Шумилина В.Е., канд. экон. наук, доцент кафедры «Экономическая безопасность, учет и право» ФГБОУ ВО ДГТУ, г. Ростов-на-Дону, Россия; shumilina.vera@list.ru

Казакова В.А., студент 5 курса ДГТУ, г.Ростов-на-Дону, Россия; victoria-357@mail.ru

КОММЕРЧЕСКАЯ ТАЙНА И ОТВЕТСТВЕННОСТЬ ЗА ЕЕ РАЗГЛАШЕНИЕ

Аннотация.В данной статье раскрываются способы разглашения информации, составляющую коммерческую тайну и последствия данного деяния, а так же виды ответственности и меры по обеспечению сохранности этой информации.

Ключевые слова: коммерческая тайна, разглашение, ответственность, сохранность информации.

Shumilina V.E., Candidate of Economic Sciences, Associate Professor of the Department of «Economic Security, Accounting and Law», Rostov-on-Don, Russia shumilina.vera@list.ru

Kazakova V.A., 5th year student of DSTU, Rostov-on-don, Russia; victoria-357@mail.ru

COMMERCIAL SECRET AND LIABILITY FOR HER DISCLOSURE

Abstract. This article reveals the methods of disclosing information that constitutes a trade secret and the consequences of this act, as well as the types of responsibility and measures to ensure the safety of this information.

Keywords: commercial secret, disclosure, responsibility, safety of information.

Коммерческая тайна – это информация, которую компания не раскрывает в целях увеличения доходов, избегания ненужных расходов, поддержания или улучшения своего положения на рынке или получения любых других коммерческих преимуществ. Засекретить можно рыночную стратегию и

бизнес-тактику, списки клиентов и поставщиков, правила ценообразования [3].

Коммерческая тайна может включать в себя любую информацию, имеющую реальную или потенциальную коммерческую ценность из-за того, что она не известна третьим лицам, для которых она не является свободно доступной на законной основе и для которой владелец такой информации ввелрежим конфиденциальности.

Коммерческая тайна может быть разнообразной: информация о методах работы с покупателями, разработке новых продуктов, использовании оборудования, новых технологий и многое другое. Это любая информация, которая позволяет организации получать прибыль или определенный доход.

Под режимом коммерческой тайны понимаются организационные, технические или правовые меры, принимаемые владельцем для защиты своей конфиденциальности.

Согласно Федеральному закону «О коммерческой тайне» от 29.07.2004 №98-ФЗ, к информации, составляющей коммерческую тайну, могут относиться данные, представленные на рисунке 1.

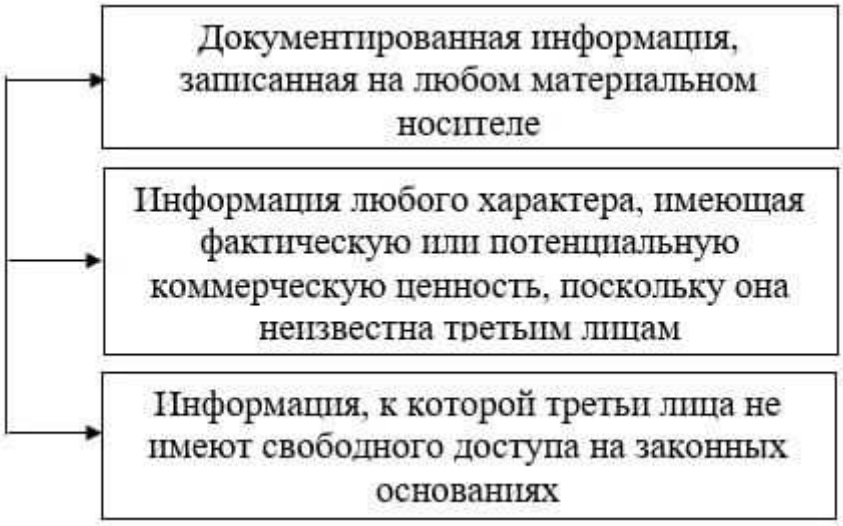

Рисунок 1 – Информация, составляющая коммерческую тайну [1]

Однако коммерческая тайна не может быть установлена в отношении информации, указанной в на рисунке 2.

Рисунок 2 – Информации, в отношении которой режим коммерческой тайны не устанавливается

Информация, составляющая коммерческую тайну, должна быть предоставлена государственным органам по их мотивированному запросу. При этом государственные органы обязаны обеспечивать конфиденциальность предоставляемой информации, не допускать ее распространения или утечки.

Меры по защите конфиденциальной информации должны включать[2]:

– определение перечня сведений, составляющих коммерческую тайну;

– ограничение доступа к этой информации путем установления порядка обращения с этой информацией и контроля за ее соблюдением;

– регистрацию лиц, получивших доступ к информации;

– регулирование отношений по использованию этой информации с работниками на основании трудовых договоров с контрагентами на основании гражданско-правовых договоров;

– нанесение грифа на материальных носителях (документах) с указанием владельца данной информации.

Все это позволяет создавать определенные барьеры для распространения такой информации и тем самым поддерживать конкурентное преимущество организации. Однако за информационную безопасность в первую очередь отвечает сама организация. И это в основном зависит от того, насколько хорошо хранится эта информация. В конце концов, любой конкурент, любая другая организация может пожелать получить доступ к новым технологиям, моделям обслуживания клиентов и т.п. при случайных обстоятельствах. Компания несет ответственность за безопасность этих данных.

В целях защиты конфиденциальной информации работодатель обязан ознакомить работника с подписанием установленного режима коммерческой тайны и мерами ответственности за его нарушение, а также создать необходимые условия для соблюдения работником этого режима. Соответственно, у организации должен быть документ, регулирующий эти вопросы, а также перечень информации, к которой применяется этот режим. Кроме того, каждый сотрудник должен прочитать этот документ. В противном случае иск о разглашении коммерческой тайны ему не может быть предъявлен.

При раскрытии информации, в отношении которой установлена коммерческая тайна, нематериальность самого предмета (информации) приводит к объективной сложности доказательств как самого факта раскрытия, так и факта его возникновения. Если предмет был нематериальным, будет очень сложно доказать, что он был украден, распространен тем или иным способом, а главное, украден конкретным человеком. Работа с коммерческой тайной – это случай, когда преступление легче предотвратить, чем позже доказать факт его совершения и найти виновных в разглашении коммерческой тайны.

В соответствии с законодательством Российской Федерации к виновным в незаконном разглашении и использовании конфиденциальной информации, а также информации, составляющей коммерческую тайну, могут быть

привлечены такие виды ответственности: дисциплинарная, гражданско-правовая, административная и уголовная.

Правовая защита информации, составляющей коммерческую тайну, обеспечивается установлением в организации особого правового режима для коммерческой тайны. Режим – это совокупность правовых средств, которые характеризуют систему запретов, разрешений, рекомендаций, обязательств, стимулов и санкций во взаимодействии друг с другом. Необходимой мерой для надежного поддержания режима коммерческой тайны является составление его держателями должным образом оформленных соглашений о конфиденциальности или других документов, подтверждающих обязательство не разглашать коммерческую тайну.

Помимо обязательных мер, руководитель может устанавливать дополнительные меры обеспечения коммерческой тайны (рисунок 3).

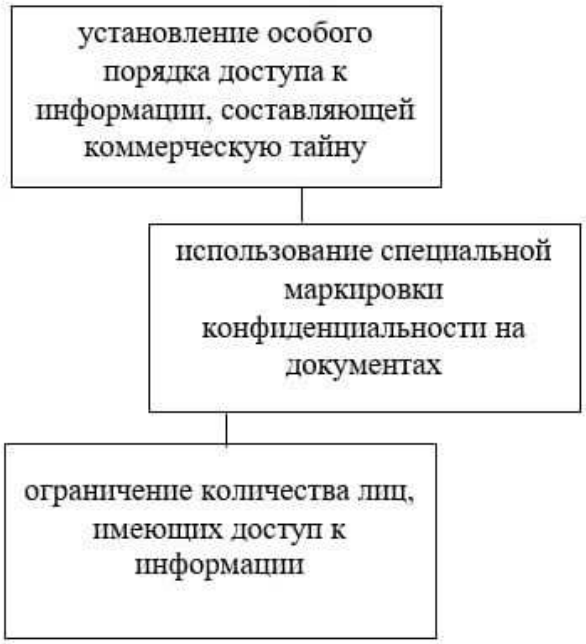

Рисунок 3 – Дополнительные меры по обеспечению режима коммерческой тайны

Основными методами обеспечения безопасного хранения информации, составляющей коммерческую тайну, являются барьеры, маскировка информации и регулирование. Основным средством защиты конфиденциальной информации является сохранение физических, программных, организационных и конфиденциальных документов.

Для обеспечения качественной системы безопасности необходимо рассматривать каждый метод в отдельности, а также определять наиболее приемлемые способы защиты коммерческой тайны для каждого метода.

Для совершенствования системы защиты коммерческой тайны на предприятии необходимо улучшить несколько различных показателей. В первую очередь необходимо обрати внимание на физические средства защиты (рисунок 4).

Рисунок 4 – Физические методы защиты конфиденциальных данных

Наиболее рациональным выбором мер физической безопасности для многих предприятий является использование системы охраны периметра и создание удаленного доступа к чувствительным объектам за счет использования на предприятии высокотехнологичного и дорогостоящего оборудования. При выборе и проектировании системы следует учитывать множество факторов. Однако любая периметральная система должна отвечать определенному набору требований.

Другой мерой защиты конфиденциальной информации на предприятии может быть внедрение системы управления конфиденциальными документами, поскольку некоторые данные записываются на бумаге. Конфиденциальное ведение записей помогает сохранить данные, содержащие коммерческую тайну, а также обеспечить безопасный доступ к этой информации и ее уничтожение. Документ, описывающий правила использования конфиденциальных данных,

является инструкцией по обращению конфиденциальных документов (рисунок 5).

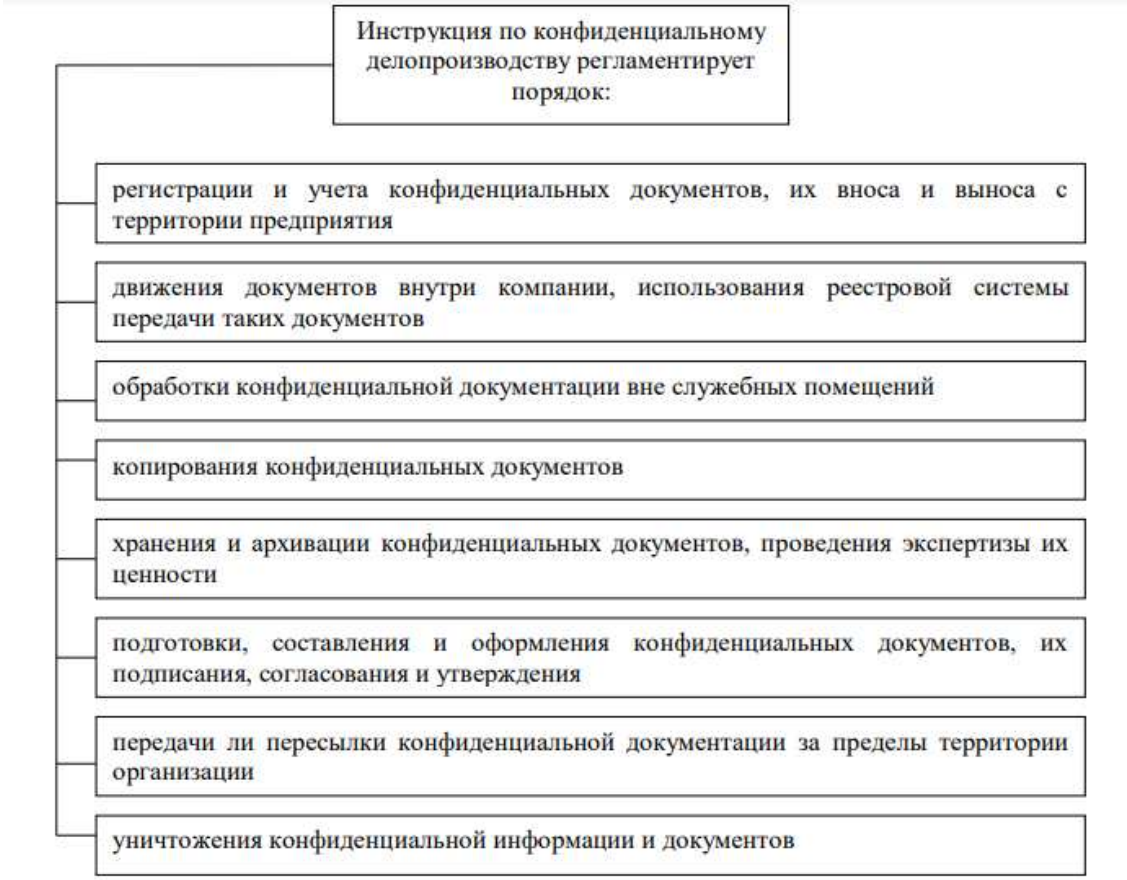

Рисунок 5 – Инструкция по ведению конфиденциального делопроизводства

Еще одна мера защиты конфиденциальной информации – это защита программного обеспечения.

Программное обеспечение безопасности включает программы для идентификации пользователя, удаления остаточной информации, контроля доступа и т. д. Однако у них есть как достоинства, так и недостатки. Преимущества программных инструментов влияют на их универсальность, гибкость, надежность и модифицируемость. К недостаткам можно отнести высокую чувствительность к случайным изменениям, возможную зависимость от типов компьютеров.

Основным источником утечки информации на предприятии является ее персонал. Свести к минимуму человеческий фактор – самый сложный и самый основной механизм безопасности. Существуют определенные рекомендации по

системе организационных мероприятий, направленных на сохранность информации (рисунок 6).

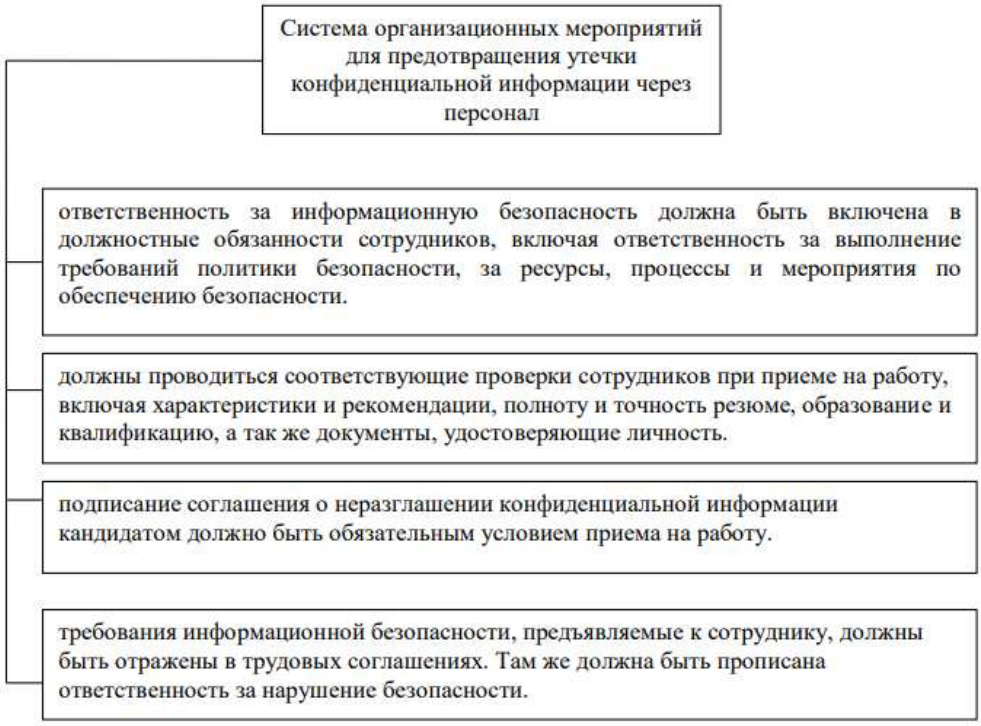

Рисунок 6 – Система организационных мероприятий для предотвращения утечки конфиденциальной информации через персонал

Для того, чтобы проводить обучение и контролировать определенный уровень знаний предприятия необходимо учитывать несколько вопросов (рисунок 7).

Рисунок 7 – Информация, необходимая для ознакомления сотрудниками предприятия

Всю кадровую работу по защите коммерческой тайны необходимо разделить на несколько этапов:

1. Предварительный – мероприятия перед приемом на должность.

2. Этап трудовых отношений специалиста в компании.

3. Заключительный этап – процесс увольнения сотрудника.

Организационные меры, направленные на усиление защиты режима коммерческой тайны, следует возложить на штатных сотрудников компании. Не рекомендуется привлекать сторонних специалистов в связи с действующим на предприятии режимом секретности.

Раскрытие информации, составляющей коммерческую тайну, – это действие или бездействие, в результате которого эта информация станет известной любой третьей стороне в любой допустимой форме без согласия владельца этой информации или в нарушение трудового или гражданско-правового договора.

Есть несколько способов украсть информацию. Самый распространенный способ – продать информацию конкурентам. Эти действия выполняются сотрудниками, имеющими доступ к коммерческой тайне. Возможна ее продажа для личной выгоды, или бывают случаи, когда сотрудники хотят «отомстить» своему руководству и поэтому рассматривают продажу коммерческих секретов как хорошую возможность для этого.

Разговорчивые сотрудники тоже могут стать причиной разглашения коммерческой тайны. Сотрудник может без злого умысла раскрывать семье, друзьям или коллегам информацию, которая составляет для них коммерческую тайну. Любой, кто узнает об этих конфиденциальных данных, может использовать их в своих целях против компании. Но даже если такие действия не наносят вреда бизнесу, они все равно считаются разглашением коммерческой тайны.

Если кто-то случайно или по ошибке получает доступ к коммерческой тайне и разглашает ее, не подозревая, что он нарушает закон, он не несет за это

ответственности. Однако затем можно обязать его хранить информацию в секрете, и повторное разглашение не останется безнаказанным [6].

Сотрудник, получивший секретную информацию напрямую от своего владельца, получил ее на законных основаниях. Однако, если нигде не записано, что он знает коммерческую тайну, его нельзя привлечь к ответственности. Поэтому необходимо договариваться с сотрудниками и брать расписку [5]. Привлечь сотрудника к ответственности без документов, требующих коммерческой тайны, практически невозможно.

Еще один способ разглашения коммерческой тайны – предоставить свободный доступ к информации посторонним. Оставляя данные без присмотра на рабочем месте или открытый документ на компьютере, сотрудник может распространять информацию среди других сотрудников и посетителей компании.

При открытии собственного дела сотрудник также может использовать информацию, полученную на старых рабочих местах. Этот метод раскрытия деловой информации можно назвать «хищением», поскольку предыдущие работодатели не давали согласия на использование информации. Есть много причин для кражи данных, но главная причина – это собственная прибыль.

Разглашение коммерческой тайны имеет негативные последствия для компании, а именно приводит к снижению ее производительности, ведь коммерческая тайна – это данные, которые позволят предотвратить неоправданное падение прибыли, максимизировать ее и, конечно же, занять лидирующие позиции на рынке.

Таким образом, можно сделать вывод, что разглашение коммерческой тайны является нарушением и тот, кто его совершил, должен быть наказан.

Работодатель и государство обязаны принимать различные меры для обеспечения безопасности информации, составляющей коммерческую тайну.

Для компании должна быть очень важна защита своей коммерческой тайны, поэтому в соответствии с федеральным законом работодатель должен

установить режим коммерческой тайны, который представляет собой ряд мер, предпринимаемых работодателем для обеспечения безопасности информации.

Работник обязан не разглашать информацию, составляющую коммерческую тайну, принадлежащую работодателю и его контрагентам, и не использовать эту информацию в личных целях без их согласия в течение всего срока действия коммерческой тайны и даже после расторжения трудового договора. Однако на практике очень сложно доказать вину за имущественный ущерб, нанесенный действиями бывших работников, поэтому работодателям стоит задуматься о необходимости легализации служб безопасности, которые следят за утечкой информации, повышают качество своей работы, поскольку сотрудники часто могут получить секретную информацию из-за недостаточного контроля над данными. Совершенно необходимо вести учет людей, имеющих доступ к информации, составляющей коммерческую тайну.

Работодатель должен быть заинтересован в защите коммерческой тайны и поэтому должен создать для сотрудника условия в компании, которые позволят ему соблюдать режим коммерческой тайны.

Государство также не должно оставаться в стороне и, следовательно, должно разрешить работодателям вводить строгие меры контроля и проверки за этой информацией.

Следует обратить внимание на тот важный момент, что к ответственности привлекаются только лица, совершившие кражу коммерческой тайны, а покупатели этой информации, которые могли оказать на них давление с целью совершения этого преступления, остаются безнаказанными. Эти покупатели так же виновны в этом деянии, как и рабочие, которые его совершили. Следовательно, государству необходимо рассмотреть возможность разработки положений в законодательстве, которые вводят ответственность для лиц, получивших информацию. Для компании это было бы действенной мерой по защите коммерческой тайны, поскольку в этом случае конкуренту придется несколько раз подумать, стоит ли покупать украденную информацию, если он несет серьезную юридическую ответственность за такие действия.

Таким образом, можно сделать вывод, что коммерческая тайна является очень важным элементом любого предприятия, а ее разглашение является серьезным преступлением со стороны сотрудника, которое может привести к крупным убыткам. Если сотрудник будет признан виновным в раскрытии информации, к нему будут применены соответствующие санкции. Работодатель должен использовать различные методы защиты коммерческой тайны. Государству также следует рассмотреть возможность введения в законодательство конкретных стандартов, которые улучшат методы защиты коммерческой тайны.

Список литературы:

1. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (ред. от 09.03.2021).
2. Давыдова О.Б. Коммерческая тайна и меры по ее защите // Вестник науки и образования. – 2018. – №6. – С. 91-93.
3. Крутин Ю.В. Защита коммерческой тайны: конспект лекций. – Екатеринбург, 2020. – 31с.
4. Рудакова А.Н., Макаревич М.Л. Обеспечение сохранности коммерческой тайны на предприятии // Международная научно-практическая конференция, 2017.– С.226-230.
5. Сапрунов С.Р., Колесник В.В. Актуальные проблемы защиты коммерческой тайны в Российской Федерации // Colloquium-journal. – 2019. – №3-4(27). – С.62-63.
6. Слюсарь И.В. Коммерческая тайна: основные положения, основы правового регулирования // Молодой ученый. – 2020. – №3(293). – С.224-227.
7. Шумилина, В. Е. Информационная безопасность как составляющая экономической безопасности предприятия / В. Е. Шумилина, Е. В. Тетунашвили // Управление безопасностью

бизнеса в современных условиях. – Москва : AUSPUBLISHERS, 2021. – С. 119-129.

8. Шумилина, В. Е. Основные проблемы защиты конфиденциальной информации и пути их решения / В. Е. Шумилина, Ю. И. Коптева, С. А. Тевосян // : Современные проблемы экономической безопасности, учета и права в Российской Федерации. Том 3, 11 января 2018 года – 31 2019 года, 2019. – С. 9. – DOI 10.26526/conferencearticle_5c5060d2f3afe7.25271992.
9. Шумилина, В. Е. Информационная безопасность как фактор обеспечения экономической безопасности / В. Е. Шумилина, К. Н. Абдуллаева, Ю. А. Топор // Актуальные вопросы обеспечения экономической безопасности в Российской Федерации в условиях цифровой экономики. – Мельбурн : AUS PUBLISHERS, 2018. – С. 1-7.
10. Шумилин, П. Е. Влияние корпоративного мошенничества на бизнес и экономическую безопасность страны в целом / П. Е. Шумилин, П. С. Нежижимова // : Современные проблемы экономической безопасности, учета и права в Российской Федерации. Том 2, 11 января 2018 года – 31 2019 года, 2019. – С. 5. – DOI 10.26526/conferencearticle_5c50608a3442c1.05921536.
11. Управление безопасностью бизнеса в современных условиях / Н. Ю. Изварина, А. Н. Соколова, Ю. Р. Мезенцева [и др.]. – Москва : AUSPUBLISHERS, 2021. – 239 с. – DOI 10.26526/978-0-6487435-9-0.

References:

1. Federal Law of 29.07.2004 No. 98-FZ "On Commercial Secrets" (as amended on 09.03.2021).

2. Davydova O.B. Commercial secret and measures to protect it // Bulletin of Science and Education. – 2018. – No. 6. – pp. 91-93.
3. Krutin Y.V. Protection of trade secrets: lecture notes. – Yekaterinburg, 2020. – 31p.
4. Rudakova A.N.,Makarevich M.L. Ensuring the safety of commercial secrets at the enterprise // International Scientific and Practical Conference, 2017, pp. 226-230.
5. Saprunov S.R., Kolesnik V.V. Actual problems of protecting commercial secrets in the Russian Federation // Colloquium-journal. – 2019. – No. 3-4 (27). – pp.62-63.
6. Slyusar I.V. Commercial secret: basic provisions, foundations of legal regulation // Young scientist. – 2020. – No. 3 (293). – pp.224-227.
7. Shumilina, V. E. Information security as a component of the economic security of an enterprise / V. E. Shumilina, E. V. Tetunashvili // Business security management in modern conditions. - Moscow: AUSPUBLISHERS, 2021 .-- S. 119-129.
8. Shumilina, V. E. The main problems of protecting confidential information and ways to solve them / V. E. Shumilina, Yu. I. Kopteva, S. A. Tevosyan //: Modern problems of economic security, accounting and law in the Russian Federation. Volume 3, January 11, 2018 - 31 2019, 2019 .-- P. 9. - DOI 10.26526 / conferencearticle_5c5060d2f3afe7.25271992.
9. Shumilina, V. Ye. Information security as a factor in ensuring economic security / V. E. Shumilina, K. N. Abdullaeva, Yu. A. Topor // Topical issues of ensuring economic security in the Russian Federation in the digital economy. - Melbourne: AUS PUBLISHERS, 2018 .-- S. 1-7.
10. Shumilin, P. Ye. Influence of corporate fraud on business and economic security of the country as a whole / P. E. Shumilin, P. S. Nezhimova //: Modern problems of economic security, accounting and law in the

Russian Federation. Volume 2, January 11, 2018 - 31 2019, 2019 .-- P. 5. - DOI 10.26526 / conferencearticle_5c50608a3442c1.05921536.

11. Business safety management in modern conditions / N. Yu. Izvarina, AN Sokolov, Yu. R. Mezentseva [and others]. - Moscow: AUSPUBLISHERS, 2021 .-- p. 239. - DOI 10.26526 / 978-0-6487435-9-0.