of cases of leakage of information representing commercial secrets increased by 8 times, this growth is mainly due to the use of information technologies, primarily computer networks. This situation causes significant damage to the economy of the country and individual organizations, and also increases the risks of illegal withdrawal and distortion of information in electronic document management systems and when

citizens use electronic payment systems. The most dangerous are unauthorized distribution of information and illegal access to information resources. The use of software and technical methods to protect computers reduces the economic consequences of the spread of malicious programs. However, the population is still wary of the benefits of informatization. Most people prefer face-to-face communication when solving emerging issues, both in the field of public services and in commercial activities. Mistrust in information technologies is due to various reasons, including imperfection of computer programs and technical means of communication, as well as shortcomings in the field of legal protection of information. It is necessary to strengthen not only the software and hardware protection of information in networks, but also to revise the legal regulation of this area of activity. In connection with the rapid development of the digital economy, there is an objective need to improve Russian legislation in terms of increasing the efficiency of the system for protecting economic information. At the same time, work should continue to improve the quality of software and hardware protection tools, including cryptographic methods.

Key words: trade secrets, legal protection of information, informatization, information leakage, technical protection of information, cryptography, innovative development, digital transformation.

References

1. Ganieva I.A., Bobrov N.E. Digital platforms in agriculture in Russia: the legal aspect of implementation. [Tsifrovye platformy v selskom khozyaystve Rossii: pravovoy aspekt vnedreniya]. // *Dostizheniya nauki i tekhniki APK. - Achievements of science and technology of the agro-industrial complex*. 2019. Vol. 33. № 9. P. 83-86.

2. Valyuzhenich N. *Kommercheskaya tayna: predprinimatelstvo i loyalnost personala.* [Commercial secret: entrepreneurship and personnel loyalty]. M.: KnoRus, 2018. P. 779.

3. Gazetdinov M.Kh. *Metodicheskie voprosy perekhoda k tsifrovoy ekonomike v selskom khozyaystve. // Razvitie APK i selskikh territoriy v usloviyakh modernizatsii ekonomiki: materialy I Mezhdunarodnoy nauchno-prakticheskoy konferentsii, posvyaschennoy 90-letiyu so dnya rozhdeniya d.e.n., professora N.S. Katkova*. (Methodological issues of the transition to a digital economy in agriculture. // Development of the agro-industrial complex and rural areas in the context of economic modernization: proceedings of I International scientific and practical conference, dedicated to the 90th anniversary of the birth of Doctor of Economics, Professor N.S. Katkov). Kazan: Idatelstvo Kazanskogo GAU, 2018. – P. 56-59.

4. Ezangina I.A. *Problemy i tendentsii razvitiya infrastruktury kreditnykh rynkov v Rossii. // Ekonomicheskaya bezopasnost Rossii i strategii razvitiya ee regionov v sovremennykh usloviyakh: Sbornik nauchnykh trudov Mezhdunarodnoy nauchno-prakticheskoy konferentsii*. (Problems and trends in the development of credit markets infrastructure in Russia. // Economic security of Russia and strategies for the development of its regions in modern conditions: Collection of scientific papers of International scientific and practical Conference). / Volgograd: Volgogradskiy gosudarstvennyy tekhnicheskiy universitet, 2015. P. 67-70.

5. Khachaturyan G.Yu. Institutional foundations of the economic security of banking in the modern economy. [Institutsionalnye osnovy ekonomicheskoy bezopasnosti bankovskoy deyatelnosti v sovremennoy ekonomike]. // *Vestnik universiteta (gosudarstvennyy universitet upravleniya). – The Herald of University (State University of Management)*. 2015. № 21. P.15-22.

6. Sazonov S.P., Ezangina I.A., Evseev R.S. Economic security of a credit institution: factors, threats, directions of strengthening. [Ekonomicheskaya bezopasnost kreditnoy organizatsii: faktory, ugrozy, napravleniya ukrepleniya]. // *Finansovaya analitika: problemy i resheniya. - Financial analytics: problems and solutions*. 2016. № 31 (313). P. 42-56.

7. *Ekonomicheskaya bezopasnost predpriyatiya. Obektivnye prichiny poyavleniya kommercheskoy tayny.* (Economic security of the enterprise. Objective reasons for the emergence of commercial secrets). URL: http://pmn.narod.ru/secur/jgurnal/kt/oppkt.htm (date of access: 27.05.2020).

8. Akmarov P.B., Gazetdinov M.Kh., Knyazeva O.P. State and main directions of the digital economy development in agriculture of Russia. [Sostoyanie i osnovnye napravleniya razvitiya tsifrovoy ekonomiki v selskom khozyaystve Rossii]. // *Vestnik Kazanskogo GAU. – The Herald of Kazan State Agrarian University*. 2019. №1 (52). P. 107-112.

9. *Federalnyy zakon ot 27 iyulya 2006 g. № 149-FZ "Ob informatsii, informatsionnykh tekhnologiyakh i o zaschite informatsii"*. (Federal Law of July 27, 2006 № 149-FZ "On information, information technologies and information protection"). Available at: http://base.garant.ru/12148555/ (date of access: 27.05.2020).

10. Koshkina I., Sharamko M. Economic security and Internal control of the Academic Research projects. // Procedia - Social and Behavioral Sciences. 2015. No 214. P. 858 - 865.

11. Klebanov L.R. Illegal receipt of information, constituting commercial, tax or banking secrets: qualifications features. [Nezakonnoe poluchenie svedeniy, sostavlyayushchikh kommercheskuyu, nalogovuyu ili bankovskuyu taynu: osobennosti kvalifikatsii]. // *Vestnik Omskogo Universiteta. Seriya: Pravo. The Herald of Omsk University. Series: Law*. 2014. №2 (39). P. 137-140.

12. Ziganshin B.G., Gazetdinov Sh.M. *O nekotorykh metodologicheskikh aspektakh sozdaniya i razvitiya tsifrovoy ekonomiki. // Razvitiye APK i selskikh territoriy v usloviyakh modernizatsii ekonomiki: materialy I Mezhdunarodnoy nauchno-prakticheskoy konferentsii, posvyaschennoy 90-letiyu so dnya rozhdeniya d.e.n., professora N.S. Katkova*. (On some methodological aspects of the creation and development of the digital economy. // Development of agro-industrial complex and rural areas in the context of economic modernization: proceedings of I International scientific-practical conference, dedicated to the 90th anniversary of the birth of Doctor of Economics, Professor N.S. Katkov). Kazan: Idatelstvo Kazanskogo GAU, 2018. P. 9 -11.

13. High Technology Entrepreneurs and the Patent System: Results of the 2008 Berkeley Patent Survey / S.J.H. Graham, R.P. Merges, P. Samuelson, et al. // Berkeley Tech. L.J. 2009. №. 4. С. 1255–1328.

14. *Indikatory tsifrovoy ekonomiki: statisticheskiy sbornik*. [Indicators of the digital economy: statistical collection]. M.: NIU VShE, 2019. P. 248.

15. Bombard G.S. Three Key Distinctions between the Uniform Trade Secrets Act and the Common Law // Commercial & Business Litigation. 2016. No.2. P. 23-27.

16. Akmarov P.B., Voytovich V.Yu., Tretyakova E.S. Increasing the efficiency of public administration in the context of the information society development. [Povyshenie effektivnosti gosudarstvennogo upravleniya v usloviyakh razvitiya informatsionnogo obschestva]. // *Nauka Udmurtii. - Science of Udmurtia*. 2019. № 1 (87). P. 11-18.

Authors:

Akmarov Petr Borisovich – Ph.D. of Economic Sciences, Professor of Economic Cybernetics and Information Technologies Department, e-mail: izgsha_ur@mail.ru

Izhevsk State Agricultural Academy, Izhevsk, Russia.

Gazetdinov Mirsharip Khasanovich - Doctor of Economics, Professor of Economics and Information Technologies Department, e-mail: mirsharip@yandex.ru

Kazan State Agrarian University, Kazan, Russia.

Tretyakova Ekaterina Sergeevna – Ph.D. of Economic Sciences, associate professor of Economic Cybernetics and Information Technologies Department, e-mail: katiu83@yandex.ru

Izhevsk State Agricultural Academy, Izhevsk, Russia.