

Дата поступления рукописи в редакцию: 05.04.2025

DOI: 10.24412/3034-4395-2025-1-43-49

Дата принятия рукописи к печати: 30.04.2025

**ГЛУШКОВ Валентин Алексеевич,**

*Студент Кузбасского гуманитарно-педагогического института федерального государственного бюджетного образовательного учреждения высшего образования «Кемеровский государственный университет»,*

*e-mail: valekpike@gmail.com*

*Научный руководитель:*

**БЕЛАРЕВА Ольга Александровна,**

*Кузбасский гуманитарно-педагогический института федерального государственного бюджетного образовательного учреждения высшего образования «Кемеровский государственный университет»,*

*e-mail: belarev@mail.ru*

## **КЛАССИФИКАЦИЯ ДАННЫХ В DLP-СИСТЕМАХ: ПРОБЕЛЫ В ЛОКАЛЬНОМ РЕГУЛИРОВАНИИ И ПРАВОВЫЕ ПОСЛЕДСТВИЯ**

**Аннотация.** В современном цифровом мире использование систем предотвращения утечек данных стало неотъемлемой частью информационной безопасности организаций. Однако отсутствие локальных нормативных актов, классифицирующих данные как персональные или коммерческую тайну, создает правовые пробелы, которые затрудняют привлечение сотрудников к ответственности за разглашение информации. В статье анализируются основные юридические риски, возникающие при отсутствии ЛНА, определяющих статус данных, исследуются последствия таких пробелов для правоприменительной практики, а также предлагаются меры по совершенствованию локального и нормативно-правового регулирования в этой сфере.

**Ключевые слова:** классификация данных, DLP, пробелы в локальном регулировании, правовые последствия, легитимизация DLP.

**GLUSHKOV Valentin Alekseevich,**

*Student, Kuzbass Humanitarian Pedagogical Institute of the Federal State Budgetary Educational Institution of Higher Education "Kemerovo State University"*

*Scientific supervisor:*

**BELAREVA Olga Alexandrovna**

*Kuzbass Humanitarian Pedagogical Institute of the Federal State Budgetary Educational Institution of Higher Education "Kemerovo State University"*

## **CLASSIFICATION OF DATA IN DLP SYSTEMS: GAPS IN LOCAL REGULATION AND LEGAL IMPLICATIONS**

**Annotation.** In the modern digital world, the use of data leak prevention systems has become an integral part of the information security of organizations. However, the absence of local regulations classifying data as personal or commercial secrets creates legal gaps that make it difficult to hold employees accountable for disclosing information. The article analyzes the main legal risks that arise in the absence of LNA, which determines the status of data, examines the consequences of such gaps for law enforcement practice, and suggests measures to improve local and regulatory regulation in this area.

**Key words:** data classification, DLP, gaps in local regulation, legal consequences, legitimization of DLP.

В современном мире данные являются ключевым активом, определяющим успешность и устойчивость бизнеса. Защита информации, особенно персональных данных (далее - ПД) и коммерческой тайны (далее - КТ), становится все более важной задачей для компаний. С развитием технологий растет не только объем данных, но и число угроз их утечки, включая внутренние инциденты, вызванные действиями сотрудников. В таких условиях организации активно внедряют системы Data Loss Prevention (далее - DLP), способные мониторить и предотвращать утечки данных. Однако несмотря на высокую технологическую эффективность DLP-систем, их использование в России сталкивается с серьезными юридическими ограничениями. Главным из них является отсутствие локальных нормативных актов (далее - ЛНА), регулирующих порядок обработки данных и реагирования на инциденты.

ЛНА, представляющие собой внутренние документы компании, закрепляют ключевые аспекты работы с информацией: правила ее классификации, обработки, разграничения доступа, а также порядок действий в случае инцидентов. В них должны быть отражены как законодательные требования, так и внутренние потребности организации. Но, как показывает практика, многие компании ограничиваются минимальным набором правил или вовсе не разрабатывают такие документы. Это создает юридический вакуум, когда действия сотрудников и использование DLP-систем оказываются вне четкого правового поля. Особенно это касается работы с ПД и КТ, которые требуют строгого соблюдения норм законодательства и учета прав всех вовлеченных сторон.

Без локальных нормативных актов работодатели сталкиваются с множеством рисков. Например, мониторинг сотрудников без их информирования может быть расценен как нарушение их прав. Данные, собранные через DLP-системы, могут быть признаны недопустимыми в суде, если не существует четко прописанного порядка их использования. Отсутствие ЛНА также осложняет защиту КТ, так как без утвержденного перечня таких данных их разглашение сложно квалифицировать как нарушение. Эти и другие проблемы требуют более глубокого анализа, а также разработки практических рекомендаций по созданию и внедрению ЛНА.

Цель данной статьи — исследовать

роль ЛНА в защите ПД и КТ, проанализировать существующее законодательство и судебную практику, а также предложить конкретные решения для минимизации юридических рисков, связанных с использованием DLP-систем. Особое внимание будет уделено разработке регламентов, обеспечивающих защиту интересов работодателя и соблюдение прав сотрудников.

ЛНА занимают центральное место в системе внутреннего регулирования компании, особенно в вопросах обработки и защиты данных. Эти документы создают основу для работы с информацией, определяя правила и процедуры, которых должны придерживаться все сотрудники. В условиях цифровизации ЛНА стали важнейшим инструментом не только для обеспечения безопасности данных, но и для минимизации юридических рисков.

Например, одна из ключевых функций ЛНА заключается в классификации данных. Компания должна четко определить, какие категории информации являются конфиденциальными и подлежат защите. Это особенно важно для коммерческой тайны и персональных данных, поскольку законодательство РФ предъявляет к ним особые требования. Без четко прописанной классификации работодатель не сможет доказать, что определенные сведения относятся к коммерческой тайне, а значит, не сможет привлечь сотрудника к ответственности за их разглашение. Подобные ситуации неоднократно становились предметом судебных разбирательств, где отсутствие утвержденного перечня КТ играло решающую роль в пользу работников.

Кроме того, ЛНА регламентируют порядок работы DLP-систем. Предмет регулирования включает мониторинг трафика, анализ действий сотрудников и хранение данных, которые могут быть использованы для расследования инцидентов. Например, DLP-система может зафиксировать факт передачи сотрудником конфиденциальной информации на внешний носитель. Но если внутренние регламенты не предусматривают таких действий или сотрудники не уведомлены о мониторинге, такие данные могут быть признаны незаконно собранными. Таким образом, ЛНА позволяют легализовать использование DLP-систем и обеспечить соответствие законодательству процесс сбора данных.

Одной из центральных проблем, с

которыми сталкиваются компании при отсутствии ЛНА, является неясность в классификации данных и правовой статус информации. Российское законодательство определяет два ключевых понятия — ПД и КТ, которые требуют особого режима защиты.

Персональные данные, согласно статье 3 Федерального закона №152-ФЗ «О персональных данных» [3], (далее – Федеральный закон №152-ФЗ) включают любую информацию, относящуюся к прямо или косвенно определенному физическому лицу (например, имя, номер телефона, адрес электронной почты, данные о здоровье или биометрические данные). Коммерческая тайна, в свою очередь, определяется статьей 3 Федерального закона №98-ФЗ «О коммерческой тайне» [4] (далее – Федеральный закон № 98-ФЗ) как информация, которая имеет коммерческую ценность в силу ее неизвестности третьим лицам, не является общедоступной и охраняется организацией, принявшей меры для ее защиты.

Обе категории данных требуют строгого соблюдения правовых норм. Для ПД это означает обязательное информирование субъектов данных о целях обработки, а также меры по защите конфиденциальности. Для КТ необходимо создание перечня охраняемой информации, установление режима коммерческой тайны и обеспечение его соблюдения. ЛНА становятся ключевым инструментом для выполнения этих требований, поскольку без них компания не может четко зафиксировать статус данных или установить порядок их защиты.

Без ЛНА компании часто оказываются в ситуации, когда использование персональных данных сотрудников становится юридически ничтожным. Например, согласно статье 86 Трудового кодекса РФ [2], работодатель обязан уведомить работников о сборе, обработке и хранении их персональных данных. Отсутствие документального подтверждения таких действий, как правило, приводит к судебным спорам и административным штрафам.

Примером является дело компании «Альфа», где сотрудники оспорили действия работодателя, связанного с мониторингом их электронной переписки через DLP-систему [12]. В отсутствие утвержденных ЛНА, описывающих порядок использования таких систем, суд признал действия компании незаконными. Работодатель

был оштрафован на основании статьи 13.11 КоАП РФ [1] за нарушение порядка обработки ПД.

Схожая ситуация возникла в деле №44а-1189/2018 [6], когда компания использовала данные сотрудников для внутреннего расследования. Сотрудники подали жалобу, заявив, что их не уведомляли о сборе таких данных. В результате Роскомнадзор привлек компанию к ответственности и наложил штраф в размере 300 000 рублей.

Для коммерческой тайны ситуация еще сложнее, так как ее защита требует активных действий со стороны компании. Согласно статье 10 Федерального закона №98-ФЗ, для признания информации коммерческой тайной организация должна не только включить сведения в соответствующий перечень, но и обеспечить конфиденциальность. Если данные не классифицированы и не закреплены в ЛНА, суды отказываются признавать их коммерческой тайной.

Примером служит дело № 2-1809/2020 [7], где компания предъявила иск бывшему сотруднику за разглашение коммерческой тайны. Ответчик передал внутренние отчеты конкурентам, однако суд отказался признать их охраняемой информацией, так как у истца отсутствовал утвержденный перечень сведений составляющих КТ, а сам режим коммерческой тайны не был formalizован.

В другом деле, № 2-3998/2020 [8], компания попыталась привлечь к ответственности сотрудника, который опубликовал данные о маркетинговой стратегии в открытом доступе. Суд отказал в удовлетворении требований, сославшись на то, что организация не приняла мер для обеспечения конфиденциальности этих сведений, включая отсутствие политики по защите КТ.

Еще одним важным аспектом является использование DLP-систем для мониторинга действий сотрудников. Такие системы анализируют рабочую активность, включая доступ к файлам, отправку писем, использование внешних устройств. Однако без четко прописанных ЛНА их применение может быть расценено как нарушение прав работников.

Например, в деле № 33-2043/2021 [9] суд рассматривал жалобу сотрудника, уволенного за передачу конфиденциальной информации третьим лицам. Работодатель представил данные, собранные DLP-системой, но суд признал их недопустимыми доказательствами, так как сотрудники не были

уведомлены о работе системы и не давали согласие на мониторинг.

Схожий случай произошел в деле № 1-9/2014 [10]. Компания использовала данные из DLP-системы для выявления источника утечки клиентских баз. Однако в ходе судебного разбирательства выяснилось, что политика работы DLP-системы не была утверждена, а персонал не был ознакомлен с такими правилами. Суд указал на нарушение прав сотрудников и признал действия компании незаконными.

Отсутствие ЛНА приводит к значительным финансовым и репутационным потерям. Компании рискуют столкнуться не только с административными штрафами, но и с невозможностью защитить свои интересы в суде. Например, если сотрудник передает конфиденциальные данные конкурентам, но у компании нет перечня КТ и других необходимых документов, суды, как правило, отказываются рассматривать такие дела в пользу работодателя.

Ситуации с обработкой ПД добавляют еще больше сложностей. Например, сотрудники могут подать жалобу в Роскомнадзор на действия работодателя, что может привести к проверкам и штрафам. В случае нарушения режима обработки ПД размер штрафов может достигать 6 миллионов рублей (в соответствии с изменениями в КоАП РФ, введенными в 2021 году) [5].

В совокупности эти примеры демонстрируют критическую важность разработки ЛНА для юридической защиты компании. Прописанные и утвержденные регламенты позволяют минимизировать риски и обеспечивать защиту прав всех сторон, вовлеченных в процесс обработки данных.

Для разработки эффективных локальных нормативных актов (ЛНА) компаниям требуется интегрированный подход, учитывающий законодательные требования, специфику корпоративных процессов и современные вызовы в области информационной безопасности. ЛНА должны быть не просто документами, удовлетворяющими формальные требования проверяющих органов, но инструментами, помогающими предотвращать утечки данных и защищать интересы компании. Важно, чтобы такие акты могли быть легко внедрены в практическую деятельность и использованы в судебных спорах, если они возникнут.

Начальным этапом разработки ЛНА является проведение аудита процессов обработки и защиты данных. Это включает анализ текущих рабочих процессов, выявление всех точек взаимодействия сотрудников с данными и определение рисков. Например, если в компании регулярно используются общедоступные корпоративные мессенджеры, это повышает вероятность утечки данных, и политика их использования должна быть четко прописана в ЛНА.

Результаты аудита позволяют определить приоритеты и выбрать подходящие юридические и технические меры. Одновременно важно учитывать все законодательные требования, такие как Федеральный закон №152-ФЗ «О персональных данных», №98-ФЗ «О коммерческой тайне», а также положения Трудового кодекса РФ.

Для обеспечения эффективности и юридической обоснованности ЛНА рекомендуется включить следующие элементы:

#### 1. Общие положения

Этот раздел должен описывать цели и задачи ЛНА, область их применения и основные принципы. Например, цель акта может быть сформулирована как «обеспечение защиты конфиденциальной информации и соблюдение требований законодательства». Здесь же следует указать перечень регулируемых категорий данных, таких как персональные данные, коммерческая тайна или служебная информация.

#### 2. Классификация данных

Классификация — один из важнейших разделов ЛНА. Например, персональные данные можно подразделить на общие (имя, фамилия, должность) и специальные (данные о здоровье, биометрия), как это указано в ФЗ-152. Для коммерческой тайны необходимо составить подробный перечень информации, подлежащей защите, например, финансовые отчеты, клиентские базы, данные о стратегическом планировании. Это поможет избежать юридических сложностей в случае утечки данных.

#### 3. Порядок работы с данными

В этом разделе следует подробно описать правила обработки данных: кто имеет доступ к информации, какие действия с ней допускаются, как она передается внутри компании и за ее пределы. Например, политика может предусматривать запрет на использование личных устройств для хранения

данных компании.

#### 4. Использование DLP-систем

Для DLP-систем требуется отдельный регламент. В нем нужно описать, какие данные мониторятся, как осуществляется сбор и хранение информации, а также каким образом она используется. Например, при анализе электронной переписки сотрудники должны быть уведомлены, что их рабочие письма могут мониториться для предотвращения утечек.

#### 5. Реагирование на инциденты

Особое внимание стоит уделить разделу, посвященному действиям при выявлении утечки данных. ЛНА должны содержать алгоритм расследования инцидентов, включая этапы сбора доказательств, порядок взаимодействия с правоохранительными органами и возможные меры ответственности для сотрудников.

#### 6. Права и обязанности сотрудников

Важной частью документа является описание прав и обязанностей персонала. Например, сотрудники должны быть обязаны подписывать соглашение о неразглашении информации, если они работают с коммерческой тайной. Также важно разъяснить их права, например, право получать информацию о том, как их данные обрабатываются.

Для иллюстрации того, как ЛНА могут применяться на практике, рассмотрим несколько кейсов.

##### Мониторинг рабочих устройств

Компания «ТехноСофт» внедрила DLP-систему для мониторинга рабочих компьютеров [13]. ЛНА компании содержал четкие положения о том, какие данные анализируются (например, пересылаемые документы, адреса электронной почты) и в каких случаях информация может быть использована. Это позволило компании выявить утечку клиентской базы, а собранные данные были приняты судом в качестве доказательств, поскольку сотрудники были заранее уведомлены о мониторинге.

##### Классификация коммерческой тайны

Компания «АльфаФинанс» разработала перечень коммерческой тайны, включив в него финансовые отчеты, внутренние инструкции и данные клиентов [14]. ЛНА также предусматривал меры защиты, включая ограничение доступа и запрет на копирование таких данных на

внешние устройства. В результате, когда бывший сотрудник попытался передать конкурентам конфиденциальный отчет, компания смогла привлечь его к ответственности по статье 183 УК РФ.

Внедрение ЛНА требует не только утверждения документов, но и их интеграции в корпоративные процессы. Важным этапом является обучение сотрудников, которое может включать тренинги, семинары и регулярные проверки знаний. Например, компания может проводить ежегодные курсы по защите данных, объясняя, как сотрудники должны работать с коммерческой тайной и какие действия запрещены.

Еще одним важным шагом является регулярный пересмотр и актуализация ЛНА. Например, если компания внедряет новые технологии, такие как облачные хранилища или системы удаленного доступа, это должно быть отражено в ЛНА.

При разработке ЛНА компании также стоит учитывать требования надзорных органов, таких как Роскомнадзор. Например, если компания работает с персональными данными, она обязана уведомить Роскомнадзор о начале их обработки и соблюдать порядок их защиты. В случае внедрения новых технологий или изменений в политике обработки данных компания может проконсультироваться с юристами, чтобы избежать штрафов.

Грамотно составленные ЛНА имеют важное значение при рассмотрении споров в судах. Например, если компания предъявляет иск сотруднику за разглашение данных, суд потребует доказательства, что информация охранялась должным образом. ЛНА в таком случае становится ключевым доказательством. Примером служит дело №11-33789 [11], в котором суд принял сторону работодателя, поскольку компания представила ЛНА с перечнем КТ, а сотрудник подписал соглашение о неразглашении.

Исследование показало, что ЛНА играют ключевую роль в правовом обеспечении работы DLP-систем, защите ПДиКТ. Без четко прописанных внутренних регламентов компании сталкиваются с юридическими и организационными проблемами, включая невозможность квалификации утечек данных, риски привлечения к ответственности за нарушение прав работников и утрату возможности защиты информации в суде.

Одним из важнейших аспектов является классификация данных, которая создает основу для их правовой защиты. ЛНА должны включать перечень КТ, порядок работы с ПД и регламентировать использование DLP-систем. Грамотное документирование всех процессов позволяет минимизировать юридические риски, а также обеспечивать законность действий работодателя при мониторинге рабочих устройств и данных сотрудников.

Практические рекомендации по разработке ЛНА включают следующие этапы: аудит процессов обработки данных, разработку классификационных

критериев, установление процедур использования DLP-систем, а также обучение сотрудников. Грамотно составленные ЛНА не только помогают предотвращать утечки данных, но и выступают ключевым доказательством в судебных спорах.

Выводы подчеркивают необходимость интеграции ЛНА в корпоративные процессы, регулярного обновления документов и соответствия требованиям действующего законодательства. Компании, уделяющие внимание разработке и внедрению ЛНА, обеспечивают не только безопасность своей информации, но и юридическую устойчивость в условиях цифровизации.

### **Список литературы:**

[1] Кодекс Российской Федерации об административных правонарушениях. Принят Государственной Думой 30 декабря 2001 года, Федеральный закон №195-ФЗ от 30 декабря 2001 года (с изменениями и дополнениями). – М.: Проспект, 2024.

[2] Трудовой кодекс Российской Федерации. Принят Государственной Думой Федерального Собрания Российской Федерации 30 декабря 2001 года, Федеральный закон №197-ФЗ от 30 декабря 2001 года (с изменениями и дополнениями). – М.: Юрайт, 2024.

[3] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) «О персональных данных». Официальное издание. – М.: Юридическая книга, 2024.

[4] Федеральный закон № 98-ФЗ «О коммерческой тайне». Принят Государственной Думой Федерального Собрания Российской Федерации 29 июля 2004 года (с изменениями и дополнениями). – М.: Юриспруденция, 2024.

[5] Дело №12-790/2023 [Электронный ресурс] // Судакт: [сайт]. — URL: <https://sudact.ru/regular/doc/Wh8EcGPGEoZj/> (дата обращения: 09.12.2024).

[6] Дело № 4А-1189/2018 [Электронный ресурс] // Актофакт: [сайт]. — URL: <https://actofact.ru/case-59OS0000-4a-1189-2018-2018-08-03-1-3/> (дата обращения: 09.12.2024).

[7] Дело № 2-1809/2020 [Электронный ресурс] // Судакт: [сайт]. — URL: <https://sudact.ru/regular/doc/J5NOQBpFaoR/> (дата обращения: 09.12.2024).

[8] Дело № 2-3998/2020 [Электронный ресурс] // Судакт: [сайт]. — URL: <https://sudact.ru/regular/doc/eHsK0jW2rIV5/> (дата обращения: 09.12.2024).

[9] Дело № 33-2043/2021 [Электронный ресурс] // Актофакт: [сайт]. — URL: <https://actofact.ru/case-75OS0000-33-2043-2021-2021-06-01-0-1/> (дата обращения: 09.12.2024).

[10] Дело № 1-9/2014 [Электронный ресурс] // Актофакт: [сайт]. — URL: <https://actofact.ru/case-52RS0007-1-9-2014-1-160-2013-2013-04-18-2-0/> (дата обращения: 09.12.2024).

[11] Дело № 5-72/2021 [Электронный ресурс] // Судакт: [сайт]. — URL: <https://sudact.ru/vsrf/doc/RfVjv0eblMIW/> (дата обращения: 09.12.2024).

[12] Компания «АльфаФинанс». Перечень коммерческой тайны компании. Отчет аналитиков М.: АльфаФинанс, 2024.

[13] Мониторинг рабочих устройств. Внедрение DLP-системы для мониторинга рабочих компьютеров в компании «ТехноСофт». – М.: ТехноСофт, 2024.

[14] Компания «АльфаФинанс». Перечень коммерческой тайны компании. Внутренние инструкции. – М.: АльфаФинанс, 2024

### **Spisok literatury:**

[1] Kodeks Rossijskoj Federacii ob administrativny'x pravonarusheniyax. Prinyat Gosudarstvennoj

*Dumoj 30 dekabrya 2001 goda, Federal'nyj zakon №195-FZ ot 30 dekabrya 2001 goda (s izmeneniyami i dopolneniyami).* – M.: Prospekt, 2024.

[2] *Trudovoj kodeks Rossijskoj Federacii. Prinyat Gosudarstvennoj Dumoj Federal'nogo Sobraniya Rossijskoj Federacii 30 dekabrya 2001 goda, Federal'nyj zakon №197-FZ ot 30 dekabrya 2001 goda (s izmeneniyami i dopolneniyami).* – M.: Yurajt, 2024.

[3] *Federal'nyj zakon ot 27.07.2006 № 152-FZ (red. ot 08.08.2024) “O personal'nyx dannyx”.* Oficial'noe izdanie. – M.: Yuridicheskaya kniga, 2024.

[4] *Federal'nyj zakon № 98-FZ “O kommercheskoj tajne”. Prinyat Gosudarstvennoj Dumoj Federal'nogo Sobraniya Rossijskoj Federacii 29 iyulya 2004 goda (s izmeneniyami i dopolneniyami).* – M.: Yurisprudenciya, 2024.

[5] *Delo №12-790/2023 [E'lektronnyj resurs] // Sudakt: [sajt].* — URL: <https://sudact.ru/regular/doc/Wh8EcGPGEoZj/> (data obrashheniya: 09.12.2024).

[6] *Delo № 4A-1189/2018 [E'lektronnyj resurs] // Aktofact: [sajt].* — URL: <https://actofact.ru/case-59OS0000-4a-1189-2018-2018-08-03-1-3/> (data obrashheniya: 09.12.2024).

[7] *Delo № 2-1809/2020 [E'lektronnyj resurs] // Sudakt: [sajt].* — URL: <https://sudact.ru/regular/doc/J5NOQB6pFaoR/> (data obrashheniya: 09.12.2024).

[8] *Delo № 2-3998/2020 [E'lektronnyj resurs] // Sudakt: [sajt].* — URL: <https://sudact.ru/regular/doc/eHsK0jW2rIV5/> (data obrashheniya: 09.12.2024).

[9] *Delo № 33-2043/2021 [E'lektronnyj resurs] // Aktofact: [sajt].* — URL: <https://actofact.ru/case-75OS0000-33-2043-2021-2021-06-01-0-1/> (data obrashheniya: 09.12.2024).

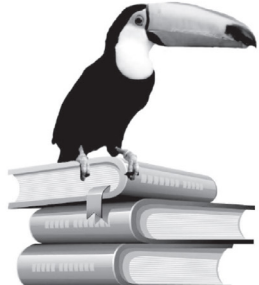
[10] *Delo № 1-9/2014 [E'lektronnyj resurs] // Aktofact: [sajt].* — URL: <https://actofact.ru/case-52RS0007-1-9-2014-1-160-2013-2013-04-18-2-0/> (data obrashheniya: 09.12.2024).

[11] *Delo № 5-72/2021 [E'lektronnyj resurs] // Sudakt: [sajt].* — URL: <https://sudact.ru/vsrf/doc/RfVjv0eblMIW/> (data obrashheniya: 09.12.2024).

[12] *Kompaniya “Al'faFinans”. Perechen' kommercheskoj tajny kompanii. Otchet analitikov M.: Al'faFinans, 2024.*

[13] *Monitoring rabochix ustrojstv. Vnedrenie DLP-sistemy dlya monitoringa rabochix komp'yutero v kompanii “TexnoSoft”. – M.: TexnoSoft, 2024.*

[14] *Kompaniya “Al'faFinans”. Perechen' kommercheskoj tajny kompanii. Vnutrennie instrukcii. – M.: Al'faFinans, 2024*



**ЮРКОМПАНИ**  
[www.law-books.ru](http://www.law-books.ru)

Юридическое издательство  
**«ЮРКОМПАНИ»**

Издание учебников,  
учебных и методических  
пособий, монографий,  
научных статей.

Профессионально.

В максимально  
короткие сроки.

Размещаем  
в РИНЦ, E-Library.