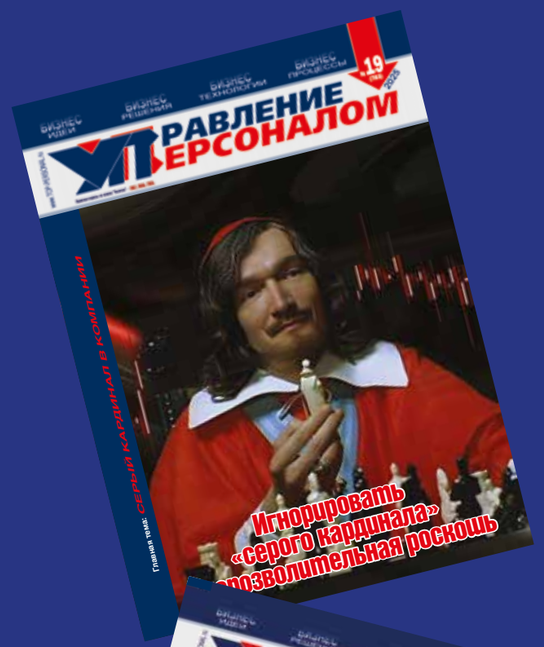
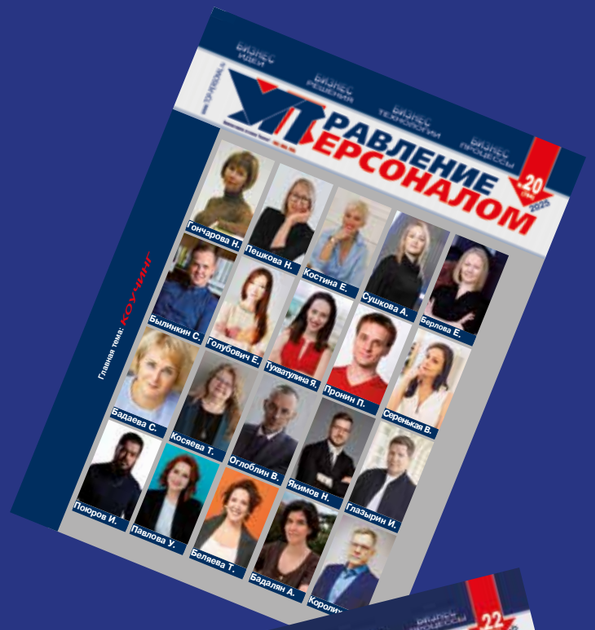
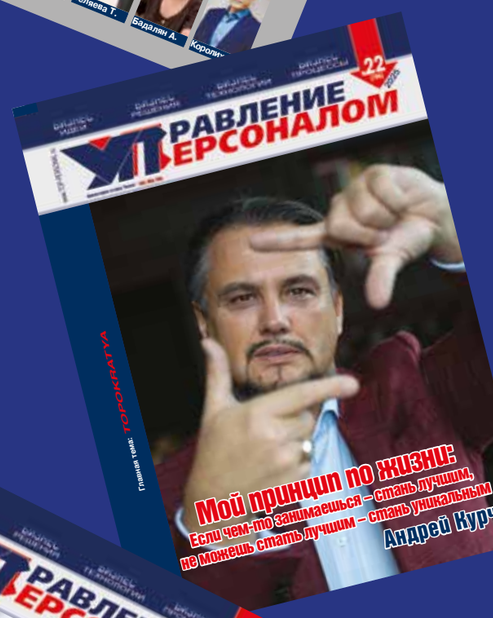






WWW.TOP-PERSONAL.RU

ИНФОРМАЦИОННО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

ЕЖЕКВАРТАЛЬНЫЙ ЖУРНАЛ

ДЕЛОПРОИЗВОДСТВО

www.TOP-PERSONAL.RU

(июль-сентябрь)

№3
2025

В номере:

При поддержке:

УПРАВЛЕНИЕ ПЕРСОНАЛОМ

Издательский дом

представляет ведущие деловые журналы

Подписные индексы: По объединённому каталогу ГК РФ

СОДЕРЖАНИЕ

Главный редактор журнала
Гончаров Александр
Зам. гл. редактора журнала
Орленко Василий
Редакционная коллегия:
Ремизов Алексей, Лохман Екатерина, Тюминкина Лариса, Ситдикова Татьяна, Шумейко Дмитрий, Журавлева Алеся, Шестаков Глеб, Ордынская Ирина, Красильников Сергей, Келин Дмитрий, Кузнецова Анна, Агаева Екатерина, Никулина Светлана, Фёдоров Максим, Белоусова Наталья, Сергеева Ольга, Митрахович Алла, Кочанова Татьяна
Дизайн/вёрстка:
Дегнер Оксана
Корректор:
Кочетков Павел
Прямая подписка:
7447273@bk.ru
Реклама: 89258817901 вацап
Гл. редактор
ИД «Управление персоналом»
Гончаров А. Н.

Подписные индексы:
по каталогу агентства «Роспечать» — 29659 (на полугодие).

Учредитель: ООО «Журнал «Управление персоналом».
Регистрационное свидетельство ПИ № 77415415.
Выдано Комитетом Российской Федерации по печати.
Издательство не несет ответственности за ущерб, нанесенный в результате использования, неиспользования или ненадлежащего использования информации, содержащейся в настоящем издании.
Перепечатка материалов (полная или частичная) допускается только с письменного разрешения редакции.
Издатель: ООО «Топ-Персонал» с 2011 г.

© «Делопроизводство», 2025.
Подписано в печать 20.08.2025.
Формат 60x90 1/8.
Печать офсетная.
Бумага офс. № 1. Печ. л. 13.
Тираж 10 000. Заказ

9 785870 573724

Колонка редактора

Главная тема номера — Аудиовизуальные документы

Получите в подарок новые журналы:

Коммерческие споры

№ 1-3

Мастер Продаж

№ 1-4

ПРАКТИЧЕСКИЙ ДЕЛОВОЙ ЖУРНАЛ
IT РЕВЬЮ
ОБЗОРЫ·КОММЕНТАРИИ·ПРАКТИКА №1/2025

№ 1-2

СТАРТАПЫ & ИДЕИ ДЛЯ БИЗНЕСА

№ 1

Ждём заявки на 7447273@bk.ru
Вацап 89263501881

Национальный мессенджер и обработка персональных данных. Чего ждать?

Татьяна Кочанова, юрист

24 июня президент России Владимир Путин подписал закон о многофункциональном сервисе обмена информацией и изменениях в законодательство о персональных данных. Но применяться Основные правила о российском многофункциональном сервисе обмена информацией будут не сразу.

С 1 сентября 2025 года согласие на обработку персональных данных нужно всегда оформлять отдельным документом — нельзя будет включать его в состав других договоров или соглашений, которые подписывает гражданин. Изменение направлено на обеспечение осознанного согласия субъектов предоставить личную информацию и исключение ситуаций, когда такое согласие дается автоматически.

Часто «скрытые» формулировки разрешают использовать данные не только для основной услуги, но и для маркетинга, аналитики и других целей. Пользователи либо вообще не подозревают о них, либо вынуждены подписывать документ целиком, не имея возможности отказаться.

Еще в 2022 году в законодательство о защите прав потребителей внесли изменения, запрещающие отказывать в заключении договора из-за нежелания клиента предоставлять персональные данные. Однако эти поправки оказались недостаточно эффективными — они не охватывают все случаи «скрытых» согласий, поскольку не распространяются, например, на сферу предоставления цифрового контента.

Закон сохраняет возможность обработки персональных данных без согласия, если для этого есть другие законные основания. Например, когда она необходима для заключения или исполнения договора (пункт 5 части 1 статьи 6 Закона о персональных данных). Однако если данные используются шире, оператору придется получать отдельное согласие — включать такие условия в сам договор будет запрещено.

Рекомендация операторам

Новые правила призваны лучше защищать права граждан. В то же время многим компаниям предстоит актуализировать существующий документооборот и адаптировать внутренние процессы к этим изменениям.

Необходимо пересмотреть стандартные документы — пользовательские соглашения, оферты, договоры с клиентами — и убрать из них положения о согласии на обработку персональных данных.

Если обработка данных предполагает цели, выходящие за рамки исполнения договора (например, маркетинг или аналитика), потребуется разработать отдельную процедуру получения такого согласия.

Национальный мессенджер: вызовы и риски

Законопроект также предусматривает разработку так называемого национального мессенджера. Российской компанией, определенной правительством, будет создано приложение с широким функционалом, а именно:

- подтверждение личности без бумажных документов при помощи цифрового ID;
- совершение сделок в цифровой форме с использованием УКЭП и УНЭП;
- интеграция с Госуслугами;
- обмен мгновенными сообщениями (мессенджер);
- организация взаимодействия между участниками образовательных отношений (школьные чаты).

Предполагается также, что в будущем приложение будет интегрировано с ведущими российскими цифровыми платформами и содержать функционал социальных сетей — поддержку каналов и чат-ботов, возможность совершения звонков. Конкретные механизмы работы мессенджера планируется представить этим летом.

Инициатива направлена на создание отечественного аналога иностранным социальным сетям и защиту граждан от мошенничества. В то же время, сосредоточение такого большого объема данных в одной информационной системе повышает риски утечек и создает новые возможности для злоупотреблений.

Другой значимый вопрос — будет ли использование приложения обязательным? В настоящий момент речь идет исключительно о добровольной регистрации. Вместе с тем, не исключено, что со временем некоторые сервисы могут полностью перейти на отечественную платформу.

В любом случае, последствия данной инициативы пока сложно объективно оценить — во многом они будут зависеть от уровня защищенности приложении, а также от развития правового поля, регулирующего использование мессенджера и его аналогов.

Правительство определило национальный мессенджер, а Минцифры перечислило его основные функции, изложив их в Распоряжении Правительства РФ от 12.07.2025 N 1880-р,

Российский многофункциональный сервис обмена информацией будет работать на базе «Цифровой платформы MAX». Распоряжение об этом размещено на сайте правительства 15 июля 2025 года.

По данным Минцифры, на платформе уже доступны, например:

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

енные чаты поддержки также несут риск. Когда пользователь кликает и отправляет сообщение, его персональные данные (например, номер телефона, аккаунт) уходят на серверы WhatsApp или Telegram за рубежом. По закону это квалифицируется как трансграничная передача данных. Meta1 (владелец WhatsApp, Facebook1, Instagram1) и другие иностранные компании из «недружественных» стран сейчас фактически вне российской юрисдикции, их сервисы не подчиняются нашим законам о данных. Использование их инструментов на сайте приравнивается к вывозу данных клиентов за границу.

Иностранные SaaS и облака. Если ваш сайт интегрирован с CRM-системой, почтовым сервисом (например, Gmail, Mailchimp) или другими облачными платформами, стоит проверить, где хранятся данные. Если серверы находятся не в РФ, требуется специальное уведомление в Роскомнадзор, иначе компания нарушает порядок трансграничной передачи. Часть

ПОДАРОК!!!

Пришлите заявку на вацап 89263501881

Вместе с журналом «Делопроизводство» вы можете получать в подарок другие бизнес-издания Издательства: «Управление персоналом», «Мастер продаж», «Трудовое право», «Жилищное право», «Коммерческие споры», «Секретарское дело», «Клуб главных бухгалтеров», «Айти ревью», «Альманах» и пр.

Персональные данные в кадрах: что и кому можно обрабатывать, а что грозит миллионными штрафами

Максим Лагутин, эксперт по защите персональных данных, основатель компании Б-152

30 мая 2025 года вступили в силу поправки по ответственности за нарушения требований по персональным данным. Появились новые составы правонарушений, увеличились штрафы за уже существующие нарушения. Теперь игнорирование 152-ФЗ может обернуться для компании крупными штрафами, вплоть до оборотных за утечки персональных данных.

Что можно и нельзя делать в рамках обработки персональных данных в кадровой сфере, объяснил Максим Лагутин, эксперт по защите персональных данных, основатель компании Б-152.

Виды персональных данных

Базовые персональные данные сотрудника — это информация о гражданине, необходимая для оформления и ведения трудовых отношений. Они делятся на несколько категорий.

- Идентификационные данные: ФИО, дата рождения, паспортные сведения.
- Контактная информация: адрес проживания, телефон, e-mail.
- Профессиональные сведения: образование, квалификация, трудовой стаж.
- Финансовые реквизиты: ИНН, СНИЛС, банковские данные для зарплатных выплат.

Специальные категории персональных данных — это информация о сотруднике, которая

требует особой защиты. Это расовая и национальная принадлежность, политические и религиозные взгляды, состояние здоровья, интимная жизнь. Обработка этих сведений возможна только при наличии особых условий, среди них — требования законодательства, осуществление правосудия, оказание медицинских услуг и т. д. Полный их перечень указан в ч. 2 ст. 10 152-ФЗ.

Например, сведения о здоровье правомерно обрабатывать, если работодатель проводить обязательные медицинские осмотры для определенных категорий работников или обеспечивает специальные условия труда для сотрудников с ограниченными возможностями. Особое место занимает вопрос сбора справок о судимости работников. Если это прямо не предусмотрено отраслевым законодательством, то запрашивать такие сведения от работников строго запрещено (ч. 3 ст. 10 152-ФЗ). У компаний, незаконно обрабатывающих сведения о судимости работников, появляется риск ответственности за обработку сведений вне предусмотренных законом случаев по ч. 2 ст. 13.11 КоАП РФ. Кроме того, в случае, если произойдет утечка таких данных, то компании может прийти штраф от 10 до 15 миллионов рублей по ч. 16 ст. 13.11 КоАП РФ. После достижения целей обработки такие данные подлежат уничтожению или обезличиванию.

Биометрические данные — это уникальные физиологические или биологические характеристики человека, используемые для установления его личности. Так, фотография нужна для пропуска или распознавания лица при видеонаблюдении, а отпечатки пальцев для работы в СКУД.

За незаконную обработку биометрии предусмотрены штрафы в соответствии со ст. 13.11 КоАП РФ. Но и здесь есть нюансы. Ключевым условием определения биометрических персональных данных является цель — установление личности. Например, фотография в личном деле не является биометрией. Но то же фото становится биометрией, если используется в системе распознавания лиц для пропускного режима или для верификации личности при электронном документообороте.

Согласия всегда нужны или можно обойтись без них?

Согласие работника не нужно, если обработка ПДн осуществляется для исполнения трудового законодательства и, в частности, трудового договора. Так, например, работодателям не требуются согласия для оформления сотрудника в штат, ведения внутреннего документооборота, обеспечения безопасности на рабочем месте и сохранности имущества компании, проведения обучений, связанных с охраной труда и т. д. Также нужна информация о сотруднике для оформления отпусков, больничных, командировок, медосмотров и допускам к работе. Кроме того, на работодателя возлагается ответственность по подаче различной отчетности по своим работникам в государственные органы — ФНС, СФР, Военкомат, МВД, отраслевые ведомства. Для исполнения данных обязанностей получение согласия также не требуется.

ЕСЛИ В КОМПАНИИ ВЕДЕТСЯ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ (КЭДО), СОГЛАСИЯ ДОПУСТИМО ПОДПИСЫВАТЬ ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Когда согласие обязательно

Биометрические персональные данные,

а также специальные категории ПДн можно собирать только с согласия гражданина в письменной форме.

Аналогично согласие в письменной форме нужно получить от работника, если любые сведения о нем передаются третьим лицам вне обязательств, предусмотренных законодательством — например, банковским, страховым организациям, а также подрядчикам для проведения корпоративов и тимбилдингов.

Нужно согласие, если используете персональные данные в маркетинговых целях. Например, когда сотрудники участвуют в опросах или маркетинговых исследованиях.

Формы согласий на обработку персональных для разных целей

Закон не предусматривает унифицированных бланков для согласий в письменной форме на обработку персональных данных, но устанавливает строгие требования к их содержанию. В документе обязательно должно быть отражено 8 пунктов:

- Сведения о субъекте ПДн,
- Данные оператора,
- Цели обработки,
- Перечень обрабатываемых данных,
- Сведения об обработчике (при наличии),
- Действия, способы обработки,
- Срок действия согласия и способ его отзыва,
- Подпись субъекта.

Это означает, что организации вправе самостоятельно разрабатывать формы таких согласий, но с учетом перечисленных условий.

КОПИИ ПАСПОРТОВ, СНИЛС, ИНН И ДРУГИХ ЛИЧНЫХ ДОКУМЕНТОВ РАБОТНИКОВ НУЖНО УНИЧТОЖАТЬ ПОСЛЕ ДОСТИЖЕНИЯ ЦЕЛИ, НАПРИМЕР, ПОСЛЕ ОФОРМЛЕНИЯ ТРУДОВОГО ДОГОВОРА

Важно отметить, что Роскомнадзор в отношении согласий в письменной форме придерживается позиции «одна цель — одно согласие». Это значит, что будет нарушением перечисление всех целей обработки и всех третьих лиц в одном согласии.

При публикации ПДн в открытых источниках, в том числе на сайте компании, а равно при передаче неопределенному кругу лиц действуют особые правила получения согласия, в соответствии с ч. 1 ст. 10.1 152-ФЗ и Приказом РКН №18 от 24.02.2021. Кроме стандартных пунктов необходимо добавить выбор, какие данные гражданин использовать разрешает, запрещает или разрешает с условиями, а также эти условия перечислить. В течение 3 рабочих дней оператор должен опубликовать условия обработки на своём сайте.

В отношении иных целей обработки допускается получение простого общего согласия от работника.

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Работа с аудиовизуальными документами в организации: правовые и практические аспекты

Светлана Никулина, юрист

С развитием цифровых технологий все большее число организаций использует аудио- и видеозаписи не только как инструмент коммуникации, но и как деловые документы. Аудиовизуальные документы находят применение в обучении сотрудников, проведении совещаний, фиксации переговоров, доказывании позиций в суде и других сферах. Однако их использование связано с рядом юридических и организационных особенностей, требующих внимательного подхода.

Понятие и виды аудиовизуальных документов

Аудиовизуальные произведения представляют собой серию последовательно сменяющих друг друга изображений, связанных между собой. Они могут сопровождаться звуком или быть без него (ст. 1263 Гражданского кодекса РФ (далее — ГК РФ). К аудиовизуальным произведениям относятся фильмы, видеоролики, презентации с видеофрагментами и другие виды визуального повествования.

В контексте деловой практики аудиовизуальные документы — это не только объекты авторского права, но и **непрофессиональные записи**, которые создаются внутри компании для внутреннего использования или для

передачи третьим лицам. Эти записи могут включать в себя:

- Записи встреч, совещаний и переговоров.
- Обучающие и инструктажные видеоматериалы.
- Документальные подтверждения выполненных работ или действий.
- Видеозаписи происшествий, инцидентов и других событий.

Отличительной чертой таких документов является то, что они могут быть юридически значимыми, если **соответствуют требованиям законодательства и оформлены надлежащим образом**.

ПРИМЕР 1. Для того чтобы зафиксировать факт присутствия участников ООО на собрании и принятые на нём решения, общество может использовать видеозапись. Однако сначала необходимо закрепить такой порядок в уставе или принять единогласное решение на собрании. Решение участников о фиксации решений в виде видеозаписи должно быть заверено нотариально (подп. 3 п. 3 ст. 67.1 ГК РФ, п. 2 Обзора судебной практики по некоторым вопросам применения законодательства о хозяйственных обществах, утв. Президиумом Верховного суда РФ от 25.12.2019).

ПРИМЕР 2. В соответствии с Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (далее — Закон № Закона № 323-ФЗ), медицинские организации могут вести аудио- и видеозаписи в лечебных кабинетах. Это позволяет обеспечить гражданам доступ к качественной и полноценной медицинской помощи, не нарушая при этом их конституционные права. Медицинские организации могут предоставлять эти данные контролирующим органам без согласия пациента, в том числе для целей внутреннего контроля (п. 10 ч. 4 ст. 13 Закона № 323-ФЗ).

Объекты авторского права — произведения науки, литературы и искусства независимо от достоинств и назначения произведения, а также от способа его выражения. Например, литературные произведения, драматические и музыкально-драматические произведения, сценарные произведения, хореографические произведения и пантомимы, и другие (ст. 1259 ГК РФ).

Объекты авторского права защищены с момента их создания, и автор имеет исключительные права на использование своего произведения, включая право на воспроизведение, распространение, публичное исполнение и адаптацию.

Оформление аудиовизуальных документов

Рассмотрим требования к оформлению аудиовизуальных документов.

Требование 1. Согласие участников. Особенно важно при записи переговоров, совещаний, интервью. В случае отказа одного из участников запись может быть признана недопустимым доказательством.

Если запись содержит изображение или голос конкретного лица, необходимо, по общему правилу получить согласие на обработку персональных данных (ст. 86 Трудового кодекса РФ, ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных») и предусмотреть возможность отзыва согласия.

Чтобы избежать необходимости получать согласие на аудио или видеозапись, необходимо выполнить четыре условия:

1. Видеозапись ведётся только для определенных и заранее установленных законных целей, связанных с выполнением сотрудниками своих обязанностей.
2. Сотрудники осведомлены о том, что ведется видеозапись.
3. Информация о видеозаписи включена в трудовой договор или локальные нормативные акты, с которыми сотрудники ознакомлены под подпись.
4. Запись ведется открыто.

Видеозаписи, снятые в общественных местах и на охраняемых территориях, не считаются персональными данными до тех пор, пока они не будут использованы для идентификации конкретного человека.

Требование 2. Наличие метаданных (дата, время, место, список участников, цели создания документа). Метаданные — это информация, которая описывает другие данные. Вот как могут выглядеть метаданные для аудиовизуального документа:

- Дата создания записи: например, 2025-07-01.
- Время начала записи: например, 14:30.
- Место: геолокация, где была сделана запись (например, «Москва, Парк Горького»). Это может быть указано в виде координат (широта и долгота) или текстового описания.
- Список участников: имена или идентификаторы людей, участвующих в записи: например, «Иван Иванов, Мария Петрова, Алексей Сидоров».
- Цели создания документа: описание причины записи: например, «Интервью для уточнения концепции», «Запись инструктажа по охране труда», «Годовое собрание акционеров».

Перечисленные метаданные рекомендуют фиксировать при создании аудиовизуальных документов. Метаданные можно извлечь с помощью различных программ и инструментов.

Требование 3. Техническое качество. Запись должна быть четкой, без помех и искажений. Качество записи должно быть высоким. Непрерывность записи: запись должна быть непрерывной и полной, чтобы не потерять важные моменты. Условия съемки: запись не должна проводиться в темноте или против света. Качество оборудования: используемое записывающее устройство должно обеспечивать высокие качественные характеристики для получения четкой аудиодорожки и изображения лиц участников.

Частые ошибки организации при создании аудиовизуальных документов

1. Использование записи без согласия участников.

2. Отсутствие метаданных или идентификации участников.

3. Нечеткая запись, что может сделать ее недоказательной.

Аудиовизуальные документы как доказательства в суде

В ходе судебного разбирательства иногда используются аудио- и видеозаписи, содержащие сведения о рассматриваемом деле. Эти доказательства объединяет необходимость применения специальных технических устройств для воспроизведения информации. С помощью таких устройств можно прослушать аудиозаписи и просмотреть видеозаписи.

Лицу, которое предоставляет суду аудио- или видеозапись, необходимо предоставить информацию о том, когда, кем и при каких обстоятельствах была сделана запись (ст. 77 ГПК РФ). Без этих сведений суд не примет аудио- или видеозапись в качестве доказательства.

Данную информацию, как правило, указывают в ходатайстве о приобщении документа к материалам дела. В ходатайстве также рекомендуется обосновать, во-первых, какие юридически значимые факты подтверждает аудиовизуальный документ, во-вторых, почему эти обстоятельства невозможно или сложно установить с помощью других средств доказывания, в-третьих, на какое устройство была сделана запись, в-четвертых, кто фигурирует на записи.

Также важно предоставить суду расшиф-

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Конфиденциальность данных — тоже головная боль

Алексей Оносов,
эксперт-журналист
Телеграм @alexey_on

Аудиодокументы окружают нас повсюду в рабочих процессах. Интервью с кандидатами, планерки, обучающие сессии — всё записывается и потом лежит мертвым грузом. Искать что-то конкретное в часах записей… это просто кошмар. Может быть такое, что приходится восстанавливать детали переговоров трёхмесячной давности и перематывать два часа аудио, чтобы найти одну фразу! Текстовый формат гораздо практичнее для поиска и анализа, но как превратить звук в читаемый текст?

Ручная расшифровка — это настоящая пытка. Час записи съедает 4–6 часов рабочего времени, а то и больше. Сидишь, перематываешь туда-сюда, вслушиваешься в неразборчивое бормотание участников. К середине процесса мозг уже отключается, пропускаешь важные моменты. Человеческий фактор никуда не денешь — ошибки восприятия, усталость, банальная невнимательность. А в итоге получается каша из неструктурированного текста, где найти что-то конкретное почти невозможно. И самое обидное — через неделю сам автор расшифровки не помнит, о чём там вообще речь.

Конфиденциальность данных — тоже головная боль.

Передавать записи переговоров или интервью сторонним расшифровщикам… мягко говоря, рискованно. Мало ли что там обсуждалось. Профессиональные транскрибаторы берут приличные деньги за свои услуги,

но даже это не гарантирует ни качества, ни скорости. Проверено на собственном опыте — лучше автоматизировать то, что можно автоматизировать.

Автоматизированные решения на базе искусственного интеллекта значительно ускоряют процесс транскрибации. Но тут есть свои подводные камни, и какие! Качество звука — главный враг любой автоматики. Фоновый шум, акценты, региональные диалекты превращают даже продвинутые алгоритмы в беспомощных младенцев. А многоканальные записи, где несколько человек говорят одновременно, вообще ставят систему в тупик.

Групповые интервью или совещания с перекрывающейся речью требуют дополнительной обработки, иначе получается винегрет из слов.

Не все сервисы гарантируют защиту данных на должном уровне. Некоторые передают файлы на серверы в других странах, что создает дополнительные риски. При выборе решения для транскрибации стоит обращать внимание на несколько критериев. Скорость обработки особенно важна для срочных задач — отчеты по собеседованиям нужны быстро, пока впечатления свежи. Поддержка различных форматов тоже критична, не все системы работают с видеофайлами или специфическими аудиоформатами. Возможность качественной обработки сложных записей отделяет серьёзные решения от игрушек.

А безопасность данных — это вообще отдельная тема для размышлений. Шифрование, соглашения о неразглашении, локальное хранение файлов должны быть обязательными условиями. Для решения этого вопроса мы разработали сервис по транскрибации — «Транскрибум» — там реализован гибкий подход. Автоматическая расшифровка плюс ручная доработка для идеального результата. Скорость обработки до 100 и более раз быстрее ручной работы при точности до 99%.

ГРУППОВЫЕ ИНТЕРВЬЮ ИЛИ СОВЕЩАНИЯ С ПЕРЕКРЫВАЮЩЕЙСЯ РЕЧЬЮ ТРЕБУЮТ ДОПОЛНИТЕЛЬНОЙ ОБРАБОТКИ, ИНАЧЕ ПОЛУЧАЕТСЯ ВИНЕГРЕТ ИЗ СЛОВ

Файлы не передаются третьим лицам, что решает проблему конфиденциальности. Система справляется даже со сложными аудио — шумы, акценты, технические термины обрабатываются корректно. Синхронизация с тайм-кодами удобна для анализа интервью, можно сразу перейти к нужному моменту. Готовые форматы экспорта в Word, PDF, даже субтитры для видео… Для корпоративных систем предусмотрена интеграция через программный интерфейс.

В практике управления персоналом транскрибация решает множество задач.

Собеседования становятся гораздо эффективнее — можно быстро найти ключевые фразы кандидата через поиск по

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Цифровизация породила изощренные способы кражи интеллектуальной собственности, которые сложно квалифицировать в рамках традиционного права

Макс Лоумен,
эксперт по юридической стратегии бизнеса

Последние пять лет кардинально изменили ландшафт споров по интеллектуальной собственности в российских судах. ***Если раньше типичными делами были иски о продаже контрафактных кроссовок или пиратских дисков, то сегодня в арбитражных судах рассматриваются споры на сотни миллионов рублей за украденные алгоритмы, промышленные образцы и коммерческие тайны.***

Современные нарушители действуют изощренно, используют правовые пробелы и международную юрисдикцию для легализации присвоенных технологий. Меняются не только масштабы ущерба, но и сами методы краж.

Коммерческая тайна как объект краж: новые реалии

Структура нарушений кардинально изменилась за последние годы. Производственные и технические сведения, включая уникальные технологии, рецептуры, методы производства, чертежи, спецификации, а также результаты

НИОКР, выходят на первое место по количеству исков и размеру компенсаций. Причина понятна — один алгоритм может стоить миллионы, а доказать факт копирования кода крайне сложно. Особенно уязвимы сведения о клиентской базе, поставщиках, контрагентах и партнерах: списки клиентов, условия заключенных сделок, объемы отгрузок, стоимость единицы продукции и деловая переписка. Украсть такую информацию проще, чем защитить права в суде.

Экономические и финансовые сведения также стали мишенью: данные о ценообразовании, системах скидок, финансовые модели, бюджеты, планы инвестиций, а также информация о внешнем и внутреннем финансировании. Эти данные позволяют конкурентам получить критические преимущества в ценовой политике и финансовом планировании.

Почему компании проигрывают в судах

Суды все более строго подходят к оценке того, насколько полно и правильно компания выполнила все требования законодательства по установлению и поддержанию режима конфиденциальности.

Анализ судебных решений выявляет критические ошибки компаний:

✔ Отсутствие правильного режима защиты.

Наиболее частая причина — суды указывают на то, что компания не предоставила достаточных доказательств введения режима коммерческой тайны и мер по ее защите.

Например, не был утвержден перечень конфиденциальных данных, сотрудники не были ознакомлены с ним под роспись.

✔ Формальные нарушения в документообороте.

Судебные решения подтверждают, что простого получения обязательства о неразглашении от сотрудника недостаточно для установления режима коммерческой тайны.

Необходима комплексная система защиты.

✔ Невозможность доказать ущерб.

Если компания не может доказать, что утечка информации привела к конкретным убыткам или что снижение доходов напрямую связано с действиями бывшего сотрудника, иск может быть отклонен.

✔ Нарушение процедур.

Суды также могут отказать работодателю, если были нарушены установленные сроки для применения дисциплинарных мер или другие процедурные требования.

ОСОБЕННО УЯЗВИМЫ СВЕДЕНИЯ О КЛИЕНТСКОЙ БАЗЕ, ПОСТАВЩИКАХ, КОНТРАГЕНТАХ И ПАРТНЕРАХ

Новые схемы присвоения

Цифровизация породила изощренные способы кражи интеллектуальной собственности, которые сложно квалифицировать в рамках традиционного права.

Реверс-инжиниринг как прикрытие стал классическим приемом. Компания официально нанимает экспертов для «независимого анализа» чужого продукта, а затем создает «собственное» решение, воспроизводящее ключевые функции оригинала. Формально никто ничего не копирует, на практике получается точная копия с минимальными косметическими изменениями.

Корпоративный шпионаж через кадровые перестановки стал обыденностью в высокотехнологичных отраслях. Компании целенаправленно переманивают ключевых специалистов конкурентов, получая вместе с ними доступ к организационным сведениям: внутренним бизнес-процессам, управленческой отчетности, протоколам совещаний, а также особенностям осуществления профессиональной деятельности.

Использование правовых пробелов. Нарушители эксплуатируют тот факт, что перечень сведений, которые могут быть признаны коммерческой тайной, не является исчерпывающим и определяется каждой организацией самостоятельно. Если компания неточно определила границы своей коммерческой тайны, защитить ее становится невозможно.

Что должны доказать пострадавшие

Для успешной защиты коммерческой тайны в суде необходимо доказать четыре основных факта:

Во-первых, что информация действительно была тайной. Истец должен убедительно продемонстрировать, что разглашенная информация соответствовала всем признакам коммерческой тайны на момент инцидента.

Во-вторых, что режим соблюдался. Суду необходимо представить доказательства того, что компания фактически ввела и поддерживала режим коммерческой тайны. Сюда входят утвержденные перечни, приказы, журналы учета, соглашения о неразглашении, наличие грифа «Коммерческая тайна» на материальных носителях информации с указанием обладателя.

НАИБОЛЕЕ ЧАСТАЯ ПРИЧИНА — СУДЫ УКАЗЫВАЮТ НА ТО, ЧТО КОМПАНИЯ НЕ ПРЕДОСТАВИЛА ДОСТАТОЧНЫХ ДОКАЗАТЕЛЬСТВ ВВЕДЕНИЯ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ И МЕР ПО ЕЕ ЗАЩИТЕ

В-третьих, что нарушение совершил конкретный человек. Необходимо установить лицо, ответственное за разглашение. Здесь помогают записи камер видеонаблюдения, логи доступа к информационным системам, обнаруженные документы.

В-четвертых, что компания понесла убытки. Для взыскания убытков истец должен доказать факт их понесения, их размер, наличие противоправных действий ответчика и причинную связь между этими действиями и наступившими неблагоприятными последствиями.

Практические проблемы доказывания

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

ДЕЛОВОЙ КЛУБ «КАПИТАНЫ РОССИЙСКОГО БИЗНЕСА» /ИЮНЬ УП 20/2025

Коучинг: новый этап в России.

Обзор дискуссии на деловом клубе «Капитаны российского бизнеса»

Надежда Гончарова

Коучинг развивается и востребован в России как философия/подход в работе с людьми и как профессия. Такой вывод у меня сложился в результате дискуссии на деловом клубе «Капитаны российского бизнеса». Встреча клуба была посвящена теме «Коучинг: новый этап в России». На мой взгляд, участники с разных сторон раскрыли тему и подсветили много интересных моментов для бизнеса, которые касаются коучинга и коучингового рынка. В клубе участвовали очень разные эксперты: это, конечно, коучи – маститые, с большим числом часов практики и молодые, а также супервизоры, менторы, заказчики коучинга, провайдеры услуг, представители одной из российских ассоциаций и другие участники рынка, которые так или иначе соприкасаются с коучингом. Если обобщить многообразие мнений и высказываний, выходят следующие важные моменты:

— уход ICF с российского рынка не оказал сильного влияния на коучинговый рынок. По-прежнему коучи оказывают услуги, работая как по международным стандартам, так и по российским; есть заказчики, есть провайдеры;

— коучинг как профессия в России, оказывается, тоже есть. Работает специальная комиссия на федеральном уровне. Процесс идет. Правда, по этому пункту осталось много вопросов;

— коучинг применяется эффективно не только в бизнес-структурах, но и государственных;

— эксперты применяют мультиформатный подход в работе с человеком или с командой, куда входит и коучинг.

*Надежда Гончарова, ведущая делового клуба «Капитаны российского бизнеса», директор по развитию ИД «Управление персоналом», бизнес-коуч, супервизор

Эксперты клуба делятся опытом:

Наталья Пешкова

— Из своего опыта могу сказать, что за последние два-три года коучинг набирает большие обороты, популярность его растет. По моему опыту, девяносто процентов клиентов — это бизнесмены. Заметила, меняется возраст клиентов.

Если раньше в основном люди 30–40 лет и более молодые, готовые к новому, то сейчас 40+. Что касается запросов, то я в основном работаю с бизнесом. Но бизнес делают люди. Поэтому, когда клиент приходит с темой командообразования, делегирования, масштабирования, фокуса внимания, в любом случае в работе с коучем всегда все это упирается в личное. На мой взгляд, очень популярны запросы: делегирование и командообразование — потому что люди грязнут в операционке.

БИЗНЕС ТЕХНОЛОГИИ ПРОЦЕССЫ
УПРАВЛЕНИЕ ПЕРСОНАЛОМ
www.TOP-PERSONAL.ru

***Наталья Пешкова**, executive бизнес-коуч

Елена Костина

— В прошлом году наша федерация проводила исследования на тему бизнес-коучинга и в результате мы отметили, что и у наших клиентов, и в общем российский рынок бизнес-коучинга следует общим мировым тенденциям, прирастает в среднем на 15–17 % в год. При всем при этом есть различия, как раз продолжая то, что сказала Наталья Пешкова, отличие в том, что глобальный коучинг в основном принадлежит корпорациям и является корпоративным, а в России практически 50–60 % коучей — это представители микро и малого бизнеса. Также развивается новая тенденция: услуги коучей заказывают госструктуры, и этот тренд действительно двигается семимильными шагами.

***Елена Костина**, вице-президент Национальной Федерации профессиональных менторов и коучей

О чём спорят компании сегодня

Кристина Воронина, юрист в сфере интеллектуальной собственности и блогосферы, основатель юридического бутика
▪ Эксперт СМИ (Коммерсантъ, Ведомости, Mail.ru, РБК, Rambler и т. д.),
▪ Спикер мероприятий: центра Мой бизнес, Инстадиум (онлайн сцена), Форум недвижимости Черноземья и др.,
▪ Член Союза юристов-блогеров на базе МГЮА при АЮР,
▪ Основатель своего проекта по правовому просвещению предпринимателей.

Какие проблемы интеллектуальной собственности сегодня в топе споров?

Юридическая компания ЭБР провела исследование о судебных спорах в сфере интеллектуальных прав в 2024 г., из которого можно отметить незначительный рост в 5% общего количества судебных процессов в данной области: в сфере защиты авторских и смежных прав рост составил 35%, а по товарным знакам, наоборот, небольшое уменьшение, также меньше на 43% стало споров по фирменному наименованию.

Активное развитие IT-сферы: регистрации программ, баз данных, создание отечественного программного обеспечения, использование нейросетей — однозначно имеет прямое влияние на рост споров в этой области.

Можно спрогнозировать увеличение количества споров по товарным знакам, в связи с тем, что зарубежные бренды уходили с рынка России, а по закону в случае, если товарный знак не используется в течение трех лет, его правовая охрана может быть окончена. А сейчас наблюдается продление товарных знаков или подача заявок на новые знаки зарубежных брендов, что связывали с возможным возвратом их в Россию. Однако некоторые компании все-таки утратили право на товарный знак, что может привести к волне судебных разбирательств из-за регистрации сходных знаков.

Что касается так называемой «кражи» интеллектуальной собственности, а именно незаконного использования ПО, товарных знаков,

фотографий и других объектов, можно сделать вывод, что нарушения и будут продолжаться в связи с уровнем правовой культуры граждан и предпринимателей, многие из нарушителей, как показывает практика, просто не знают, что нельзя использовать чужое фото, название из сети Интернет, скачивать нелицензионное ПО.

IT — о чем хотят спорить владельцы ПО?

В сфере IT споры о незаконном использовании программ для ЭВМ являются одними из самых распространенных.

Например, использование нелицензионного ПО, например, в деле № А41-42667/12 ИП использовал программу без заключения договора с правообладателем в своем интернет-клубе и проиграл 230 тыс. руб. в пользу ООО «1С»; а в похожем деле № А15-9795/2023 об использовании программных продуктов без разрешения и соответствующего договора истец ООО «1С-СОФТ» выиграл суд на 915 тыс. руб. компенсации.

Часто спорят работодатели и сотрудники относительно прав на созданные продукты: работодатели просят суды признать права на ПО за ними, а работники пытаются взыскивать компенсацию за использование таких продуктов с работодателей.

Суды отказывают работникам, если работодатель предоставляет документы, подтверждающие создание продукта во исполнение служебных обязанностей, подписание актов, а значит отсутствует незаконное использование и права на продукт перешли к работодателю (Постановление Суда по интеллектуальным правам от 1 августа 2019 г. по делу № А40-202764/2018, Решение Савеловского районного суда г. Москвы от 24 ноября 2017 г. № 02-6298/2017); или работник не доказал, что работодатель использовал служебное произведение (программу для ЭВМ) (дело № 33-5564/2017).

Большой пласт споров в IT сфере также вытекает из лицензионных договоров, о правах использования программного обеспечения, баз данных, а в условиях нынешних реалий — споры, связанные с уходом многих IT-компаний из РФ, например, взыскание неосновательного обогащения в связи с прекращением технической поддержки в связи с уходом компании (дело № А40-234757/23-110-1891); расторжение договора из-за отсутствия обслуживания программы (дело № А40-140041/2022).

ЧАСТО СПОРЯТ РАБОТОДАТЕЛИ И СОТРУДНИКИ ОТНОСИТЕЛЬНО ПРАВ НА СОЗДАННЫЕ ПРОДУКТЫ: РАБОТОДАТЕЛИ ПРОСЯТ СУДЫ ПРИЗНАТЬ ПРАВА НА ПО ЗА НИМИ, А РАБОТНИКИ ПЫТАЮТСЯ ВЗЫСКИВАТЬ КОМПЕНСАЦИЮ ЗА ИСПОЛЬЗОВАНИЕ ТАКИХ ПРОДУКТОВ С РАБОТОДАТЕЛЕЙ

Технологии — чем отличаются споры здесь?

С активным развитием технологий в сфере искусственного интеллекта, а также отсутствие в законодательстве четкого регулирования и правового статуса ИИ, стало больше и споров в этой области.

За период с 1 марта 2023 по 1 марта 2024 согласно исследованию RTM Group было вынесено 406 судебных актов, предметом разбирательств которых связан с использованием технологий ИИ. Основными категориями споров по технологиям ИИ являются:

1. споры по договорам на ПО, использующее технологии ИИ;

2. споры о нарушении авторских прав на произведения, созданные с использованием ИИ, например, дело № А40-200471/23-27-1448,

3. административные правонарушения.

В связи с неурегулированностью правового положения технологий искусственного интеллекта прогнозируется рост числа споров в этой области и в дальнейшем.

Дизайн — здесь тоже неспокойно?

Поскольку дизайн относится к объектам авторского права, в этой сфере также много судебных споров. Какие разбирательства встречаются по незаконному использованию дизайна, его элементов?

Взыскание компенсации за нарушение исключительных прав на дизайн упаковок и этикеток (дело № А31-578/2024, № А68-6331/2024, № А51-13908/2023, № А41-84104/23).

Споры встречаются и по правам на дизайн-проекты: так, по делу А63-20181/2023 была взыскана компенсация за нарушение прав на дизайн-проект пиццерии, дизайн фасадной вывески, на паттерны. А в деле А40-166128/24-15-1281 на дизайн-проект выставочного стенда.

Часто правообладатели или их представители регулярно подают иски к предпринимателям, имеющим небольшие торговые точки с различными товарами о нарушении прав на дизайн игрушек, таких как кот Басик (№ А12-2255/2024, А15-5626/2024), зайчик по имени «Зайка Ми» (№А50П-714/2023, № А50-23788/2023), «Гараж пожарная часть», «Гараж с подъемными воротами» (№А35-10006/2023).

Нередки споры о незаконном использовании прав на дизайн изделий, среди таких объектов: рукоятка зубной щетки — 50 тыс. руб. (№ А50-28038/2023), дизайн медалей МК181, МК182, МК183 в размере 150 тыс. руб. (№ А40-117491/17-12-1053), дизайн смесителя — 150 тыс. руб. (№ А41-89897/23), дизайн макеты для семейных пазлов — 30 тыс. руб. (№А60-36794/2024).

Можно сделать вывод, что копирование дизайна материальных предметов часто становится причиной судебных разбирательств, причем в самых разных направлениях.

Товарные знаки — наиболее заметные споры?

По данным исследования юридической компании ЭБР, в прошлом году число дел по товарным знакам уменьшилось на 6% (до 18087 дел).

Рассмотрим интересные споры по товарным знакам.

— В 2023 г. суд по интеллектуальным правам поставил точку в споре Coca-Cola против «Напитков из Черноголовки». Coca-Cola выступала против предоставления правовой охраны товарному знаку «Фантола» и ссылалась на наличие вероятности смешения указанного названия с зарегистрированными ранее на имя компании: «ФАНТА», «FANTA». Судом решено: «Фантоле» быть, товарные знаки Fanta и «Фантола» не ассоциируются друг с другом. Дело № С01-2406/2022, СИП-353/2022 https://kad.arbitr.ru/Card/ce1d2672-1d1d-434d-a92a-055010a75603

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Документирование инженерных проектов, переход на ЭДО

Пётр Сухоруких, предприниматель, эксперт по антикризисному PR, основатель международного агентства цифровой репутации «Невидимка»

Бумажный архив уязвим по определению

Что на самом деле хранит ваш архив: активы или риски? Почему ЭДО — это ответ из области стратегии, но никак не технологий.

Если завтра к вам придет запрос от Ростехнадзора на предоставление полного комплекта исполнительной документации по объекту, сданному три года назад, сколько времени потребуется вашей компании на его выполнение? Неделя? День? Час? Ответ на этот вопрос с предельной точностью определяет уровень цифровой зрелости вашего бизнеса и, в конечном счете, его операционную устойчивость.

Меня зовут Петр Сухоруких, и в сфере моей компетенции — управление репутационными рисками. На основе анализа десятков кризисных ситуаций в строительной и производственной отраслях я утверждаю: подавляющее большинство финансовых потерь и репутационных провалов имеют в своей основе не технологические, а управленческие ошибки. И корень этих ошибок зачастую кроется в архаичной системе работы с документами.

В инженерном деле документация — это не побочный продукт, но неотъемлемая часть производственного цикла.

Чертеж, смета или акт скрытых работ обладают той же значимостью, что и физические активы. Рассматривать процессы их создания, согласования и хранения как второстепенную,

офисную задачу — это управленческий парадокс, который неизбежно ведет к потерям. Поэтому переход на электронный документооборот (ЭДО) следует рассматривать не как дань моде, а как стратегический императив.

Аудит рисков: анатомия бумажного документооборота

Любая система, основанная на бумажных носителях, по своей природе содержит ряд системных уязвимостей. Их необходимо не просто осознавать, но и оценивать как прямую угрозу бизнесу.

Конфликт версионности и отсутствие «единого источника правды».

Наличие нескольких версий одного и того же чертежа в разных отделах, на сервере и в распечатанном виде — это не рабочая ситуация, а прямой путь к производственной катастрофе.

Использование неактуальной версии проектного документа на объекте гарантирует срыв сроков и финансовые убытки, размер которых может быть сопоставим со стоимостью всего проекта.

Латентные временные издержки. Процесс физического согласования документов — «бегунок» — это классический пример скрытых потерь. Время высококвалифицированных инженеров и руководителей тратится не на профильные задачи, а на логистику бумажных листов. Эти издержки не всегда очевидны в отчетах, но они системно снижают маржинальность и скорость реализации проектов.

Риски физической утраты и неконтролируемого доступа. Бумажный архив уязвим по определению. Пожар, затопление, элементарная халатность при хранении могут безвозвратно уничтожить интеллектуальную собственность компании и ее юридическую защиту по сданным объектам. Более того, бумажный документ легко скопировать или вынести, что создает риски утечки коммерческой тайны.

Комплаенс-риски и регуляторная уязвимость. Скорость и точность предоставления документации по запросу надзорных органов или заказчика — это ключевой показатель надежности компании. Неспособность оперативно найти нужный акт или сертификат подрывает доверие и может привести к серьезным штрафным санкциям, вплоть до приостановки деятельности.

КОРЕНЬ ЭТИХ ОШИБОК ЗАЧАСТУЮ КРОЕТСЯ В АРХАИЧНОЙ СИСТЕМЕ РАБОТЫ С ДОКУМЕНТАМИ

Стратегия внедрения ЭДО: от тактической задачи к системной трансформации

Переход на ЭДО — это не проект IT-отдела. Это полноценный бизнес-проект, который должен курироваться на уровне первого лица компании. Его успех зависит от правильной методологии.

Этап 1: Стратегическое позиционирование. Ключевая задача руководства — позиционировать проект не как центр затрат, а как

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Как увольнять топов и выживать после этого: практический опыт Вячеслава Баженова

В условиях кадровой турбулентности, постоянной перетасовки управленцев и конкуренции за сильных специалистов вопрос увольнения топ-менеджеров становится для бизнеса не менее важным, чем их найм. Вячеслав Боженов, руководитель бухгалтерской группы Bridge Group, поделился с редакцией своим подходом к расставанию с управленцами — и сделал это без прикрас.

БИЗНЕС ИДЕЙ БИЗНЕС РЕШЕНИЯ БИЗНЕС ТЕХНОЛОГИИ БИЗНЕС ПРОЦЕССЫ
УПРАВЛЕНИЕ ПЕРСОНАЛОМ
www.TOP-PERSONAL.ru

Когда увольнение — это не конфликт, а управленческий процесс

По мнению Боженова, эффективное увольнение — это не эмоциональный всплеск, а продуманный процесс. Он делит его на две составляющие:

Юридическую: корректные трудовые договоры, должностные инструкции, испытательный срок, прописанные KPI;

Управленческую: подготовка, спокойный тон и переговоры без давления.

«95% руководителей, если с ними поговорить без унижения и с фактами на руках, уходят по-хорошему», — утверждает Боженов.

Вячеслав Баженов
Bridge Group

Электронный архив компании: анализ проблем, создание и ведение

Николай Маевский, руководитель группы Управление развития и сопровождения информационных систем и решений, Группа развития портала и ОТ ООО «Центр корпоративных решений»

Евгения Воротынская, директор по сопровождению продаж ООО «Центр корпоративных решений».

Делимся полезными советами и уроками для бизнеса, которые мы усвоили за 6 лет работы электронного архива ЦКР

В июле 2019 года в Центре корпоративных решений появился свой электронный архив. С тех пор прошло почти 6 лет, и за это время команда ЦКР накопила существенный опыт работы с системой. Настало время им поделиться: начнем с общих советов по выбору платформы.

Как выбрать платформу для внедрения электронного архива / СЭД?

Одни проще дорабатывать, но на них более дорогие лицензии — другие, наоборот, дешевле, но сложнее и дороже в развитии. Важно также учитывать сложность дальнейшего сопровождения и наличие компетенций на рынке труда. Давайте разберемся, какой может быть целевая платформа.

По методу установки выделяют:

1. On-premise платформы (установленные внутри инфраструктуры компании)

Плюсы: высокая безопасность данных (данные не уходят дальше компании), гибкость (возможность модернизировать систему в зависимости от потребности).

Минусы: затраты на поддержку инфраструктуры и команду сопровождения платформы;

2. Клаудные решения (решение, развернутое на инфраструктуре вендора)

Плюсы: высокая стабильность, надёжность (вендор гарантирует, что система будет работать 99,7% времени в год), отсутствует необходимость в содержании внутренней команды поддержки со стороны инфраструктуры и самой системы.

Минусы: отсутствие гибкости в развитии (вендор имеет обязательства по доступности, поэтому не может рисковать), крайне высокая стоимость доработок (доработку может сделать только вендор, в связи с чем он завышает цены).

Как показывает наша практика — on-premise лучше, чем клауд.

По размеру компаний, для которых подходит платформа:

1. Энтерпрайз. Данные ECM-системы спроектированы под большой объём данных, справляются с большой нагрузкой, имеют практически бесконечные возможности масштабируемости. Но данные системы, как правило, очень дорогие.

2. Системы для малого бизнеса. Данные ECM-системы стоят дешевле и являются более простыми, чем энтерпрайз решения, но обладают меньшим набором функционала, значительно сложнее масштабируются, хуже справляются с нагрузкой.

По методу распространения:

1. Open Source

Плюсы: бесплатные.

Минусы: решение не имеет конкретного вендора и, как следствие, не имеет вендоровской поддержки, могут быть сложности с установкой.

2. Проприетарные решения

Плюсы: получают регулярное обновления, имеют официальную поддержку вендора, в связи с их коммерческой сутью обладают большим функционалом, чем open source решения, и значительно проще в установке.

Минусы: платность.

На этапе внедрения важно задуматься о том, что в электронном архиве потребуются отчеты по большому объёму данных. Если этого не сделать, то примерно после года работы станет ясно, что для их обработки системе требуются серьезные оптимизации в части базы данных, а возможно и пересмотр процесса обработки документов.

Электронный архив может хранить в себе любую документацию, в том числе и персональные данные граждан, которые требуют особого уровня защищенности. Как следствие, системе необходимо повышенное внимание служб информационной безопасности и отдельных протоколов работы.

В чем может быть сложность внедрения электронного архива / СЭДа?

Как и любая автоматизация, внедрение СЭД предполагает, в первую очередь, систематизацию всех процессов: обмена и хранения документов и их централизации и унификации между всеми подразделениями. Именно эта работа позволяет гладко и бесперебойно переложить документооборот на строгие рельсы системы.

Как правило, ECM-системы, на базе которых делаются электронные архивы и СЭДы, это не просто «файловое хранилище» (многие воспринимают его именно так), а мощный инструмент организации работы с корпоративным контентом. Он включает в себя, в том числе, автоматизацию бизнес-процессов, делая их более прозрачными и понятными для

Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru

всех участников.

Это ведёт и к неочевидным экономическим эффектам: например, можно «заставить» систему саму пересылать документы между участниками в зависимости от принятых ими решений, что оптимизирует их бумажную передачу. А внедрение OCR-системы (распространённый кейс: документы, которые заводятся в архив / СЭД, заводить через OCR) позволяет автоматически создавать для документов карточки с реквизитами, которые были распознаны OCR-системой, с последующей их автоматической отправкой в обработку).

Сейчас там, где документы, обязательно есть и ЭЦП

Поэтому возможность массового подписания необходимо обязательно учесть в проработке внедрения выбранной вами системы.

Часто бывает так, что архив внедряется параллельно с учётными системами. Очень важно, чтобы у команды реализации все системы были в одном приоритете. Так как если архивное хранилище и его связи с внешними ИС проработаны поверхностно, то это обязательно выльется в дополнительные трудозатраты и доработки, как архива, так и систем. Функционал ECM систем бесконечен, так как разработать можно всё.

Пример: ведение бумажного архива

Поделимся одним из функционалов, который есть в системе, но далеко не всегда используется: ведение бумажного архива. Любой бумажный документ должен передаваться на централизованное хранение в бумажный архив, где далее хранится в течении срока, определенного законодательством.

ECM-система позволяет отслеживать перемещение бумажных документов между субъектами компании (например, между офисами в разных локациях), отслеживать срок хранения этих документов, маркировать документы к «утилизации», помогает в физическом поиске этих документов по архиву. В системе можно генерировать и печатать специальны

ПОДАРОК!!!

Вместе с журналом «Делопроизводство» вы можете получать в подарок другие бизнес-издания Издательства: «Управление персоналом», «Мастер продаж», «Трудовое право», «Жилищное право», «Коммерческие споры», «Секретарское дело», «Клуб главных бухгалтеров», «Айти ревью», «Альманах» и пр.

Пришлите заявку на вацап 89263501881

Увольнять «трудных, но сильных» гораздо сложнее, чем слабых

БИЗНЕС ИДЕЙ БИЗНЕС РЕШЕНИЯ БИЗНЕС ТЕХНОЛОГИИ БИЗНЕС ПРОЦЕССЫ
УПРАВЛЕНИЕ ПЕРСОНАЛОМ
www.TOP-PERSONAL.ru

В каждой компании есть такой человек… Сложный, но «с руками». Знает всё, держит в голове полсистемы, умеет «разрулить», когда все разводят руками. Цепкий, остроумный, резкий. А иногда токсичный, непредсказуемый, вредящий культуре. И ты как руководитель сто раз себе говорил: «Если он уйдёт — все рухнет». А потом приходит день, когда ты понимаешь: если он не уйдёт — все рухнет…

Сергей Былинкин
бизнес-тренер

И вот ты уже не решаешь: увольнять или нет. Ты решаешь: как это сделать профессионально, по-взрослому и по-человечески.

Этап 1. Подготовка: увольнение начинается с головы, а не с приказа.

Если вы всерьёз готовитесь к расставанию с «незаменимым», начните с себя.

Признайте факт: он уже не вписывается.

Рынок ЦОД и дата центров: непрерывный рост, технологическая адаптация и региональная локализация

Денис Копытов,
СК ГОРОД

К началу 2025 года совокупная мощность ЦОДов в России превысила 3,6 ГВт. Реализация крупнейших текущих проектов строительства новых дата-центров смогут увеличить эту цифру вдвое.

Особенности и главные тенденции

Рост объемов рынка ЦОД и дата-центров — мировая тенденция. Если к концу 2024 года он оценивался в 347,64 млрд долларов США, то уже к декабрю этого года аналитики прогнозируют цифру в свыше 386 млрд. Дальнейшие прогнозы также впечатляют — постоянный рост минимум на 12% в год и общий оборот, превышающий 1 трлн долларов в 2034. Сегодня это один из самых стабильных мировых рынков.

Главным фактором роста является взрывной, постоянно нарастающий спрос. Это видно и в мировой тенденции, и на примере российского сегмента. Развитие ИИ и повышение спроса на облачные хранилища привели к тому, что в мае заказчики Московской области столкнулись с дефицитом свободных мощностей. Все введенные в систему к 2024 году площадки были арендованы уже в 1 квартале 2025-го, а стоимость размещения выросла более, чем на 31%.

Анализируя рынок ЦОД важно учитывать его географию: более 85% центров в России расположены в непосредственном соседстве с мегаполисами. 76% - сосредоточены в столице, где сегодня функционирует 53,4тысяч стойко-мест. Причины такого распределения просты: близость основных потребителей, большое количество специализированных кадров и наличие крупных электростанций. Электричество в целом — одно из главных преимуществ в развитии ЦОД и дата-центров в России. При среднемировом тарифе в 8,67 ₽ за кВт/ч в нашей стране кВт/ч обходится всего в 4,8 ₽. С учетом того, что энергия — это основная доля расходов в процессе эксплуатации ЦОД, такое преимущество не может не привлекать инвесторов.

Стратегические направления

Одной из главных тенденций развития рынка в России в ближайшее время станет децентрализация ЦОД и появление новых центров в регионах, обладающих менее нагруженной энергетической системой. Среди возможных направлений: республика Хакасия, Иркутская и Мурманская область, Красноярский край.

Еще одно важное направление развития — комплексное инфраструктурное строительство ЦОДов с внедрением собственных генерирующих мощностей, включая инвестиции в альтернативную возобновляемую энергетику и системы накопления энергии для нивелирования последствий пиковых нагрузок.

Преодоление главных вызовов

Динамичное развитие рынка в России идет параллельно с нарастанием санкционного давления. Ограничения существенно повлияли на структуру поставок и логистику, но большинству поставщиков удается не только сохранять высокий уровень надежности и сервиса, но и модернизировать оборудование. В многом помогают системы параллельного импорта, но все более яркой тенденцией становится переход на отечественные решения и наше оборудование. Конечно, этот процесс требует непростой адаптации и обучения команд поддержки, но те мощности, которые уже работают на российском оборудовании, дают хорошие показатели отказоустойчивости.

В свете описанных выше тенденций важнейшим вопросом, встающим перед операторами ЦОД становится поиск и обучение специалистов. Развертывание и техническое обслуживание таких систем требует профессионального подхода и быстрой адаптивности команд. Большинство компаний, создающих свои центры обработки, и дата-центры, стараются «выращивать» своих специалистов, заточенных под технологию и оборудование. Именно поэтому одна из тенденций развития системы ЦОД — их приближение к наукоградам и агломерациям, славящимся своими техническими вузами.

Стоит признать, что отрасль дата-центров в нашей стране — это «рынок поставщика». В условиях дефицита стойко-мест именно оператор диктует условия и создание собственной экспертизы — обязательное условие стабильной работы. Именно поэтому среди возможных площадок реализации проекта технополиса на 5 тысяч стойко-мест мы выбрали именно Серпухов.

Строительство новых центров

- Рынок ЦОД в 2025 году можно охарактеризовать целым рядом важных для понимания и развития отрасли трендов:
- Цифровизация и повышение спроса на облачные сервисы — залог 25-процентого

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

роста рынка в деньгах;

- Дефицит стойко-мест будет только нарастать вместе со спросом;
- Рынок постепенно входит в стадию зрелости, а значит число крупных игроков и инвесторов начнет расти;
- Нехватка специалистов в отрасли скоро станет одним из основных факторов риска в эксплуатации ЦОД.

Безусловно, строительство масштабных центров будет только набирать обороты. Уже сегодня десятки крупнейших игроков страны уже запустили возведение собственных ЦОД и дата-центров. Цент

«Яндекс» занимается развертыванием масштабного центра на 3,8 тысяч стоек в Калуге, «Росатом» возводит объект на тысячу стоек в Нижегородской области, Wildberries планирует ввести в этом году дата-центры в Дубне и Наро-Фоминске.

Такое активное строительство не могло не повлечь ужесточения контроля со стороны Минстроя. В результате в действие вступили новые стандарты проектирования и строительства дата-центров (СП 541.1 325 800.2024). Обновленные правила предъявляют четкие требования к участкам и инфраструктуре, энергоэффективности и устойчивости объектов.

Технологические площадки нового времени

Именно основываясь на всех этих вводных мы и приступаем к проектированию нового кластера, получившего имя «Технополис Сер-пухов». Он станет площадкой для развития SaaS-решений, дата-центров и интеллектуальных систем видеоаналитики и будет включать 5 тысяч стоек. Мы учли все тенденции рынка, выбрали регион с высоким кадровым и инфраструктурным потенциалом, проработали инженерные решения, которые позволят снизить энергопотребление на 25% и использовать альтернативные источники энергии. Именно за такими проектами будущее российских ЦОД, которые позволят пользователям получать целый ряд услуг для цифровизации:

- Colocation —размещение клиентского оборудования у оператора ЦОД с подключением к энергосети и каналам связи и обеспечением условий функционирования.
- Dedicated server — аренда физического сервера в дата-центре провайдера с полным контролем над ресурсами. Это один из самых востребованных форматов среди небольших компаний и стартапов так как экономит средства и позволяет быстро масштабироваться.
- Cloud —набор инструментов для доступа к виртуальной облачной инфраструктуре, в частности на основе моделей IaaS, SaaS, PaaS и другим.
- SaaS –предоставление пользователям онлайн-доступа к программному обеспечению, которое обслуживает и развивает оператор, а клиент подключается к уже готовому продукту через Интернет.
- PaaS — аренда готовой облачной платформы для разработки, тестирования и развёртывания приложений. Пользователь-разработчик получает полноценную виртуальную среду разработки, которую может настраива

Вместе с журналом «Делопроизводство» вы можете получать в подарок другие бизнес-издания Издательства:

«Управление персоналом», «Мастер продаж»,
«Трудовое право», «Жилищное право», «Коммерческие споры»,
«Секретарское дело», «Клуб главных бухгалтеров»,
«Айти ревью», «Альманах» и пр.

Пришлите заявку на вацап 89263501881

Зачем крупным компаниям собственные дата-центры?

Алексей Рубаков, основатель компании N E T R A C K — ведущий оператор комплексных решений в области ЦОД

Дата-центр — это не про сервера. Это про архитектуру будущего, которую компания закладывает уже сейчас.

— Кому сегодня действительно нужны дата-центры?

— Дата-центры нужны тем, кто работает с большими объёмами данных, где информация — не вспомогательный инструмент, а стратегический актив. Тем, у кого данные — это не вспомогательный инструмент, а ключ к бизнесу. Это финансовый сектор, телеком, ритейл, госсектор, крупная промышленность. Но сегодня к ним добавились и те, кого раньше трудно было представить в числе высокотехнологичных игроков — агрохолдинги, транспортные компании, образовательные и медицинские учреждения. Объединяет их то, что объёмы данных растут экспоненциально, а требования к их безопасности, скорости обработки и доступности — становятся критически важными. Они ежедневно генерируют, анализируют и хранят колоссальные объёмы информации, и без собственных ИТ-инфраструктур обойтись уже невозможно. Дата-центр в этом смысле — не просто помещение с серверами, а стратегическая часть бизнес-модели.

— Почему в последние годы крупные компании всё чаще строят собственные ЦОДы?

— Казалось бы, есть облака — арендуй и пользуйся. Зачем кукушке строить гнездо? Хорошая метафора, но не точная. Кукушка откладывает яйца и уходит, а компании наоборот — берут ответственность и строят под себя. Причин несколько. Во-первых, это контроль над данными. Свой дата-центр означает полное управление данными без зависимости от внешних провайдеров. Это особенно важно для банков, телекомов, критично для компаний, которые обязаны строго соблюдать регуляции по защите персональных данных или работают с государственными заказами. Кроме того, у каждой компании есть свои особенности: архитектура приложений, специфические требования к отказоустойчивости, пропускной способности, безопасности. Ну и, наконец, имиджевая составляющая. Для технологических брендов, финансовых структур, да и для многих индустриальных компаний наличие собственного ЦОДа — это маркер зрелости, стратегичности, надёжности. Но и есть другой логичный вопрос — особенно со стороны финансов или HR-директора — зачем вкладываться в «железо», когда всё можно арендовать? Собственный ЦОД — не всегда и не всем нужен. Это дорого, долго и требует глубокой инженерной экспертизы, особенно в современном мире, когда технологии работы с данными постоянно меняются. Поэтому разумная альтернатива — доверять тем внешним операторам, которые действительно соответствуют высочайшим стандартам. Мы также видим, как растёт спрос на гибридные решения — когда часть ИТ-инфраструктуры уходит в частное облако, часть — в арендуемые стойки в коммерческом ЦОДе, а наиболее чувствительные компоненты остаются на своих площадках. Такой подход позволяет компаниям не выбирать между «своё» и «в аренду», а использовать лучшее от обеих моделей. Плюс экономика масштаба: когда бизнес перерастает в терабайты, стоит оценить, что выгоднее — аренда в коммерческом ЦОДе, или инвестировать в собственную площадку, с учетом окупаемости этих инвестиций. По сути, вопрос не в том, строить ли «гнездо» самому или воспользоваться надёжным чужим — вопрос в том, как обеспечить устойчивость и управляемость данных, не потеряв фокус на основном бизнесе.

ВОПРОС В ТОМ, КАК ОБЕСПЕЧИТЬ УСТОЙЧИВОСТЬ И УПРАВЛЯЕМОСТЬ ДАННЫХ, НЕ ПОТЕРЯВ ФОКУС НА ОСНОВНОМ БИЗНЕСЕ

И здесь доверие к внешним ЦОДам — это уже не просто компромисс, а стратегическое решение, если за ним стоят технологии, процессы и команда с настоящей инженерной культурой.

— Как формируется команда, которая обслуживает такой сложный объект? Где брать людей, которые умеют работать с дата-центрами?

— Это один из главных вызовов отрасли. Дата-центр — это инженерная экосистема, которая требует высокой квалификации и полной синхронности между отделами. Здесь работают системные инженеры, специалисты по сетевой безопасности, энергетики, проектировщики, дежурные смены, и каждый из них влияет на стабильность всей системы. Мы в Netrack уже давно поняли: «готового» специалиста с рынка взять почти невозможно. Поэтому основной акцент делаем на внутреннюю подготовку и выстраивание кадрового контура. Мы сотрудничаем с профильными

вузами — Бауманкой, МЭИ, ИТМО. Работаем с колледжами — для подготовки технического персонала, который потом растёт внутри компании. Но самое главное — у нас есть собственная система наставничества и адаптации. Мы не просто «нанимаем», мы растим команду, потому что в ЦОДе критично важны не только знания, но и доверие, предсказуемость, устойчивость. Это командная работа 24/7.

— Какие управленческие особенности есть у персонала ЦОД?

— Это же не классический ИТ-отдел. Совершенно верно — это даже не совсем ИТ. Управление персоналом в ЦОДе — это баланс между инженерной дисциплиной, ИБ-культурой и оперативной устойчивостью. Здесь критически важна работа смен, ответственность за процессы, точность регламентов. Люди должны не просто знать, что делать, но понимать — почему. Команду мы формируем вокруг идеи надёжности. У нас нет «случайных» сотрудников. Все проходят стресс-тесты, обучение по стандартам TIA, Uptime, и обязательно — модули по психологической устойчивости. Работа в ЦОДе — это про стабильность и долгую игру. И она возможна только тогда, когда внутри есть чувство плеча и сопричастности. Дата-центр — это экосистема, где растут и развиваются люди. — Какие проблемы сейчас наиболее остро стоят перед отраслью? Начну с очевидного — оборудование. Поставки серверов, систем хранения, ИБП, кабельных решений всё ещё нестабильны. Это добавляет непредсказуемости в проектирование и ввод новых объектов. Второе — рост стоимости электроэнергии. Дата-центры — энергоёмкая отрасль, и даже небольшое колебание тарифа бьёт по всей экономике объекта. Третье — охлаждение. Классические решения с холодными коридорами и фальшполами уже не справляются, особенно в высокоплотных зонах. Всё чаще обсуждается переход на жидкостное охлаждение, но это требует и новых технологий, и нового мышления. Четвёртая проблема — кадры. Мы её уже обсудили, и она комплексная: это не просто нехватка людей, это необходимость формировать внутри компании полноценную образовательную среду.

ЭТО ВОПРОС НЕ МОДЫ, А ВЫЖИВАНИЯ. ТЕ, КТО УПРАВЛЯЮТ СВОИМИ ДАННЫМИ, ПОЛУЧАЮТ НЕ ПРОСТО КОНКУРЕНТНОЕ ПРЕИМУЩЕСТВО

— Что нового на горизонте в плане технологий хранения и обработки данных?

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Время «офисного планктона» прошло

БИЗНЕС ИДЕЙ БИЗНЕС РЕШЕНИЯ БИЗНЕС ТЕХНОЛОГИИ БИЗНЕС ПРОЦЕССЫ
УПРАВЛЕНИЕ ПЕРСОНАЛОМ
www.TOP-PERSONAL.ru

Какие бизнес-вызовы стоят сегодня перед GVS RUS?

Вадим Демидов
генеральный директор GVS, Италия

В последние годы происходят системные изменения в экономике по всему миру. Меняются потребности рынка и ожидания клиентов, как следствие происходят глубокие структурные изменения. Меняется география поставок, финансовые процедуры, коммерческие условия и многое другое.

Рынок сейчас требует большой скорости реакции на возникающие потребности. Так, если раньше было нормальным прогнозировать на три-пять лет вперед и планомерно реализовывать намеченные планы, то сейчас ситуация кардинально меняется каждый месяц. Недостаточно правильно выстроить бизнес-процессы. Необходимо в режиме реального времени корректировать бизнес-процедуры, а иногда и полностью пересматривать стратегии.

Например, во время начала пандемии спрос на бактериально-вирусные фильтры возрос многократно. Многие производители как сырья, так и готовых медицинских изделий просто не справлялись с увеличением спроса. Наша компания отреагировала молниеносно, оперативно были найдены дополнительные поставщики сырья, увеличены производственные мощности, организованы дополнительные ночные смены для круглосуточного производства. Должен сказать, что во время пандемии, когда другие производители ограничивали поставки на другие

У каждой серьезной компании есть свой собственный архив с грифом «секретно»

Пётр Сухоруких, предприниматель, эксперт по антикризисному PR, основатель международного агентства цифровой репутации «Невидимка»

Когда речь заходит о документах с грифом «Совершенно секретно», воображение рисует сцены из шпионских фильмов: обмен папками на мосту, вскрытые сейфы и государственные тайны. Однако в моей практике, связанной с защитой репутации и управлением кризисами, я утверждаю: у каждой серьезной компании есть свой собственный архив с грифом «секретно». И цена утечки из него порой сопоставима с провалом разведывательной операции.

Речь, конечно, не о государственных тайнах, а о корпоративной информации, преждевременное или неконтролируемое раскрытие которой может уничтожить многомиллионную сделку, обрушить акции, разрушить карьеру топ-менеджера и нанести непоправимый ущерб репутации. Принципы работы с такой информацией, как ни странно, очень близки к тем, что приняты в спецслужбах.

Что такое корпоративные «документы с грифом»?

В нашей работе мы сталкиваемся с ними постоянно. Это не просто конфиденциальные договоры. К этой категории я отношу любую информацию, которая в конкретный момент времени является критически уязвимой.

Сделки M&A (слияния и поглощения). До официального объявления любая утечка — это риск срыва переговоров и манипуляций на фондовом рынке. Вся документация по таким проектам — это «совершенно секретно».

Антикризисные стратегии. Когда мы готовим компанию к потенциальному кризису (например, к судебному разбирательству или информационной атаке), мы разрабатываем несколько сценариев реагирования, готовим заявления, Q&A для спикеров. Эти документы — наша «красная папка». Попади она в руки оппонентов — и весь план защиты обесценится.

Информация о готовящемся ребрендинге или запуске флагманского продукта. Утечка за полгода до старта дает конкурентам огромное преимущество и убивает весь маркетинговый эффект «большого взрыва».

Персональные данные и компрометирующая информация. Досье на топ-менеджеров, детали их личной жизни, медицинские данные, которые могут быть использованы для шантажа или дискредитации.

Стратегии судебных разбирательств. Позиция адвокатов, список свидетелей, внутренняя переписка по делу — все это требует высочайшего уровня защиты.

Особенности работы: три кита корпоративной безопасности

Работа с такими данными строится на принципах, которые мы в агентстве считаем незыблемыми.

1. **Принцип «Need-to-Know»** (необходимого знания). Это золотой стандарт спецслужб. Его суть проста: доступ к чувствительной информации должен иметь не тот, у кого есть соответствующий уровень допуска, а только тот, кому эти сведения абсолютно необходимы для выполнения его конкретной задачи.

В корпоративном мире это самый часто нарушаемый принцип. Привычка ставить в копию

ЦЕНА УТЕЧКИ ИЗ НЕГО ПОРОЙ СОПОСТАВИМА С ПРОВАЛОМ РАЗВЕДЫВАТЕЛЬНОЙ ОПЕРАЦИИ

письма всех, «чтобы были в курсе», — это прямой путь к утечке. При подготовке сделки M&A информацию получает не весь совет директоров, а только рабочая группа из 3–5 человек. Юристы знают только юридическую часть, финансисты — только финансовую. И только руководитель проекта и CEO видят всю картину целиком. Чем меньше людей знает, тем ниже вероятность утечки — случайной или намеренной.

2. **Информационная гигиена**. Это комплекс практических мер, которые должны стать второй натурой для каждого, кто допущен к «секретам».

- **Цифровые каналы**. Никаких обсуждений в личных мессенджерах вроде WhatsApp или Telegram. Только защищенные корпоративные чаты, виртуальные комнаты данных (VDR) с шифрованием и контролем доступа. Все документы должны передаваться по зашифрованным каналам и храниться на защищенных серверах, а не в «облаках» общего пользования.
- **Физические носители**. Распечатки

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Сегодня нужны другие, творческие люди, которые делают то, что любят, и любят то, что делают

БИЗНЕС ИДЕЙ БИЗНЕС РЕШЕНИЯ БИЗНЕС ТЕХНОЛОГИИ БИЗНЕС ПРОЦЕССЫ
УПРАВЛЕНИЕ ПЕРСОНАЛОМ
www.TOP-PERSONAL.ru

Как меняется современная бизнес-среда?

Успешные предприниматели же, как правило, все эти годы обладали тремя характеристиками —

жадные, хитрые и быстрые.

Гарретт Джонстон

А сейчас это будет меняться, потому что в скором времени появится суперкомпьютер, умещающийся в кармане, с мощностью 3,5 триллиона операций в секунду. Этого достаточно, чтобы просчитать миллиарды сценариев, все возможные способы заработать деньги. То есть компьютеры умеют заработать деньги в миллиарды раз быстрее, чем даже самый хитрый торгаш. Представителям эпохи «купи-продай» приходит конец. 90% сегодняшних бизнесменов, которые просто «про деньги», уже не нужны. Нужны другие, творческие люди, которые делают то, что любят, и любят то, что делают.

Система распознавания лиц: куда идут ваши персональные данные. Основания для работы системы распознавания лиц

Максим Лагутин, эксперт по защите персональных данных, основатель компании Б-152

В России набирает популярность биометрическая оплата, когда система распознавания лиц идентифицирует человека по его внешности и списывает средства с привязанного к профилю счёта. Это удобно. Но все ли задумываются, где и как хранятся персональные данные (ПДн), насколько это безопасно. О правилах работы с биометрией рассказал Максим Лагутин, основатель компании Б-152, эксперт по защите персональных данных.

Что такое биометрические персональные данные?

Ст. 11 152-ФЗ даёт определение биометрических ПДн — это сведения, характеризующие физиологические и биологические особенности человека, на основании которых возможно установить его личность.

Например, фотографические данные, то есть цифровые изображения лица используют в пропускных системах и банковской верификации. Голосовые образцы с уникальными речевыми паттернами помогают усилить системы безопасности. А дактилоскопические данные, такие как отпечатки пальцев и ладоней

используют для разблокировки смартфонов и доступа в secure-зоны.

Фотография и распознавание лиц — это биометрия?

На этот вопрос Роскомнадзор отвечает в своём письме. Фотоизображение не содержит информации, являющейся биометрической по своей сути, поскольку не отражает индивидуальных параметров субъекта ПДн, таких как термограмма лица, рисунок радужной оболочки глаза, папиллярных узоров, позволяющих установить личность.

Свою позицию Роскомнадзор также обосновал в другом письме. Фотографии считаются биометрическими данными, если используются для автоматизированной идентификации личности, применяются в системах верификации или аутентификации, соответствуют установленным стандартам обработки. Для них действует ГОСТ Р ИСО/МЭК 19794-5-2013, устанавливающий требования к формату изображений, стандарты для хранения биометрических шаблонов лица и технические параметры для систем распознавания.

То есть просто фото, как в соцсетях или анкетах для собеседования, не может быть биометрией, потому что не сделано со специальными технологиями. Единственный вариант, когда обычное фото может быть использовано как биометрия — проведение оперативно-розыскной деятельности, тогда фото из соцсетей используется для идентификации преступника.

Таким образом, ФИО, телефон, e-mail, ИНН — это обычные ПДн, которые хранятся в ИСПДн при обработке через ИС. Фото сотрудника в анкете — тоже обычные ПДн, если не используется для идентификации. А если фотографию сделать с использованием специальных устройств, которые снимают биометрию — это уже биометрические ПДн, так как позволяет определить, кто именно перед нами.

Правовые основания обработки биометрических данных

Биометрию правомерно обрабатывать исключительно при наличии письменного согласия субъекта, которое должно быть конкретным и осознанным. Для каждого типа данных нужно отдельное согласие.

Однако в часть 2 статьи 11 перечислены исключения. Например, согласие не обязательно, если обработка проводится в рамках правосудия или в других случаях, предусмотренных законом для обеспечения безопасности.

При этом операторы обязаны использовать сертифицированные средства защиты, соблюдать требования к хранению и передаче данных, а также обеспечивать конфиденциальность на всех этапах обработки.

Как обрабатывать биометрию?

Биометрические ПДн хранятся в Единой биометрической системе (ЕБС) — государственной цифровой платформе для установки и подтверждения личности граждан. В ней хранятся непосредственно ПДн, а также биометрические шаблоны или векторы —созданные на основе биометрии математические модели. Также в неё входит иная информация, предусмотренная ч. 16 ст. 4 Федерального закона №152-ФЗ.

Оператором ЕБС является организация, назначенная Правительством РФ, сейчас это АО «Центр Биометрических Технологий».

Биометрические данные собирают лично с помощью сертифицированных устройств. По ВКС собирать биометрию нельзя, прислать фото как на паспорт — тоже. Собранные данные преобразуются в математические векторы, которые поступают в ЕБС через защищённый канал. Поскольку данные чувствительные, каналы должны быть обеспечены максимально защищенными, чтобы не было утечки: защищенные каналы связи, сетевые подключения только к шлюзу, контроль доступа, а также отсутствие доступа в интернет для точки доступа сбора БПД.

ЕБС хранит не исходные биометрические образцы, такие как фото или запись голоса, а только их цифровые шаблоны. При аутентификации биометрические данные сравниваются с этими шаблонами. Результатом проверки становится сообщение о том, совпадает или не совпадает человек и шаблон в ЕБС.

Хранить биометрию вне ЕБС нельзя, это

указано в ч. 7 ст. 14 572-ФЗ. Архивировать копии ЕБС для «возможной сверки» тоже неправомерно, это нарушает режим хранения. В собственной среде допустимо только временное хранение в течение 10 дней по запросу субъекта для дальнейшей передачи в ЕБС. После отправки биометрию хранить запрещено.

Можно хранить биометрию в инфраструктуре центра биометрических технологий (ЦБТ), который считается частью ЕБС.

Как и зачем подавать уведомление в Роскомнадзор

Все операторы ПДн обязаны уведомлять Роскомнадзор о факте обработки биометрии, что закреплено в ст. 22 152-ФЗ. Уведомление необходимо направлять перед началом обработки, поэтому новым компаниям это стоит сделать ещё при регистрации бизнеса, а существующим — с момента, когда приняли решение об обработке, заранее. Если нужно изменить уведомление, когда начали или перестали обрабатывать биометрию, это нужно сделать не позднее 15-го числа месяца, следующего за возникшими изменениями, эти сроки регламентирует ч. 7 ст. 22 152-ФЗ. А в случае утечки любых персональных данных, несанкционированного доступа к ним или других инцидентах — в течение 24 часов.

Это можно сделать через сайт Роскомнадзора или Госуслуги, а также на бумаге по почте или лично в территориальном органе.

За отсутствие уведомления или подачу неверных сведений для организаций и должностных лиц предусмотрены крупные штрафы.

Куда могут «уйти» ваши биометрические данные?

Биометрические данные — лакомый кусок для мошенников. Если паспорт или номер телефона можно поменять, то биометрия — это уникальные идентификаторы, которые невозможно изменить при их компрометации, поэтому так опасны утечки, в результате которых данные попадают в даркнет, где их покупают мошенники и используют для взлома банковских аккаунтов или обмана граждан.

А они могут произойти в результате взлома базы данных, ЕБС взломать проблематично, но если оператор неправомерно хранит данные еще где-то, например, на собственном сервере или в системе подрядчиков, риск взлома и утечки повышается из-за уязвимостей в ПО или слабой защиты.

Возможны угрозы со стороны недобросовестных сотрудников с доступом к ЕБС, они могут продать данные третьим лицам. Поэтому необходим жёсткий контроль доступа с двухфакторной аутентификацией и аудитом действий персонала.

Проблему могут возникнуть не только внутри компании, но и по вине подрядчиков, которые не обеспечивают должную защиту. Поэтому важно заключать договоры с жёсткими условиями конфиденциальности и проверять сертификаты безопасности сервисов.

Ответственность за нарушения в сфере обработки биометрических данных

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Компаниям все сложнее управлять парком устройств

особенно если речь идет о тысячах и даже десятках тысяч рабочих мест

Ильнур Ибрагимов, технический директор продукта «Колибри-АРМ», ICL Services

В последние годы бизнес находится в условиях постоянной трансформации. Ситуация на рынке диктует необходимость оперативной адаптации к новым требованиям — от перехода на российское ПО до интеграции с разнообразными системами управления.

По моим наблюдениям, один из ключевых вызовов сегодня — массовое внедрение и сопровождение пользовательских рабочих мест в гетерогенной (неоднородной, основанной на различных компонентах) ИТ-среде, особенно в условиях импортозамещения и распределенной инфраструктуры.

Мы в команде видим, как компаниям все сложнее управлять парком устройств, особенно если речь идет о тысячах и даже десятках тысяч рабочих мест. При этом инфраструктура часто включает в себя как старые, так и новые компоненты, решения разных вендоров, российское и зарубежное ПО, что значительно повышает нагрузку на ИТ-службы. В таких условиях рынку критически важно получить надежный инструмент централизованного управления, который бы не зависел от внешних факторов и при этом соответствовал

требованиям безопасности и совместимости с отечественными платформами.

Именно поэтому мы разработали решение Колибри-АРМ — систему массового управления автоматизированными рабочими местами, адаптированную под реалии современной корпоративной ИТ-среды. В ее основе лежит практический опыт автоматизации сотен тысяч рабочих мест в крупных российских компаниях. Это не просто альтернатива западным решениям — это продукт, спроектированный с учетом требований российского рынка, включая поддержку различных дистрибутивов Linux, российских ОС, различных сценариев использования и высокого уровня кастомизации.

Наша Колибри-АРМ позволяет централизованно разворачивать, обновлять, настраивать

ОДИН ИЗ КЛЮЧЕВЫХ ВЫЗОВОВ СЕГОДНЯ — МАССОВОЕ ВНЕДРЕНИЕ И СОПРОВОЖДЕНИЕ ПОЛЬЗОВАТЕЛЬСКИХ РАБОЧИХ МЕСТ В ГЕТЕРОГЕННОЙ (НЕОДНОРОДНОЙ, ОСНОВАННОЙ НА РАЗЛИЧНЫХ КОМПОНЕНТАХ) ИТ-СРЕДЕ, ОСОБЕННО В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ И РАСПРЕДЕЛЕННОЙ ИНФРАСТРУКТУРЫ

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

ПОДАРОК!!!

Вместе с журналом «Делопроизводство» вы можете получать в подарок другие бизнес-издания Издательства: «Управление персоналом», «Мастер продаж», «Трудовое право», «Жилищное право», «Коммерческие споры», «Секретарское дело», «Клуб главных бухгалтеров», «Айти ревью», «Альманах» и пр.

Пришлите заявку на вацап 89263501881

Ключ к снижению угроз — комплексный подход

Информационная безопасность крупных компаний и аутсорсеры как причина утечек

Дмитрий Беляев,
ООО АБТ, Директор
по кибербезопасности.
@da_belyaev

В эпоху цифровой трансформации информационная безопасность становится одним из ключевых факторов устойчивости и конкурентоспособности крупного бизнеса. Утечки данных способны не только нанести прямой финансовый ущерб, но и разрушить доверие контрагентов, партнеров, инвесторов. Особое внимание в последние годы уделяется роли интеграторов и аутсорсеров — сторонних компаний и специалистов, которым передаются функции по обслуживанию ИТ-инфраструктуры, разработке программного обеспечения, поддержке бизнес-процессов. Именно взаимодействие с интеграторами и аутсорсерами все чаще становится причиной крупных инцидентов, связанных с утечкой конфиденциальной информации, взломах и шифровании.

Рост числа и сложности кибератак

В 2025 году отмечается устойчивый рост числа киберинцидентов, а также увеличение их сложности. Крупные компании сталкиваются с атаками, использующими современные технологии, включая искусственный интеллект и

LLM, социальную инженерию, сложные вредоносные программы и эксплойты уязвимостей. При этом дефицит квалифицированных специалистов по ИБ вынуждает бизнес все чаще прибегать к услугам внешних подрядчиков и аутсорсеров, и нередки случаи, когда один человек работает на 3 и более компании сразу.

Основные угрозы:

- Смишинг/Фишинг и социальная инженерия (обман сотрудников с целью получения доступа к системам);
- Вредоносное ПО и эксплойты;
- DDoS-атаки на инфраструктуру;
- Утечки данных через внутренние и внешние каналы;
- Нарушения политик безопасности и человеческий фактор.

Почему компании выбирают аутсорсинг

- Оптимизация затрат на ИТ и безопасность;
- Доступ к экспертным знаниям и современным технологиям;
- Возможность сосредоточиться на основном бизнесе;
- Гибкость в масштабировании ресурсов.

Аутсорсеры как причина утечек данных

Механизмы возникновения утечек через аутсорсеров:

1. **Умышленные действия сотрудников подрядчика**
   - Кража данных с целью продажи конкурентам или злоумышленникам;
   - Саботаж и внедрение вредоносного ПО.
2. **Ошибки и небрежность**
   - Неправильная настройка серверов, открытые порты, слабые пароли;
   - Использование незащищенных каналов передачи данных.
3. **Недостаточный контроль доступа**
   - Избыточные права сотрудников интегратора/аутсорсера к корпоративным ресурсам;
   - Отсутствие мониторинга действий подрядчиков и своевременной блокировки доступов.
4. **Нарушения политик безопасности**
   - Отсутствие или формальный характер соглашений о конфиденциальности (NDA);
   - Игнорирование требований по шифрованию, резервному копированию, журналированию действий.
5. **Технические уязвимости**
   - Использование устаревших или несертифицированных решений, отсутствие патчей и обновлений;
   - Неавтоматизированное управление доступом и учетными записями.

Примеры реальных инцидентов

Сноуден и подрядчик АНБ: Один из самых известных случаев, когда сотрудник подрядной компании получил доступ к секретной инфор-

Основные риски аутсорсинга

Риск	Описание
Потеря контроля	Сложность мониторинга действий интегратора/аутсорсера, особенно если он работает удаленно
Недостаточная квалификация подрядчика	Не все интеграторы/аутсорсеры обладают необходимым уровнем экспертизы и зрелыми процессами ИБ
Нарушения конфиденциальности	Риск передачи или утраты коммерческой тайны, персональных данных, критической информации
Технические уязвимости	Использование устаревших или неправильно настроенных решений, отсутствие регулярных обновлений
Внутренние угрозы	Недобросовестные сотрудники интегратора/аутсорсера могут сознательно или случайно стать источником утечки
Юридические и регуляторные риски	Несоблюдение требований законодательства по защите данных, особенно при трансграничной передаче информации

мации и организовал ее утечку, что привело к глобальному скандалу и пересмотру политики работы с аутсорсерами в государственных и частных структурах. В России и мире фиксируются регулярные инциденты, когда подрядчики, обслуживающие ИТ-инфраструктуру или разрабатывающие ПО, становятся источником компрометации данных из-за ошибок, халатности или злого умысла.

Причины уязвимости крупных компаний

Человеческий фактор:

- Сотрудники аутсорсера могут не иметь достаточного уровня подготовки по вопросам ИБ;
- Высокая текучесть кадров у подрядчиков затрудняет контроль и обучение персонала;
- Недостаточная мотивация к соблюдению стандартов безопасности.

Организационные проблемы:

- Отсутствие четких регламентов взаимодействия с подрядчиками;
- Недостаточная детализация SLA (Service Level Agreement) по вопросам ИБ;
- Формальный подход к заключению NDA и других юридических документов.

Технические аспекты:

- Использование подрядчиками собственных ИТ-решений и инфраструктуры, несовместимых с политиками безопасности заказчика;
- Нехватка инструментов для мониторинга и аудита действий подрядчиков в режиме реального времени.

Каналы и типы утечек данных:

- Электронная почта (пересылка файлов вне защищенных каналов):
- Съемные носители (флешки, внешние диски);
- Облачные сервисы и мессенджеры;
- Печать и копирование документов;
- Неавторизованный доступ к корпоративным системам;
- Удаленный доступ через VPN без 2FA, RDP и другие протоколы.

Как минимизировать риски утечек через аутсорсеров

Юридические меры:

- Подробное прописывание ответственности за утечку в договорах и NDA;
- Введение штрафных санкций и компенсаций за инциденты;
- Обязательное заключение соглашений о неразглашении с каждым сотрудником подрядчика.

Организационные меры:

- Проведение аудита подрядчиков перед началом сотрудничества;
- Регулярное обучение и инструктаж сотрудников аутсорсера по вопросам ИБ;
- Внедрение многоуровневого контроля доступа и принципа минимальных привилегий;
- Мониторинг и аудит всех действий подрядчика в корпоративной инфраструктуре.

Технические меры:

- Использование DLP-систем для предотвращения утечек данных;

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Информационная безопасность крупных компаний и аутсорсеры как причина утечек

Александр Вайс,
Серийный FinTech and DeFi предприниматель, разработчик и аналитик WEB3Bureau.
Эксперт по финансовой логистике и трансграничным расчетам
Член комиссии по ЦФА ТПП РФ и РСПП РФ

Когда компания передаёт часть функций подрядчикам, она фактически открывает внутренний периметр для внешних игроков. Даже если отношения оформлены контрактом и регламентированы политиками безопасности, аутсорс остаётся одной из самых уязвимых точек.

Данные важнее денег

Представьте, еще сто лет назад грабители в шляпах и сомбреро с винчестерами останавливали поезда, а условные Бонни и Клайд грабили банки, вскрывали сейфы и уходили с мешками наличных. Сегодня, чтобы получить доступ к деньгам, оружие больше не нужно. Достаточно украсть доступ — и ты уже внутри банка или внутри всей компании.

Всем давно понятно, что деньги — это больше не купюры. Это данные. Управление транзакциями, клиентские базы, конфиденциальные документы, пароли, приватные ключи. Доступ к этим данным ровняется контролю над бизнесом. Особенно в FinTech и DeFi, где одна скомпрометированная строка в коде или незащищённый API может стоить десятки миллионов долларов.

Но при этом парадокс: чем больше компания, тем больше людей вовлечены в процессы, тем чаще она делегирует задачи вовне — и тем больше у неё уязвимостей. Безопасность рушится не от продвинутых атак, а от обыч-

ной логистики доступа. И всё чаще — это не внутренние сотрудники, а подрядчики, фрилансеры, агентства.

Аутсорс стал нормой — это удобная и быстрая оптимизация работы. Но с ним пришёл и новый класс угроз. Когда внешний подрядчик получает доступ в вашу систему, он автоматически становится частью периметра. И если вы не контролируете, как он работает, вы теряете контроль над своей безопасностью.

Под аутсорсерами сегодня понимается широкий круг внешних специалистов и компаний, которым передаются функции, ранее исполнявшиеся внутри организации. Формально они не являются частью компании, но часто имеют доступ к её внутренним данным, системам и даже ключевым процессам.

Главные причины — экономия, гибкость и нехватка собственных специалистов. Аутсорсинг позволяет быстро закрыть задачи, не

ДАННЫЕ ВАЖНЕЕ ДЕНЕГ

В этой статье я разберу, как и почему аутсорсеры становятся причиной утечек, на что не обращают внимания крупные компании, и как выстроить процессы так, чтобы внешние люди не становились внутренней угрозой.

Как работает корпоративная информационная безопасность в реальности

На бумаге информационная безопасность в крупных компаниях выглядит внушительно.

Есть политики безопасности, утверждённые руководством, регулярно обновляемые процедуры реагирования на инциденты, внутренние регламенты, аудит и целый арсенал технических средств — от DLP-систем до SIEM-платформ. Работает Центр мониторинга безопасности (SOC), ведутся логи, проводятся тренинги по кибер-гигиене, а ежегодные аудиты подтверждают соответствие стандартам ISO/IEC 27001, PCI DSS, GDPR и другим.

На практике формализм и бюрократия часто подменяют реальную эффективность. Документы пишутся «под аудит», SOC перегружен событиями и сигналами тревоги, которые никто не успевает анализировать, а тренинги превращаются в обязательную «галочку» в системе корпоративного обучения.

В результате — все формальности соблюдены, а риск утечки данных остаётся критически высоким. Руководство уверено, что защита работает, потому что отчёты — в порядке, но отчётность не равно безопасность.

Аутсорс — удобный, но рискованный ресурс тратя ресурсы на найм, обучение и удержание персонала.

Аутсорс как канал утечки данных

Когда компания передаёт часть функций подрядчикам, она фактически открывает внутренний периметр для внешних игроков. Даже если отношения оформлены контрактом и регламентированы политиками безопасности, аутсорс остаётся одной из самых уязвимых точек. Почему?

- **Удалённый доступ**

Почти все аутсорсеры работают удалённо: через VPN, терминальные сессии, облачные панели администрирования. Это значит, что защита физического периметра компании перестаёт играть роль — злоумышленник может попасть внутрь, скомпрометировав удалённого подрядчика.

Удалённый доступ часто предоставляется не по принципу минимальных привилегий, а «для удобства» — полный доступ к средам разработки, базам данных, административным интерфейсам. Такие уровни доступа дают огромные возможности как для легитимной работы, так и для утечки.

- **Общие ключи, VPN, SSH**

Типичная практика — одна учётная запись или один ключ доступа на всю команду подрядчика. При увольнении одного специалиста пароль или ключ часто остаются без изме-

нений. В случае компрометации отследить виновника практически невозможно.

Даже если используются более безопасные методы, такие как SSH с ключами, компании редко реализуют полноценную систему управления этими ключами: ротация, логирование, аудит — всё это делается нерегулярно или только «на бумаге».

Реальные инциденты: утечки данных через подрядчиков и сопутствующий ущерб

Практика показывает, что именно через внешние подрядные структуры злоумышленники нередко получают доступ к критически важной информации. Вот реальные кейсы

НА БУМАГЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРУПНЫХ КОМПАНИЯХ ВЫГЛЯДИТ ВНУШИТЕЛЬНО

Человеческий фактор: низкая мотивация, текучка, субподряд

Аутсорсеры, особенно на нижнем уровне, редко вовлечены в культуру безопасности компании-заказчика. Они не чувствуют ответственности за данные, не понимают последствий и часто работают «по шаблону». У них может не быть достаточной квалификации.

Дополнительно усиливают риски:

- Текучка кадров в аутсорсинговых компаниях — человек сегодня работает, завтра уходит, но доступы остаются.
- Низкая мотивация — подрядчики заинтересованы в скорости выполнения задачи, а не в защите данных.
- Субподряд — если задача передаётся третьим сторонам, это создаёт слепую зону для основного заказчика: кто на самом деле работает с его данными, уже неясно.

таких утечек.

Revolut: компрометация через человеческий фактор

В сентябре 2022 года финтех-компания Revolut сообщила об инциденте безопасности. Были скомпрометированы персональные данные более 50 000 клиентов. По официальной информации, утечка произошла в результате атаки с использованием социальной инженерии, направленной на одного из сотрудников или подрядчиков из клиентской поддержки.

В результате несанкционированного доступа были раскрыты имена пользователей, электронные адреса, номера телефонов, адреса проживания и в отдельных случаях — сведения о платёжных картах. Revolut подчеркнула, что инцидент не повлиял на финансовые операции, однако последствия потребовали

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

В современном бизнесе больше не существует четкого периметра защиты

Пётр Сухоруких, предприниматель, эксперт по антикризисному PR, основатель международного агентства цифровой репутации «Невидимка»

Представьте, что вы потратили миллионы на строительство неприступной цифровой крепости. У вас высокие стены — файрволлы последнего поколения. У вас бдительная стража — собственный штат специалистов по безопасности. У вас сложные замки — многофакторная аутентификация. А потом вы нанимаете садовника для ухода за газоном, отдаете ему ключ от боковой калитки и не спрашиваете, куда он его кладет на ночь. Абсурд? Именно так сегодня выглядит информационная безопасность 9 из 10 крупных компаний, активно привлекающих внешних исполнителей.

Меня зовут Петр Сухоруких, и моя работа — спасать репутацию компаний после катастроф. Я могу сказать вам с полной уверенностью: самые разрушительные утечки данных, которые мне приходилось разгребать, происходили не из-за гениальных атак на ядро корпоративной сети. Они просачивались через ту самую калитку — через ноутбук дизайнера-фрилансера, через плохо настроенный сервер маркетингового агентства, через сотрудника внешнего колл-центра.

В современном бизнесе больше не существует четкого периметра защиты. Он простирается до каждого партнера, которому вы доверяете свои данные. И главный парадокс заключается в том, что, передавая задачи

внешним исполнителям ради эффективности, вы импортируете риски, которыми зачастую совершенно не управляете. Вы можете делегировать разработку, маркетинг или бухгалтерию, но вы никогда, ни при каких обстоятельствах, не сможете делегировать и ответственность.

неса. А у них в штате три веселых дизайнера и один аккаунт-менеджер. Никакого выделенного специалиста по ИБ, пароли от CRM хранятся в общем файле в облаке, а сотрудники регулярно работают из кафе с публичным Wi-Fi. Они — идеальная точка входа для злоумышленника.

ВЫ ПОТРАТИЛИ МИЛЛИОНЫ НА СТРОИТЕЛЬСТВО НЕПРИСТУПНОЙ ЦИФРОВОЙ КРЕПОСТИ. У ВАС ВЫСОКИЕ СТЕНЫ — ФАЙРВОЛЛЫ ПОСЛЕДНЕГО ПОКОЛЕНИЯ. У ВАС БДИТЕЛЬНАЯ СТРАЖА — СОБСТВЕННЫЙ ШТАТ СПЕЦИАЛИСТОВ ПО БЕЗОПАСНОСТИ. У ВАС СЛОЖНЫЕ ЗАМКИ — МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ. А ПОТОМ ВЫ НАНИМАЕТЕ САДОВНИКА ДЛЯ УХОДА ЗА ГАЗОНОМ, ОТДАЕТЕ ЕМУ КЛЮЧ ОТ БОКОВОЙ КАЛИТКИ И НЕ СПРАШИВАЕТЕ, КУДА ОН ЕГО КЛАДЕТ НА НОЧЬ. АБСУРД? ИМЕННО ТАК СЕГОДНЯ ВЫГЛЯДИТ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 9 ИЗ 10 КРУПНЫХ КОМПАНИЙ, АКТИВНО ПРИВЛЕКАЮЩИХ ВНЕШНИХ ИСПОЛНИТЕЛЕЙ

Точки входа: где именно протекает ваш корабль?

Давайте прекратим говорить абстрактно и посмотрим на конкретные, до боли знакомые примеры уязвимостей, которые создает привлечение сторонних команд.

«Креативное» маркетинговое агентство

Вы передаете им свою базу клиентов для email-рассылки — святая святых вашего биз-

Надежная юридическая фирма на подряде

Маленькая, уважаемая компания, которая ведет ваши самые сложные дела. Вы отправляете им по почте сканы договоров, коммерческие тайны, M&A-документацию. А у них вся инфраструктура — это три ноутбука и обычный роутер из магазина электроники, который не обновлялся с момента покупки.

Команда разработчиков на аутстаффе

Вы наняли талантливых программистов,

которые пишут вам код нового продукта. Но они работают из разных стран, с личных компьютеров, на которых кроме вашей интеллектуальной собственности установлены торрент-клиенты, компьютерные игры и десятки других приложений сомнительного происхождения.

САМЫЕ РАЗРУШИТЕЛЬНЫЕ УТЕЧКИ ДАННЫХ, КОТОРЫЕ МНЕ ПРИХОДИЛОСЬ РАЗГРЕБАТЬ, ПРОИСХОДИЛИ НЕ ИЗ-ЗА ГЕНИАЛЬНЫХ АТАК НА ЯДРО КОРПОРАТИВНОЙ СЕТИ. ОНИ ПРОСАЧИВАЛИСЬ ЧЕРЕЗ ТУ САМУЮ КАЛИТКУ — ЧЕРЕЗ НОУТБУК ДИЗАЙНЕРА-ФРИЛАНСЕРА, ЧЕРЕЗ ПЛОХО НАСТРОЕННЫЙ СЕРВЕР МАРКЕТИНГОВОГО АГЕНТСТВА, ЧЕРЕЗ СОТРУДНИКА ВНЕШНЕГО КОЛЛ-ЦЕНТРА

Системный администратор-фрилансер

Вы наняли его для настройки облачного хранилища. Он сделал свою работу и ушел. Но он допустил одну маленькую ошибку в конфигурации, из-за которой ваша база данных оказалась в публичном доступе. А вы узнали об этом из новостей, когда информация уже утекла.

Цепь доверия: как взять подрядчиков под контроль

Перестать работать со сторонними командами — не вариант. Научиться управлять их рисками — единственный путь. Это не требует огромных вложений, это требует системного управленческого подхода.

Шаг 1. Due diligence «под микроскопом»

Прежде чем подписать договор, вы должны провести аудит безопасности партнера так же тщательно, как финансовый аудит. Запросите их внутренние регламенты. Узнайте, как они обучают персонал, как управляют доступами, как реагируют на инциденты. Если в ответ вы слышите молчание или невнятное мычание — это красный флаг. Отсутствие формализованных политик в этой сфере — гарантия будущих проблем.

Шаг 2. Контракт как ваше главное оружие

Ваш стандартный договор на оказание услуг здесь не подойдет. В соглашении с любым подрядчиком, имеющим доступ к вашим данным, должен быть отдельный, детально проработанный раздел, посвященный защите информации.

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Тренды в сегменте пожарной безопасности в 2025 году

Игорь Кудинов, руководитель отдела развития отраслевых решений и интеграций Okdesk

Отрасль систем и средств пожарной безопасности – одна из самых устойчивых к изменениям, где вектор развития почти полностью определяется государственными нормами и требованиями. А если учитывать, что на кону таких изменений человеческие жизни, то становится понятно, почему нововведения внедряются неспешно – это большая ответственность.

Тем не менее, собирая обратную связь и анализируя кейсы наших клиентов, мы обратили внимание на тенденции, которые оказывают всё более заметное влияние на отрасль. Хотя эти тенденции пока не стали массовыми, их проявление уже заслуживает внимания тех, кто интересуется трендами и перспективами. Безусловно, такая консервативная отрасль меняется только под воздействием государственных регуляторов, но присматриваться к ним нужно начинать уже сейчас.

Электронный документооборот

Эксплуатация систем противопожарной защиты традиционно связана с большим объёмом однотипной документации, сопровождающей каждый этап работ — от ввода в эксплуатацию до технического обслуживания. Среди экспертов давно стала очевидной необходимость автоматизировать создание типовых документов, особенно тех, содержание которых стандартизировано ГОСТами и практически не изменяется в зависимости

от объекта и обслуживаемого оборудования или системы – будь то акты, дефектные ведомости или журналы эксплуатации.

Однако несмотря на востребованность самой идеи, повсеместное внедрение электронного документооборота в отрасли пока не состоялось, хоть подчас и встречается. И на то есть свои причины:

1. **Юридическая**. В настоящее время не все отраслевые национальные стандарты допускают замену привычных бумажных журналов эксплуатации на цифровые. Если одни ГОСТы уже разрешают ведение журнала эксплуатации в электронном виде, то в других содержатся подробные описания по ведению бумажного журнала, включая требования к подшивке документов.

2. **Практическая**. Обслуживающие компании, как правило, заключают комплексные договоры на все системы противопожарной защиты объекта. Одновременное ведение журнала на часть систем в электронном виде, а на другие в бумажном не является удобным. В этой связи большинство предпочитает оставаться приверженными к классическому варианту документооборота.

3. **Экономическая**. В долгосрочной перспективе цифровизация процессов снижает операционные расходы и обходится дешевле и заказчику, и исполнителю. Однако переходный период, когда от бумаг ещё не отказались, а на электронный документооборот ещё полностью не перешли, сопровождается дополнительными расходами для обеих сторон.

4. **Инфраструктурная**. На данном этапе в индустрии нет универсальной и официально признанной цифровой среды, где заказчик и исполнитель могли бы безопасно вести электронный документооборот без опасений юридических рисков и претензий со стороны контролирующих органов.

5. **Организационная**. Переход на электронные рельсы требует перестройки взаимодействия между специалистами обеих сторон, а также пересмотра ролей, инструкций и систем внутреннего контроля. Такие кардинальные изменения неизбежно потребуют дополнительного обучения персонала и повышения его квалификации.

Тем не менее, интерес со стороны рынка заметен – потребность в электронном взаимодействии есть как у заказчика, так и у исполнителя. Учитывая этот факт, можно предположить, что в будущем мы увидим изменения в законодательной базе, способные сделать электронный документооборот новым отраслевым стандартом.

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

От Excel к ИИ: Новые возможности IT для революции в закупках и повышении эффективности бизнеса

Левон Мусоян,
Основатель МБС (mbsgroup.ru) — эксперты в автоматизации бизнеса с 2003 года.
Специализация:
• Разработка AI-решений
• Разработка BPM, HelpDesk, CRM, SRM, HRM-систем
• Золотой партнер Битрикс24

Представьте себе утро обычного менеджера по закупкам на крупном промышленном предприятии. Его рабочий стол завален бумагами, на мониторе мелькают десятки открытых Excel-таблиц, а почтовый ящик полон запросов. Он устал от бесконечных согласований, хождения по кабинетам за подписями и поездок на склад за документами. Он — оператор, аналитик, бухгалтер, логист и переговорщик в одном лице, и все это в условиях постоянного цейтнота. Знакомая картина?

Закупочная деятельность, которую часто недооценивают, на самом деле является важным рычагом для роста прибыли или источником значительных, но часто незаметных потерь.

Именно в ней кроется ключ к эффективной оптимизации расходов, надежному управлению рисками и повышению полной прозрачности компании.

Для многих предприятий это до сих пор сложный «черный ящик», где процессы ведутся «по-старинке» — через бесконечные таблицы Excel, электронную почту и ручной сбор подписей.

Но сегодня, передовые компании, стремящиеся к масштабированию и максимальной эффективности, активно обращают внимание на новые возможности IT. И в авангарде этой

трансформации стоят специализированные ИИ-агенты, способные вдохнуть новую жизнь в закупочные процессы. Они не просто автоматизируют сценарии. Работая в единой интеллектуальной SRM-системе, эти агенты переосмысливают суть взаимодействия с поставщиками, превращая рутину в управляемый, прозрачный и, что самое главное, прибыльный процесс.

«Старая гвардия»: Почему традиционные закупки тормозят ваш бизнес

Мы уже представили утро менеджера по закупкам. А теперь давайте углубимся в то, почему эти, казалось бы, привычные процессы на самом деле являются скрытым тормозом для всего бизнеса, ежемесячно «сжигая» миллионы рублей и ценное время ваших экспертов в закупках.

Рутина и хаос: Потоп в Excel и почте

Вспомните последнюю крупную закупку, скажем, на 1500 позиций для оснащения нового цеха или строительного объекта. Или вспомните, сколько дней ушло на сведение разрозненных заявок от разных подразделений. Как часто вы обнаруживали, что две заявки на, казалось бы, одинаковый «гидрораспределитель Р80» на самом деле содержат разные спецификации или артикулы, и приходилось начинать всё сначала?

Ваши менеджеры вручную фильтруют строки по ключевым словам, пытаются угадать категорию, копируют и вставляют данные в десятки новых файлов для разных отделов. Они постоянно переключаются между окнами, рискуя допустить ошибку в артикуле или количестве. По оценкам, до 30% рабочего времени квалифицированного закупщика уходит на рутинные операции, которые можно автоматизировать. Переговоры с ключевыми поставщиками отложены на «потом», а мотивация падает с каждым скопированным рядом. По сути, компания использует квалифицированного специалиста как оператора ввода данных. Это не просто потеря времени — это прямые убытки от простоя оборудования и задержек запуска производства. Каждая такая ‘переработка’ заявки или исправление ошибки может стоить компании от 5 000 до 15 000 рублей на внутренних издержках.

ДЛЯ МНОГИХ ПРЕДПРИЯТИЙ ЭТО ДО СИХ ПОР СЛОЖНЫЙ «ЧЕРНЫЙ ЯЩИК», ГДЕ ПРОЦЕССЫ ВЕДУТСЯ «ПО-СТАРИНКЕ» — ЧЕРЕЗ БЕСКОНЕЧНЫЕ ТАБЛИЦЫ EXCEL, ЭЛЕКТРОННУЮ ПОЧТУ И РУЧНОЙ СБОР ПОДПИСЕЙ

«Ценовая рулетка»: Скрытые переплаты и упущенная выгода

Вы годами работаете с одним и тем же поставщиком гофрокартона. «Надежный партнер», «проверенное качество». Но знает ли ваш менеджер, что на рынке уже полгода есть альтернатива, которая предлагает аналогичный объем на 10-12% дешевле? Это новое предприятие, построенное в рамках целевых программ развития региона, с новым технологиями и оптимизированным производством. Без объективной системы сравнения цен, основанной на актуальных данных, вы просто

«сжигаете» часть бюджета, не подозревая об этом. Эти ‘незаметные’ переплаты могут достигать сотен тысяч и даже миллионов рублей в год для крупного предприятия.

А может быть, вы закупаете металлопрокат для производства. Рыночные цены на него колеблются ежедневно. Без автоматического мониторинга вы реагируете на изменения постфактум, упуская возможность заключить контракт на 10-15% выгоднее в момент краткосрочного снижения цен. Например, задержка в принятии решения всего на несколько дней при закупке критически важного сырья может привести к потере 10-15% потенциальной экономии, что в масштабах годового объема выливается в десятки миллионов. Каждый день такой задержки — это прямая потеря маржинальности вашей конечной продукции. Это как играть в слепую, когда у вас есть все карты, но вы их не видите.

«Бутылочные горлышки» и паралич: Зависимость от незаменимых

В каждом отделе есть один-два «звездных» сотрудника, которым по умолчанию отдают все самые сложные и важные закупки. В итоге ведущий специалист завален работой: он одновременно ведет три тендера, согласовывает договор на поставку уникального оборудования и пытается найти нового поставщика. Сроки по его задачам начинают сдвигаться, что ставит под угрозу запуск новой производственной линии. Простой производственной линии из-за отсутствия критически важной детали может обходиться компании в сотни тысяч или даже миллионы рублей в день. В это же время трое других менеджеров в отделе занимаются рутинными закупками или вовсе имеют неполную загрузку. По данным исследований, более 60% компаний сталкиваются с задержками в закупках из-за неэффективного распределения задач.

А что происходит, когда ваш главный специалист по закупкам импортной электроники, который в одиночку вел всех азиатских поставщиков, уходит в двухнедельный отпуск? В этот момент приходит срочный запрос на комплектующие для экспортного контракта. Никто в отделе не знает специфику работы с этими поставщиками. Руководитель вынужден либо ждать возвращения эксперта, срывая сроки контракта, либо пытаться найти решение в авральном режиме, рискуя выбрать не того поставщика и переплатить. Компания не только теряет в эффективности, но и создает прямые риски для ключевых бизнес-процессов, делая их зависимыми от одного перегруженного человека.

«Цифровая гвардия»: Как ИИ-агенты меняют правила игры

Мы подробно разобрали, почему традиционные подходы к закупкам становятся тормозом для бизнеса. Но что, если мы скажем, что этот «черный ящик» можно не просто открыть, а превратить в прозрачный и высокоэффективный механизм? Представьте, что каждый ваш специалист по закупкам имеет персонального, высокоэффективного цифрового ассистента, работающего 24/7. Это не просто скрипт, а интеллектуальная система, которая делает общения и понимает контекст, анализирует семантику и учится на ваших данных.

ИИ-агенты раскрывают свой потенциал, работая в рамках единой интеллектуальной SRM-платформы, которая становится фундаментом для формирования, обогащения и оперирования данными. Они — те самые «цифровые помощники», которые превращают хаос в порядок, а затраты — в прибыль.

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

SWIFT, крипта и альтернативы: как переводят деньги в Азию в 2025 году

Руслан Сагинбаев. Эксперт, специалист в области международной торговли с акцентом на Китай и Индию

За последние годы платёжные маршруты между Россией и азиатскими странами претерпели заметные изменения на фоне геополитических ограничений. В таких условиях бизнесу приходится адаптироваться, искать надежные и безопасные способы расчётов. Какие схемы сегодня действительно работают, какие страны выступают в роли посредников, а какие варианты вызывают проблемы при растаможке? Руслан Сагинбаев, специалист в области международной торговли с акцентом на Китай и Индию, рассказал об актуальных способах оплаты за товары из России в страны азиатского региона — Китай, Сингапур, Малайзию, Вьетнам и Южную Корею.

Банковский перевод в юанях

На сегодняшний день наиболее распространённой и проверенной схемой остаётся оплата в китайских юанях. Это полностью легальный и прозрачный способ расчётов, который активно используют многие продавцы.

Юань спокойно отправляется из России через ВТБ. Многие компании из Вьетнама и Гонконга имеют подразделения в Китае и счета, открытые в шанхайском отделении ВТБ. Это позволяет им беспрепятственно принимать оплату в юанях.

Такая модель оплаты удобна тем, что не требует сложных посреднических структур или дополнительных операций. В условиях, когда

традиционные международные платёжные каналы ограничены или вовсе заблокированы, переход на расчёты в юанях оказался для многих бизнесов своевременным решением.

Оплата через банки третьих стран дружественных государств

Другой распространенный вариант — использование банков в странах СНГ (Казахстан, Беларусь, Кыргызстан, Армения). Однако здесь могут возникать сложности. Например, в Китае в последние месяцы наблюдаются проблемы с платежами, поступающими через банки Кыргызстана. Тем не менее, во Вьетнам деньги через такие каналы обычно проходят, хотя стоит учитывать наличие комиссий, в том числе скрытых и агентских.

При всей гибкости схемы она требует повышенного внимания к деталям, ведь правила внутри стран могут меняться, банки могут вводить внутренние ограничения, а расчётные комиссии иногда оказываются выше ожидаемых. Поэтому компании, использующие этот способ, всё чаще прибегают к юридическому и финансовому аудиту таких операций заранее.

Платежи через ОАЭ и Турцию

Наиболее стабильной и надёжной схемой на сегодняшний день считаются расчёты через банки в Объединённых Арабских Эмиратах и Турции. Эти страны предоставляют возможность проводить международные переводы без ограничений, и на практике эта схема работает без сбоев.

Российская компания может оплатить товар либо напрямую агенту, либо перевести средства на собственный счёт, открытый в Объединённых Арабских Эмиратах или Турции. Далее турецкая или арабская сторона осуществляет платёж в пользу поставщика в стране азиатского региона. Такая схема официально разрешена. Российская таможня принимает документы, подтверждающие оплату через агентов, и даёт разрешение на растаможку.

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Инновационные Стартапы

Клементьев

Экспертиза стартапов проводится институтами развития и инвесторами в целях оценки соответствия инновационного проекта определенным условиям предоставления поддержки, в том числе финансирования. Для осуществления экспертизы привлекаются экспертные организации и (или) частные эксперты, которые имеют высокие компетенции и практический опыт в предметной области реализации стартапа. Привлечение экспертов вызвано несколькими причинами. Во-первых, у институтов развития и инвесторов не всегда достаточно собственных ресурсов для проведения экспертизы. Во-вторых, привлекая стороннего эксперта обеспечивается «независимость» экспертизы ввиду незаинтересованности эксперта в результате оценки проекта. В-третьих, на эксперта ложится ответственность за результат экспертизы в части добросовестности формирования профессионального мнения, что позволяет разделить с ним ответственность за принятие решения.

Экспертиза стартапа независимо от условий программы поддержки обычно делится на два этапа: оценка на соответствие формальным требованиям, экспертиза «по существу». Причем формальная экспертиза часто не выделяется в отдельный этап и выполняется автоматически при подаче материалов заявителем в электронном виде. Формальными основаниями для отказа может стать не только несоответствие заявки требованиям программы поддержки, причем как в части характеристик самой организации (например, отсутствие регистрации в регионе, наличие

зарубежных собственников, неподходящий основной код экономической деятельности), так и в части показателей проекта (например, отсутствие необходимых промежуточных результатов, недостаточность собственного финансирования, невостребованность разработки), но и отсутствие достаточной для проведения экспертизы документации. Формальная экспертиза имеет цель отсеять заведомо отказные заявки, чтобы не тратить на них время профильных экспертов.

Экспертиза по существу имеет цель оценить эффективность стартапа в рамках программы поддержки. Для этого проект анализируется по ряду критериев. Обычно в их состав входят: актуальность, теоретическая реализуемость, наличие конкурентных преимуществ и достаточных ресурсов для реализации проекта. Традиционно применяется два подхода при принятии решения о поддержке стартапа. В первом случае по каждому рассматриваемому критерию заявке присваиваются количественные оценки, сумма которых для положительного решения о поддержке проекта должна превысить заданное минимальное значение. Например, такой подход применяется Фондом содействия инновациям (ФСИ), Фондом инфраструктурных и образовательных программ (ФИОП), Инновационным научно-технологическим центром (ИНТЦ) МГУ «Воробьевы горы». Во втором случае проект поддерживается, если каждый из анализируемых критериев или определенное их количество оценено положительно. Примером такой оценки становятся экспертизы для Фонда «Сколково», Московского инновационного кластера.

Необходимо подчеркнуть, что результат экспертизы проекта часто зависит от качества подготовки заявки и сопутствующих материалов. Поэтому важно принять правильное управленческое решение об исполнителях, задействовав необходимый персонал. Для большинства программ поддержки заявки можно рассмотреть с трех ракурсов: технического, экономического и правового. Естественно, отсутствие одной компетенции и (или) избыток другой могут привести к отрицательному результату рассмотрения проекта. Например, увлеченный инженер может развить описание преимуществ технической реализации в ущерб обоснованию экономической эффективности проекта или сбору необходимого пакета правовых документов. Кроме того, в проектной команде должен быть ответственный за формирование пакета документов сотрудник, который обладает предметными знаниями. Иначе возможны ситуации, когда не рассчитаны силы, и при возникновении дополнительных вопросов со стороны экспертов сложно оперативно получить исчерпывающий ответ. Следует отметить и существование обратной тенденции. Появились технологические компании, которые отладили у себя процесс подготовки заявок и материалов для получения поддержки и, учитывая во многом формальный подход к отбору и оценке заявок, стараются получить максимально возможное количество преференций.

2025 год ознаменовался изменением ситуации на российском рынке финансовой поддержки стартапов. Это обусловлено и изменением приоритетных государственных задач, и повышением временной стоимости денег. Как бы то ни было, тренд на охват максимальной аудитории технологического предпринимательства, в частности наблюдавшийся в Москве, сменился на точечное финансирование определенных направлений. Но этот процесс мало затронул нефинансовую поддержку, наиболее выраженную в предоставлении налоговых льгот резидентам технопарков и специальных экономических зон, что объясняется их появлением темпами, опережающими рост инновационных компаний.

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

От Excel к Word: стратегия роботизации корпоративной отчетности

Оптимизация процессов подготовки документов с помощью средств малой автоматизации на примере программы «Excel2Word Report Master»

Роман Мотин, корпоративный финансовый консультант, автор приложения «Excel2Word Report Master»

Актуальная проблема: скрытые издержки ручной подготовки отчетов

Подготовка аналитической, финансовой и производственной отчетности — неотъемлемая часть управленческих процессов в любой современной организации. Однако, несмотря на растущий уровень цифровизации, ключевой этап формирования итоговых документов — перенос структурированных данных из сред для расчетов (например, Microsoft Excel) в текстовые редакторы (Microsoft Word) — во многих компаниях до сих пор выполняется вручную.

Этот технологический разрыв порождает значительные скрытые издержки. Согласно исследованию компании Automation Anywhere, офисные сотрудники тратят более трех часов в день, или 40% своего рабочего времени,

на рутинные административные задачи, которые поддаются автоматизации. Операции ручного копирования и вставки («копи-паст») не только приводят к непроизводственным потерям рабочего времени, но и являются основной причиной ошибок: опечаток, переноса неправильных данных или нарушения форматирования. В результате компания несет финансовые и репутационные риски, а ценные специалисты тратят время на механическую работу.

Малая автоматизация как ключ к эффективности: обзор «Excel2Word Report Master»

Традиционные подходы к автоматизации часто ассоциируются с внедрением сложных и дорогостоящих ERP-систем. Однако для решения локальных, но критически важных задач, эффективным решением выступают средства малой автоматизации (Robotic Process Automation, RPA).

Программный продукт «Excel2Word Report Master» является представителем этого класса решений. Это специализированный инструмент, разработанный для полной автоматизации процесса генерации отчетов в MS Word или PDF на основе данных из MS Excel.

Ключевые возможности программы

1) **Пакетный перенос данных**: Автоматическая обработка любого количества таблиц и графиков из файла Excel в документ Word.

2) **Интеллектуальная верстка «длинных» таблиц**: Программа корректно переносит таблицы с большим количеством столбцов, автоматически распределяя их по страницам формата А4 с сохранением читаемости.

3) **Динамическое обновление**: При изменении данных в исходном Excel-файле отчет можно полностью переформировать одной кнопкой, гарантируя его актуальность.

Программа реализована на базе стандартных компонентов Microsoft Office (VBA в MS Access), что обеспечивает простоту внедрения и не требует закупки дополнительного ПО.

Методология работы: сценарный подход и нормализация данных

В основе работы «Excel2Word Report Master» лежат два ключевых принципа, которые устраняют саму причину ошибок и неэффективности.

1. **Сценарно-ориентированный подход**. Вместо ручного копирования используется предопределенный сценарий — редактируемый файл-шаблон в формате Excel. В этом файле описывается вся логика будущего отчета: расположение исходных данных, очередность таблиц и графиков, параметры форматирования, заголовки и нумерация. Такой подход полностью отделяет данные от их представления и элиминирует ручной труд. Организация может создать библиотеку сценариев для всех видов регулярной отчетности.

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Искусственный интеллект остается недосягаемой мечтой для большинства российских компаний

Comindware®

Промежуточные результаты III Всероссийского опроса по цифровой трансформации показали: 60% руководителей считают ИИ главным трендом, но не могут его внедрить из-за разрозненности IT-систем.

Российский бизнес столкнулся с технологическим парадоксом

Опрос, который проводится компанией Comindware и Artezio (ГК Ланит), при поддержке ассоциаций Руссофт и BPM-профессионалов, показывает, что российский бизнес столкнулся с технологическим парадоксом: 60% компаний признают искусственный интеллект ключевым трендом развития своей отрасли, однако только 20% реально используют ИИ-технологии для обработки данных.

Главной причиной отставания стала цифровая разрозненность — более 70% компаний не имеют единой цифровой среды, необходимой для эффективной работы современных интеллектуальных систем.

Исследование выявило критическую проблему российского бизнеса: подавляющее большинство компаний работают с набором несвязанных между собой систем. Только у 40% компаний большинство систем интегрированы между собой, при этом менее

50% сотрудников в большинстве организаций имеют доступ к единому цифровому рабочему пространству. Почти 60% опрошенных компаний называют сложность интеграции существующих систем главным препятствием для цифровизации.

> *«Без единой цифровой среды внедрение искусственного интеллекта превращается в попытку запустить суперкомпьютер без операционной системы»**, — отмечает Игорь Простоквашин ведущий аналитик Comindware.** *«ИИ требует качественных, структурированных данных из всех бизнес-процессов, а в условиях информационных «островов» это невозможно. Мы видим, что компании буквально застряли между пониманием важности технологии и невозможностью ее внедрить из-за фрагментированной IT-инфраструктуры»**.

Отсутствие единой цифровой инфраструктуры приводит к колоссальным потерям эффективности. Исследование показало, что в среднем 42,5% рабочего времени в российских компаниях уходит на рутинные задачи. Это означает, что из 40-часовой рабочей недели 17 часов сотрудники тратят на операции, которые могли бы выполнять интеллектуальные системы. При этом парадоксально, что уровень цифровой грамотности сотрудников достаточно высок — в 40% компаний более 70% персонала обладают необходимыми навыками для работы с современными цифровыми инструментами. Проблема не в людях, а в отсутствии интегрированной технологической платформы.

Анализ используемых технологий демонстрирует консервативный подход российского бизнеса к выбору инструментов обработки данных. Сорок процентов компаний используют традиционные системы управления базами данных (СУБД), почти 20% внедрили решения бизнес-интеллекта (BI) и работают с облачными технологиями, и только 20% компаний из участников всероссийского опроса реально использует искусственный интеллект.

> *«Особенно настораживает инвестиционная осторожность в отношении создания базовой инфраструктуры для ИИ»*, — продолжает Простоквашин. *«Исследование показало, что 40% компаний вообще не планируют инвестиции в создание единой цифровой среды, еще 40% обсуждают такую возможность, но не считают ее приоритетной. Фактически, только одна из пяти компаний имеет конкретные планы по созданию интегрированной IT-инфраструктуры. При этом, что интересно, критерии успеха цифровизации у большинства компаний связаны именно с теми преимуществами, которые дает искусственный интеллект: увеличение продуктивности называют 40% респондентов, сокращение времени выполнения задач — также 40%, а увеличение доли рынка — 20%»*.

По словам эксперта, российские компании оказались в своеобразной ловушке: они понимают важность искусственного интеллекта, видят его потенциал, но не готовы инвестировать в создание необходимой инфраструктуры. Это создает риск технологического отставания от глобальных конкурентов, которые уже активно используют ИИ для оптимизации всех бизнес-процессов.

Внедрение ИИ

Исследование также выявило интересную закономерность в отраслевом разрезе. Компании IT-сектора, составившие 60% выборки, демонстрируют более высокую готовность к внедрению ИИ, но даже среди них реальное использование интеллектуальных технологий

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

TOPOKRATYA® – глубинная философия власти и влияния, синтезирующая бизнес–стратегии, политическую психологию и экосистемное мышление лидеров

В последнее время все чаще в бизнесе встречается словосочетание топократическая культура бизнеса, топократическое управление.

Появилось много адептов доктрины Топократия®, однако несведущим очень сложно понять, что это такое.

БИЗНЕС ИДЕЙ БИЗНЕС РЕШЕНИЯ БИЗНЕС ТЕХНОЛОГИИ БИЗНЕС ПРОЦЕССЫ
УПРАВЛЕНИЕ ПЕРСОНАЛОМ
www.TOP-PERSONAL.ru

Неужели в системе управления бизнесом можно придумать что–то новое, более эффективное, чем то, что уже давным–давно изучено и применено?

Сегодня мы встретились с автором Доктрины Топократия® — экосистемным подходом в управления бизнесом, доктором психологических наук, основателем Академии ТОП-Менеджмента «АТОМ», Андреем Курчем.

Андрей Курч

Давайте начнем с Вашего опыта и вашей Академии ТОП Менеджмента «АТОМ». Расскажите, чем Вы занимаетесь и какие направления у Вас есть?

— Прежде всего, хочу сказать, что мое первое высшее образование — медицинское, со специализацией в кардиологии и реаниматологии. В общей сложности я

Max стал обязательным каналом для электронной подписи через «Госключ»

Источник: https://m.dzen.ru/news/story/9d187d7b-ecc0-59b6-9e6b-6c638338fb5a?story=4036f81b-de3b-57fa-a6a7-5bd4b7b2d172&share_from=yastart&share_to=link

Евгений Шуваев, Юридическая фирма «Кирьяк и партнёры», ведущий юрист, kiryak.ru

В СМИ появилась информация о предстоящих изменениях в формате работы с электронной подписью. В ближайшее время физические лица, юридические лица и индивидуальные предприниматели смогут подписывать документы с помощью усиленной квалифицированной или усиленной неквалифицированной электронной подписи, полученной через приложение «Госключ», исключительно через мессенджер Max.

Инициатива связана с тем, что национальный мессенджер должен объединить под собой функционал отечественных сервисов, предоставляющих государственные, финансовые и коммерческие услуги. По мнению разработчиков, единый мессенджер обеспечит гарантию безопасности сделок и упростит использование систем электронной подписи.

Для частных лиц, использующих усиленную неквалифицированную электронную подпись, будет доступна возможность получения сведений об ИНН, подачи декларации по форме 3-НДФЛ и заявления на возмещение убытков после ДТП по ОСАГО.

Для получения расширенного спектра

возможностей пользователю потребуется подтвердить свою учетную запись на портале «Госуслуги», предоставив персональные данные и подтвердив биометрию. После подтверждения учетной записи станет возможным оформление усиленной квалифицированной электронной подписи. Это откроет доступ к таким функциям, как регистрация прав на объекты недвижимости и постановка их на кадастровый учет, подача заявлений на распределение пенсионных накоплений, получение выписок из личного кабинета налогоплательщика, исправление сведений в ЕГРН и подача заявлений на расторжение брака.

Данный перечень можно отнести к решению частных вопросов пользователей, поскольку он исключает взаимодействие с не государственными субъектами гражданских правоотношений.

Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru

ПОДАРОК!!!

Вместе с журналом «Делопроизводство» вы можете получать в подарок другие бизнес-издания Издательства: «Управление персоналом», «Мастер продаж», «Трудовое право», «Жилищное право», «Коммерческие споры», «Секретарское дело», «Клуб главных бухгалтеров», «Айти ревью», «Альманах» и пр.

Пришлите заявку на вацап 89263501881

Сварщика из Москвы втайне сделали главой двух фирм и повесили на него долги

Источник: https://dzen.ru/video/watch/6841a0c1ff170808791fce71

Елена Гладышева, Адвокат, Управляющий партнер Адвокатского бюро г. Москвы «РИ-консалтинг», член наблюдательного совета АНО «МОССТРАТЕГИЯ» (ранее МОСИНИЦИАТИВА), член МРО «Деловая Россия» www.ri-consulting.ru

Ситуация с использованием личных данных становится уже критичной. Возможно ли избежать, сложно ответить. Поскольку зачастую такое использование является тайным. Потерпевшему становится известным лишь по факту взыскания денежных средств с него на основании решения суда. Случаи эти совершенно уже не редки и, к сожалению, стали обыденными.

Какие необходимо предпринять действия, если факт уже произошел:

Вариант 1: с Вас взыскивают задолженность, к которой вы не имеет отношения

1. **Подать заявление о преступлении** (использовании персональных данных) и причиненном вреде, а также о факте незаконных действий по регистрации фиктивных компаний (это сфера уголовного права)
2. **Выявить все вынесенные решения о взыскани**и (судебные, а также в случае налоговых мер реагирования в виде инкассовых поручений по счетам потерпевшего).
3. **Подать заявления об оспаривании**

ранее вынесенных решений (если срок на оспаривание не истек) или заявление о пересмотре ранее вынесенных решений по вновь открывшимся обстоятельствам.

4. **В случае если судами будет отказано в пересмотре ранее вынесенных судебных решений** остается только инициирование процедуры личного банкротства, в рамках которой будут рассмотрены соответствующие ранее вынесенные решения и долги гражданина могут быть списаны (если не будет установлено фактов злоупотребления должника).

Вариант 2: по Вашим документам зарегистрированы компании, о которых Вам не известно и вы не являетесь управленцем этих компаний и/или собственником

1. **Необходимо подать заявления по форме Р34001.** Такое заявление подается через нотариуса. Нотариус заполняет соответствующую форму в Вашем присутствии на основании предоставленных Вами документов и в электронной форме направляет в регистрирующий орган для принятия процессуального решения «внесение записи о недостоверности сведений, содержащихся в ЕГРЮЛ»

2. **Далее все ранее описанные действия.**

Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru

Антон Лебедев, Адвокатская палата Санкт-Петербурга

Такая регистрация возможна с использованием цифровой подписи.

Каким образом у мошенников оказалась цифровая подпись нужно разбираться следствию.

Можно предположить, что это либо неосознанные действия самого потерпевшего, либо незаконные действия центра выдачи электронных подписей.

Часто потерявший аккредитацию центр продолжает свою «деятельность».

В случае признания гражданина потерпевшим все эти регистрации можно откатить в первоначальное состояние.

По практике, он скорее всего знает тех, кто это сделал.

Относительно долгов компании ему остается два варианта: откатывать регистрацию или объявить о собственном банкротстве.

Разумеется, все эти процедуры лучше делать при сопровождении юристом.

ПОДАРОК!!!

Вместе с журналом «Делопроизводство» вы можете получать в подарок другие бизнес-издания Издательства: «Управление персоналом», «Мастер продаж», «Трудовое право», «Жилищное право», «Коммерческие споры», «Секретарское дело», «Клуб главных бухгалтеров», «Айти ревью», «Альманах» и пр.

Пришлите заявку на вацап 89263501881

Путь руководителя

Базовые технологии повседневного управления

Дмитрий Виташов

Книга Дмитрия Виташова «Путь руководителя» — это идеальный вариант для тех, кто не готов тратить время на курсы, но хочет результат. Через истории и практичные алгоритмы она показывает, как ежедневные привычки формируют стиль управления и как перейти от «исполнителя с полномочиями» к настоящему лидеру и архитектору систем. Автор предлагает готовый набор действий, мышления и процессов, которые можно внедрить сразу после прочтения. Научитесь управлять системно, забудьте про хаос, авралы и бесконечные доделки.

ПРОЦЕСС 4. ПОДГОТОВКА ДОКУМЕНТОВ

Совещания — инструмент устной коммуникации, а документы — письменной. Собравшись вместе, можно решить проблему быстрее, чем в переписке. Однако совещания требуют подготовки, синхронизации графиков, времени и места для проведения, поэтому не по каждой проблеме они уместны — только по наиболее сложным и важным. По большинству вопросов проще обменяться документами, которые можно прочитать в удобное время. Да, так проблемы будут решаться дольше, но признаем: далеко не все вопросы требуют неотложного решения. Напротив, практика бесконечных совещаний приведет к дефициту времени и вызовет организационный коллапс.

Решать вопросы устно проще только на уровне отдела: все сотрудники перед глазами, их подходы синхронизированы, и собрать людей быстрее, чем писать документ. Однако и в этом случае есть риск. Устная коммуникация не оставляет видимых следов, а память — ненадежный носитель. Уже через несколько часов, а через 2–3 недели гарантировано, что необходимость написать и подписаться сильно дисциплинирует. С одной стороны, есть время подумать над каждым словом и точно выразить мысль, с другой — возникает понимание, что потом сложно будет сказать: «Я этого не говорил» или «Я не это имел в виду». Вот текст, вот подпись: ты же в здравом уме и твердой памяти писал? В разговорах

НРАВИТСЯ ИЛИ НЕТ, НО СИСТЕМНО ВЫСТРОЕННАЯ РАБОТА ТРЕБУЕТ ДОКУМЕНТАЛЬНОГО ОФОРМЛЕНИЯ. ДАЖЕ ЕСЛИ УВОЛЯТСЯ ВСЕ СОТРУДНИКИ, СИСТЕМУ МОЖНО БУДЕТ ВОССТАНОВИТЬ

у сотрудников возникнут свои версии, что было сказано и до чего договорились. Поэтому важные указания и алгоритмы работы следует оформлять документами и доводить с фиксацией ознакомления.

Любой документ ценен не сам по себе, а теми мыслями, которые он фиксирует. Более того, правильная подготовка документа позволяет рационально выстроить мыслительный процесс и, фиксируя пункт за пунктом, двигаясь по определенной структуре, продумать ситуацию со всех сторон. Зачастую главная польза появляется именно в ходе написания: рождаются и обдумываются правильные идеи, которые в итоге воплощаются в действия.

Например, оттачивание и согласование формулировок регламента необходимо не для закрытия поручения о его подготовке, а чтобы самим понять тонкие нюансы деятельности. Написание отчетов нужно не для удовлетворения вышестоящего руководства, а чтобы самим оценить: что планировали, что получилось, что не удалось, в чем проблемы и что делать дальше? Именно этот смысл документов должен видеть и транслировать подчиненным руководитель.

Дополнительный плюс документов в том, собеседники склонны вольно обращаться со словами, поэтому полезно дополнять устную коммуникацию письменной. Зачастую только начав согласовывать протокол, участники понимают, что ни до чего на самом деле не договорились.

Даже в небольшом отделе из пяти человек документирование кажется избыточным только до тех пор, пока не начнутся проблемы с единообразием в алгоритмах работы или вместе со всем накопленным опытом не уйдут старожилы. Руководитель департамента и выше игнорировать документирование не может в принципе. Нравится или нет, но системно выстроенная работа требует документального оформления. Даже если уволятся все сотрудники, систему можно будет восстановить.

Согласно ГОСТу[1], документ — это зафиксированная на носителе информация с реквизитами, позволяющими ее идентифицировать. Чаще всего в управлении используются письма, докладные записки, протоколы, акты с регистрационными номерами, бланками и подписями должностных лиц организации.

[1] ГОСТ Р 7.0.8–2013 «Делопроизводство и архивное дело. Термины и определения».

Документами могут признаваться и имейлы, поэтому к ним следует относиться так же серьезно. Именно электронными письмами, бездумно добавляя адресатов и нажимая кнопку «Ответить всем», можно потопить коллег в потоке ненужной информации. Если так происходит, то нужно ввести стандарт переписки, исключающей подобный спам, и добиться исполнения. Это позволит сотрудникам концентрироваться на своих задачах, а не постоянно отвлекаться, выискивая значимые крупицы информации в потоке писем.

Результатом подготовки документа является письменная фиксация (сохранение на будущее) или передача информации. В первом случае необходимо не только составить точный и понятный текст, но и внести его в систематический учет для быстрого поиска. Во втором же случае важно понимать, что информация не просто направляется, а передается с целью вызвать определенные действия или изменение позиции/понимания контрагента. Нельзя сводить процесс только к написанию текста, но и нет смысла слишком расширять его содержание — например, считать, что подготовка плана или стратегии заканчивается только их успешной реализацией.

Процесс подготовки документов состоит из трех шагов:

1. Определение цели документа.
2. Создание и утверждение документа.
3. Направление и сопровождение документа.

Обычно люди концентрируются только на втором шаге, и документ из инструмента превращается в самодостаточный предмет бюрократического искусства. Начинаются многочисленные шлифовки формы, выхолащивание содержания, размножение бумаг сверх необходимости и другие пороки, которые особенно заметны в крупных организациях. Встречали же файлы с названиями типа «Письмо..._17.doc» или «Докладная записка. Версия 25.docx»? Цифры отражают очередной номер редакционной правки, внесенной руководством.

Определение цели документа. Отвечая на вопрос «Зачем нужен этот документ и нужен ли вообще?», руководитель определяет, чего он хочет добиться с его помощью, от кого и в какие сроки. Возможно, адресаты должны ознакомиться с информацией и учитывать ее в работе; или предпринять желаемые действия; или в ответном письме выразить согласие с позицией. А возможно, надо просто зафиксировать решение, чтобы в дальнейшем проконтролировать его.

Формулируя цель, мы еще раз осмысливаем, какую проблему решаем и точно ли ее нужно решать документом, а не иным способом. Например, если на предыдущее письмо не получен ответ, то лучше не писать еще одно, а позвонить исполнителю или его руководителю. Заодно можно обсудить ожидаемую позицию и установить личный контакт, который всегда способствует решению вопросов. Лишним документом можно, напротив, вызвать негатив в свой адрес — контрагент расценит это как способ давления.

Обычно документы готовятся в адрес руководства (докладные записки), других подразделений (служебные записки), организаций или частных лиц (письма) или для фиксации информации по процессам (акты, протоколы и т.д.). Зачастую вопрос

«Писать или не писать?» уже решен в регламентах, и осознать цель нужно только для того, чтобы правильно выстроить содержание документа: развернутый ответ для убеждения или формальная отписка; фиксация конкретных решений или описание всего хода совещания; хронологическое описание событий или отражение фактов, аргументирующих конкретную позицию.

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

Изменения в законодательстве в сфере трудовых правоотношений

Татьяна Кочанова, юрист

Изменения в законодательстве в сфере трудовых правоотношений май 2025 года

Целый ряд актов, касающихся педагогических работников был разработан и принят с целью улучшения законодательного регулирования трудовых правоотношений данной категории работников:

— Приказ Минтруда России от 21.03.2025 N 136н «Об утверждении профессионального стандарта «Педагог профессионального обучения, среднего профессионального образования» Зарегистрировано в Минюсте России 25.04.2025 N 81971.

С 1 сентября 2025 г. вводится профессиональный стандарт «Педагог профессионального обучения, среднего профессионального образования»

Целью профессиональной деятельности данных специалистов является педагогическая деятельность в профессиональном обучении, среднем профессиональном образовании.

Приводится описание трудовых функций, устанавливаются требования к образованию и обучению, особые условия допуска к работе, другие характеристики.

Настоящий приказ действует до 1 сентября 2031 г.

— Приказ Минтруда России от 21.03.2025 N 137н «Об утверждении профессионального стандарта «Руководитель профессиональной

образовательной организации» Зарегистрировано в Минюсте России 25.04.2025 N 81970.

С 1 сентября 2025 г. вводится профессиональный стандарт «Руководитель профессиональной образовательной организации»

Целью профессиональной деятельности данных специалистов является управление профессиональной организацией и ее структурными подразделениями при реализации образовательных программ.

Приводится описание трудовых функций, устанавливаются требования к образованию и обучению, к опыту практической работы, особые условия допуска к работе, другие характеристики.

Настоящий приказ действует до 1 сентября 2031 г.

— Приказ Минпросвещения России от 04.04.2025 N 269 «О продолжительности рабочего времени (нормах часов педагогической работы за ставку заработной платы) педагогических работников организаций, осуществляющих образовательную деятельность по основным и дополнительным общеобразовательным программам, образовательным программам среднего профессионального образования и соответствующим дополнительным профессиональным программам, основным программам профессионального обучения, и о Порядке определения учебной нагрузки указанных педагогических работников, оговариваемой в трудовом договоре, основаниях ее изменения и случаях установления верхнего предела указанной учебной нагрузки» Зарегистрировано в Минюсте России 06.05.2025 N 82070.

Установлена продолжительность рабочего времени педагогов в школах и колледжах

Продолжительность рабочего времени или нормы часов педагогической работы за ставку заработной платы педагогическим работникам устанавливаются в зависимости от их должности и (или) специальности.

Так, в частности, продолжительность рабочего времени 36 часов в неделю устанавливается: старшим воспитателям организаций, осуществляющих образовательную деятельность по образовательным программам дошкольного образования и дополнительным общеобразовательным программам, а также домов ребенка, осуществляющих образовательную деятельность в качестве дополнительного вида деятельности; педагогам-психологам; социальным педагогам; педагогам-организаторам; мастерам производственного обучения; методистам и старшим методистам; советникам директора по воспитанию и взаимодействию с детскими общественными объединениями и др.

Кроме того, документом утвержден порядок определения учебной нагрузки педагогических работников организаций, осуществляющих образовательную деятельность по основным и дополнительным общеобразовательным программам, образовательным программам СПО и соответствующим дополнительным профессиональным программам, основным программам профессионального обучения, оговариваемой в трудовом договоре, основания ее изменения и случаи установления верхнего предела указанной учебной нагрузки.

Настоящий приказ вступает в силу 1 сентября 2025 года и действует до 1 сентября 2031 года.

— Приказ Минобрнауки России от 11.04.2025 N 335 «О продолжительности рабочего времени педагогических работников, отнесенных к профессорско-преподавательскому составу, и о порядке определения учебной нагрузки указанных работников, оговариваемой в трудовом договоре, основаниях ее изменения и случаях установления верхнего предела учебной нагрузки» Зарегистрировано в Минюсте России 06.05.2025 N 82069.

Установлена продолжительность рабочего времени педагогических работников, отнесенных к профессорско-преподавательскому составу

Закреплено, что продолжительность рабочего времени педагогических работников, отнесенных к профессорско-преподавательскому составу, составляет 36 часов в неделю.

Также утвержден порядок определения учебной нагрузки указанных педагогических работников, оговариваемой в трудовом до-

говоре, основания ее изменения и случаи установления верхнего предела учебной нагрузки.

В ТК РФ планируют закрепить дополнительные признаки трудовых отношений

(Проект Федерального закона «О внесении изменений в Трудовой кодекс Российской Федерации» (по вопросам определения характерных признаков трудовых отношений и наделения государственной инспекции труда правом на обращение в суд)» (не внесен в ГД ФС РФ)

Так, с учетом постановления Пленума Верховного Суда РФ от 29.05.2018 N 15, статью 15 Трудового кодекса предлагается дополнить, в частности, следующими характерными признаками трудовых отношений:

- устойчивый и стабильный характер отношений;
- подчиненность и зависимость труда;
- наличие дополнительных гарантий работнику;
- признание работодателем прав работника на еженедельные выходные дни и ежегодный отпуск;
- осуществление периодических выплат работнику, которые являются для него единственным и (или) основным источником доходов;
- предоставление инструментов, материалов и механизмов работодателем и др.

Кроме этого, планируется наделить государственную инспекцию труда правом обращаться в суд с требованием о признании отношений трудовыми, если работодателем в соответствии с предписанием не устранено нарушение, связанное с заключением гражданско-правового договора, фактически регулирующего трудовые отношения между работником и работодателем, и (или) нарушение, выразившееся в фактическом допущении работника к работе и уклонении работодателя от оформления трудового договора.

Спецоценка условий труда ряда медработников: Минтруд обновил правила. (Приказ Минтруда России от 10.04.2025 N 197н)

Утвердили новые особенности спецоценки на рабочих местах отдельных категорий медиков. Речь идет о работниках скорой помощи, отделений реанимации, интенсивной терапии, операционных, а также о тех, кто для диагностики и лечения использует аппаратуру из перечня. **Документ вступает в силу 1 сентября 2025 года.**

В целом правила останутся такими же, как сейчас. Одно небольшое уточнение есть в порядке для отделений реанимации, интенсивной терапии, операционных. Добавили, что санитарную одежду (халат, бахилы, шапочку, маску) экспертам предоставляет организация, в которой идет спецоценка. В остальном поправки технические.

Напомним, спецоценку условий труда в медорганизациях нужно проводить с учетом особенностей для части их работников. Невыполнение этого условия может повлечь штраф от 60 тыс. до 80 тыс. руб. для клиник. Должностным лицам грозит предупреждение или штраф от 5 тыс. до 10 тыс. руб.

Изменения в законодательстве в сфере трудовых правоотношений июнь 2025

В Трудовой кодекс РФ внесены изменения, позволяющие работодателям снижать размеры премий работникам с дисциплинарными взысканиями

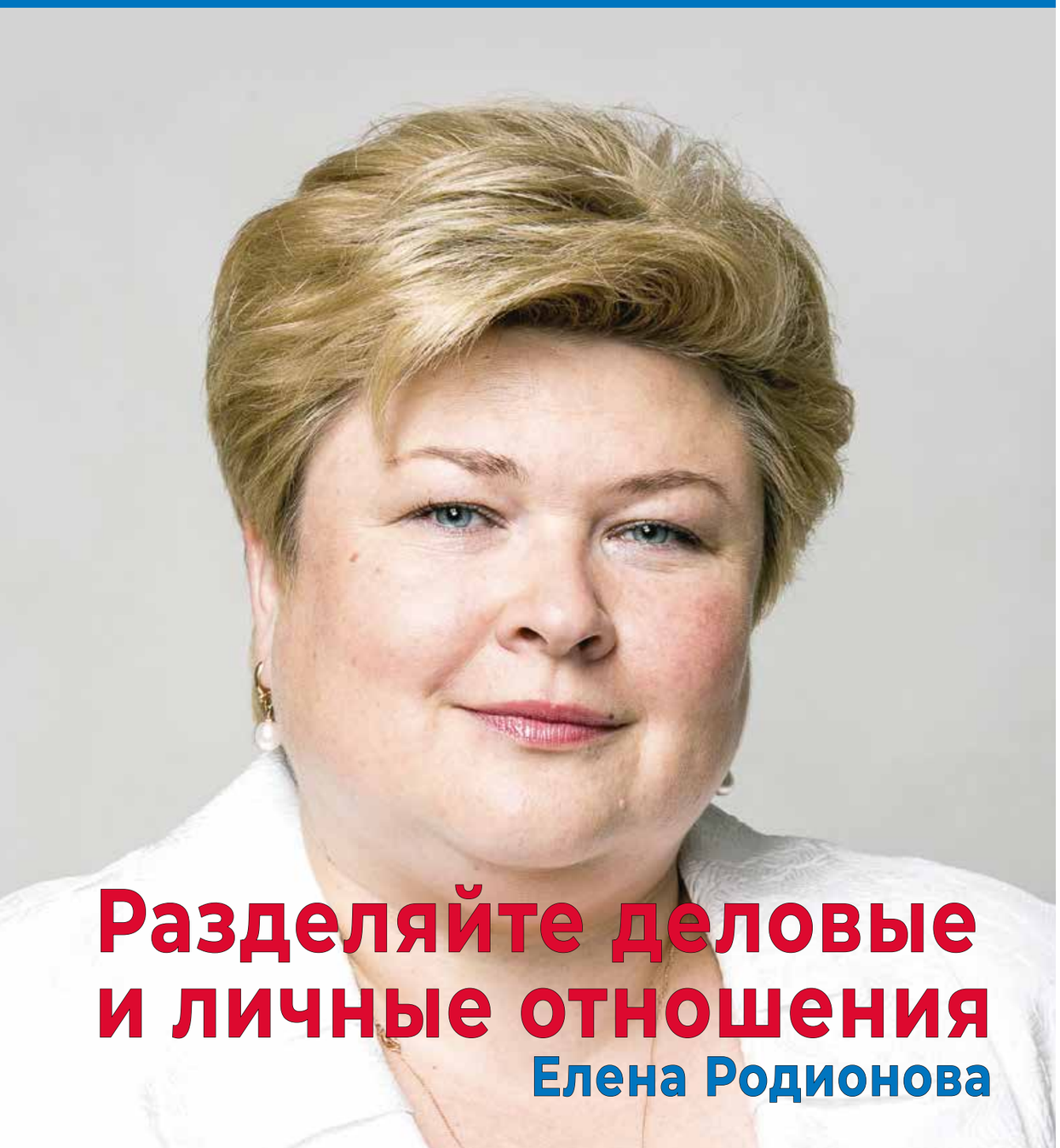
Федеральный закон от 07.06.2025 N 144-ФЗ «О внесении изменений в Трудовой кодекс

**Полные тексты статей доступны только для подписчиков.
Остальным желающим на платной основе.
Пишите: 7447273@bk.ru**

ИЗДАТЕЛЬСТВО ЖУРНАЛА
УПРАВЛЕНИЕ ПЕРСОНАЛОМ

Коммерческие споры

№ 2 / 2025



Разделяйте деловые и личные отношения

Елена Родионова

ЕЖЕМЕСЯЧНЫЙ ПРАКТИЧЕСКИЙ ЖУРНАЛ

Трудовое право

www.TOP-PERSONAL.RU

№ 8 (301)

АВГУСТ 2025

Подписные индексы: «Почта России» – 99724, Урал-Пресс: 47489