УДК 004.032.2

Варфоломеева Елена Евгеньевна, магистрант, Федеральный государственный бюджетный образовательный университет «Тольяттинский государственный университет», г. Тольятти

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТРАНСПОРТНЫХ КОМПАНИЙ САМАРСКОЙ ОБЛАСТИ: НОВЫЕ НОРМАТИВЫ И ПРАКТИЧЕСКИЕ РЕШЕНИЯ

Аннотация. В статье рассматриваются изменения в законодательстве РФ, вступающие в силу с 30 мая 2025 года, связанные с ужесточением ответственности за нарушение требований к обработке и защите персональных данных (ПД). Анализируются основные нововведения и их последствия для транспортно-логистического сектора Самарской области. Особое внимание уделяется рискам штрафных санкций, необходимости внедрения современных систем защиты информации, а также вопросам обучения персонала и обновления внутренней документации. В работе выявлены перспективные направления развития информационной безопасности в регионе, такие как создание центров компетенций, сертификация по стандартам и использование облачных решений. Основные выводы свидетельствуют о необходимости своевременной адаптации компаний к новым нормативам для снижения рисков штрафов и повышения доверия клиентов и партнеров.

Ключевые слова: информационная безопасность, транспортные компании, нормативы.

Annotation. The article discusses changes in the legislation of the Russian Federation, effective from May 30, 2025, related to increased liability for violations of the requirements for the processing and protection of personal data (PD). The main innovations and their consequences for the transport and logistics sector of the Samara region are analyzed. Special attention is paid to the risks of penalties, the need to introduce modern information security systems, as well as issues of staff

training and updating internal documentation. The paper identifies promising areas for the development of information security in the region, such as the creation of competence centers, certification according to standards and the use of cloud solutions. The main conclusions indicate the need for timely adaptation of companies to new regulations in order to reduce the risks of fines and increase the trust of customers and partners.

Keywords: information security, transport companies, regulations.

С 30 мая 2025 года в России вступили в силу новые поправки в КоАП РФ, связанные с ужесточением ответственности за нарушение требований к обработке и защите персональных данных (ПД). Для транспортно-логистических компаний, которые ежедневно работают с большим объемом информации о клиентах, партнерах и сотрудниках, эти изменения имеют особое значение. В данной статье рассмотрим основные нововведения и их последствия для отрасли.

Основными же изменения в законодательстве стали, во-первых увеличение штрафов и усиление ответственности. Согласно Федеральному закону № 420-ФЗ от 30.11.2024, штрафы за нарушение правил обработки ПД значительно выросли. Так, за утечку данных о более чем 10 000 физических лиц или 100 000 идентификаторов штраф может достигать 5–10 миллионов рублей, а за утечку данных о более чем 100 000 лиц — до 15 миллионов рублей (ст. 13.11 КоАП РФ). Для повторных нарушений санкции могут составлять 1–3% годовой выручки компании, что особенно опасно для крупных транспортных холдингов.

Во-вторых, введены новые составы правонарушений, связанные с обработкой биометрических данных, — нарушение порядка обработки, отсутствие мер по обеспечению их безопасности, обработка без соответствующей аккредитации (ст. 13.11.3 КоАП РФ). Также выделен отдельный состав отказа обслуживать клиента, отказавшегося от подтверждения личности с помощью биометрии (ст. 14.8 КоАП РФ).

В-третьих, отмена скидки за быструю уплату штрафа.С 2025 года скидка 50% при своевременной оплате штрафов отменена, что увеличивает финансовую нагрузку на нарушителей.

На что стоит обратить внимание транспортно-логистические компаниям:

Обязательства по защите данных клиентов и партнеров.

Транспортные компании обрабатывают большие объемы персональных данных: сведения о грузах, маршрутах, клиентах, водителях, сотрудниках. Новые требования требуют внедрения современных систем защиты информации, регулярных аудитов и соблюдения стандартов безопасности (например, ISO/IEC 27001).

Самарская область активно развивается в сфере информационных технологий и цифровизации. В регионе работают крупные предприятия, логистические компании, государственные учреждения, которые уже внедряют системы защиты данных. Однако, в малых и средних бизнесах уровень защиты зачастую недостаточен, что увеличивает риски штрафов и утечек.

Риск штрафных санкций и репутационные потери

Несоблюдение новых правил может привести к крупным штрафам, что негативно скажется на финансовом положении и репутации компании. Роскомнадзор и другие органы проводят проверки соблюдения требований по защите персональных данных. В регионе созданы подразделения, ответственные за контроль и мониторинг, что повышает вероятность выявления нарушений. Компании, не подготовленные к новым требованиям, рискуют столкнуться с крупными штрафами — до 15 миллионов рублей за утечку данных о более чем 100 000 лиц. Для среднего и малого предпринимательства конечно это значительные суммы и риски банкротства.

В Самарской области есть опыт внедрения систем защиты данных в крупных логистических и транспортных компаниях, что показывает возможность соответствовать новым требованиям. В то же время, для малого

и среднего бизнеса актуальна проблема недостатка ресурсов и знаний в области информационной безопасности.

Необходимость внедрения системы контроля и обучения персонала

Для снижения рисков необходимо организовать обучение сотрудников по вопросам обработки ПД, внедрить системы мониторинга и автоматизированные средства защиты данных. Следовательно на это должны быть запланированы в бюджете компании трудовые и финансовые ресурсы, а это дополнительная налоговая нагрузка для небольших фирм.

4. Внутренние процедуры и документация

Компании должны обновить внутренние регламенты, разработать процедуры уведомления о нарушениях, обеспечить хранение и обработку данных в соответствии с новыми требованиями.

Востребоваными станут запросы на услуги обучения и консалтинга. Компании могут предлагать услуги по аудиту, внедрению систем защиты данных, обучению персонала.

Перспективно развитие в создании локальных центров компетенций, развитие центров по информационной безопасности, сертификация по стандартам.

Также целесообразно использование облачных решений: для малого бизнеса — внедрение облачных платформ с встроенными средствами защиты.

Работа в условиях новых требований по защите данных в Самарской области возможна и перспективна, если компании инвестируют в современные системы защиты, проводят обучение сотрудников и сотрудничают с экспертами. Регион обладает потенциалом для развития ИБ-индустрии, что позволит не только снизить риски штрафов, но и повысить уровень доверия клиентов и партнеров. Важным фактором успеха станет своевременная адаптация к новым нормативам и внедрение лучших практик защиты информации. Новые поправки в законодательство РФ, вступающие в силу с 30 мая 2025 года, требуют от транспортно-логистических компаний усиления мер по защите персональных данных, внедрения современных

технологий и процедур. Несоблюдение новых правил грозит крупными штрафами и репутационными потерями. Поэтому важно уже сейчас подготовиться к изменениям, провести аудит информационных систем и обучить персонал.

Источники:

Федеральный закон от 30.11.2024 N 420-ФЗ «О внесении изменений в КоАП РФ»

КоАП РФ, статья 13.11, 13.11.3, 14.8

Федеральный закон № 152-ФЗ «О персональных данных»

Официальный сайт Правительства РФ и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)