



**Петр Анатольевич  
ЛЕСНИКОВ,**

основатель и управляющий  
партнер

юридической фирмы

«Лесников, Ильичев

и Партнеры»,

кандидат юридических наук

**lesnikovpro@gmail.com**

454100, Россия,

г. Челябинск,

просп. Ленина, д. 55

## Административно-правовые аспекты обеспечения кибербезопасности в цифровой таможенной инфраструктуре

**Аннотация.** Статья посвящена исследованию административно-правовых аспектов обеспечения кибербезопасности в цифровой таможенной инфраструктуре Российской Федерации. Анализируются: правовая природа таможенной информационной инфраструктуры как объекта критической информационной инфраструктуры; система субъектов административно-правового регулирования кибербезопасности в таможенной сфере и разграничение их компетенций; режим защиты сведений, обрабатываемых в ЕАИС ТО.

Выявляются структурные пробелы в регулировании: отсутствие специального правового режима кибербезопасности таможенных данных, неурегулированность ответственности за кибератаки на таможенную инфраструктуру, пробелы в правовом регулировании трансграничного информационного обмена в условиях кибератак. Предлагается концепция таможенного киберсуверенитета как административно-правовой категории.

**Ключевые слова:** кибербезопасность, информационное право, цифровая таможенная инфраструктура, критическая информационная инфраструктура, ЕАИС ТО, ФТС России, таможенные данные, административно-правовое регулирование, киберсуверенитет, информационная безопасность, ФСТЭК России

DOI: 10.17803/2311-5998.2026.142.6.136-143

**Petr A. LESNIKOV,**

founder and managing partner of the law firm

“Lesnikov, Ilyichev and Partners” (Chelyabinsk),

Cand. Sci. (Law)

**lesnikovpro@gmail.com**

55, prosp. Lenina, Chelyabinsk, Russia, 454100

### Administrative and Legal Aspects of Cybersecurity in Digital Customs Infrastructure

**Abstract.** The article is devoted to the study of administrative and legal aspects of ensuring cybersecurity in the digital customs infrastructure of the Russian Federation. The following are analyzed: the legal nature of the customs information infrastructure as an object of critical information infrastructure (CII); the system of subjects of administrative and legal regulation of cybersecurity in the customs sphere and the delineation of their competencies; the regime of protection of information processed in the EAI TO.

*Structural gaps in regulation are identified: the absence of a special legal regime for cybersecurity of customs data, the lack of regulation of liability for cyberattacks on the customs infrastructure, and gaps in the legal regulation of cross-border information exchange in the context of cyberattacks. The concept of “customs cyber sovereignty” as an administrative and legal category is proposed.*

**Keywords:** cybersecurity, information law, digital customs infrastructure, critical information infrastructure, EAIS TO, FCS of Russia, customs data, administrative and legal regulation, cyber sovereignty, information security, FSTEC of Russia

Цифровая трансформация таможенного администрирования, обеспечившая значительный прирост эффективности таможенных процедур, одновременно породила принципиально новые риски в сфере информационной безопасности. Единая автоматизированная информационная система таможенных органов<sup>1</sup> (ЕАИС ТО), обрабатывающая ежегодно свыше 5 млн деклараций на товары, содержит массивы данных, представляющих исключительную ценность — коммерческую, разведывательную и стратегическую. Компрометация данных ЕАИС ТО способна не только причинить ущерб конкретным участникам внешнеэкономической деятельности, но и нанести серьезный вред государственным интересам в сфере обеспечения экономической безопасности.

Мировая практика фиксирует устойчивую тенденцию к росту числа кибератак на таможенные и иные пограничные информационные системы. В 2021 г. масштабной кибератаке подвергся Южноафриканский порт Дурбан и сопряженные таможенные системы<sup>2</sup>; в 2023 г. фиксировались попытки несанкционированного доступа к системам таможенного оформления ряда государств ЕАЭС. Российская таможенная инфраструктура, включенная в глобальные цепочки обмена данными с иностранными таможенными администрациями, объективно подвержена аналогичным угрозам.

Вместе с тем административно-правовое регулирование кибербезопасности применительно к таможенной инфраструктуре остается фрагментарным. Российское законодательство в сфере информационной безопасности формировалось преимущественно применительно к общим категориям государственных информационных систем и объектов критической информационной инфраструктуры, не учитывая специфику таможенной сферы — ее трансграничного характера, высокой степени интеграции с информационными системами ЕАЭС и иностранных государств, а также тройственного правового режима обрабатываемых данных (коммерческая тайна, государственная тайна, персональные данные одновременно).

<sup>1</sup> Приказ ФТС России от 17.06.2010 № 1154 (ред. от 28.07.2017) «Об утверждении Положения о Единой автоматизированной информационной системе таможенных органов» // URL: <https://www.alta.ru/tamdoc/10pr1154/> (дата обращения: 09.05.2026).

<sup>2</sup> Case Study 17: Port of Durban, South Africa // URL: <https://resilientmaritimelogistics.unctad.org/guidebook/case-study-17-port-durban-south-africa> (дата обращения: 09.05.2026).



Цель настоящей статьи — исследовать административно-правовые механизмы обеспечения кибербезопасности в цифровой таможенной инфраструктуре, выявить пробелы действующего регулирования и предложить концептуальную модель таможенного киберсуверенитета как инструмента их устранения.

Правовое основание для квалификации цифровой таможенной инфраструктуры в качестве объекта критической информационной инфраструктуры создает Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»<sup>3</sup>. Согласно ст. 2 данного Закона к критической информационной инфраструктуре относятся объекты, функционирование которых критически важно для обороны страны, государственного управления, финансовой системы, топливно-энергетического комплекса, транспортной системы и иных стратегических отраслей.

Таможенные органы включены в перечень субъектов критической информационной инфраструктуры (КИИ) косвенно — через категорию государственных органов, осуществляющих функции в сфере государственного управления и обеспечения экономической безопасности. Постановление Правительства РФ от 08.02.2018 № 127<sup>4</sup>, утвердившее правила категорирования объектов КИИ, распространяется на ФТС России в части ЕАИС ТО. Вместе с тем специальных актов, определяющих порядок категорирования объектов КИИ применительно к таможенной информационной инфраструктуре, не принято.

Анализ структуры ЕАИС ТО позволяет выделить несколько категорий объектов, подлежащих отнесению к КИИ. Первая — системы обработки таможенных деклараций: нарушение их работоспособности влечет прекращение таможенного оформления на всей территории страны, что является угрозой экономической безопасности государства. Вторая — системы управления рисками: несанкционированный доступ к ним позволяет манипулировать результатами таможенного контроля в интересах недобросовестных участников ВЭД или иностранных разведок. Третья — системы межведомственного электронного взаимодействия: их компрометация создает угрозу утечки персональных данных и сведений о товарных потоках стратегического значения.

Вместе с тем действующее категорирование объектов КИИ применительно к таможенной инфраструктуре не в полной мере соответствует реальному уровню угроз. ЕАИС ТО в части обработки деклараций отнесена к третьей (наименее высокой) категории значимости объектов КИИ, тогда как реальные последствия нарушения ее работоспособности — полная остановка таможенного оформления — объективно соответствуют критериям первой категории. Данное несоответствие влечет занижение требований к защищенности системы.

<sup>3</sup> Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 07.04.2025) «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2017. № 31 (ч. I). Ст. 4736 ; 2025. № 15. Ст. 1784.

<sup>4</sup> Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 07.11.2025) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // СЗ РФ. 2018. № 8. Ст. 1204 ; 2025. № 45. Ст. 6775.

Принципиальной особенностью таможенной информационной инфраструктуры, отличающей ее от иных объектов КИИ, является ее трансграничный характер. ЕАИС ТО интегрирована с информационными системами таможенных органов государств — членов ЕАЭС в рамках Интегрированной информационной системы внешней и взаимной торговли<sup>5</sup> (ИИСВВТ), а также осуществляет информационный обмен с таможенными администрациями иностранных государств в рамках двусторонних соглашений о взаимном признании. Данная интеграция создает дополнительные векторы кибератак, которые законодательство о КИИ в части трансграничного измерения практически не регулирует.

Административно-правовое регулирование кибербезопасности применительно к таможенной инфраструктуре осуществляется множеством субъектов, компетенция которых не разграничена в достаточной мере. Данное «компетенционное рассеивание» является одной из ключевых системных проблем в рассматриваемой сфере.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является регулятором в сфере защиты информации, не составляющей государственную тайну, и ключевым органом в части обеспечения безопасности КИИ. Применительно к таможенной инфраструктуре ФСТЭК России осуществляет: методологическое руководство категорированием объектов КИИ; утверждение требований по безопасности значимых объектов КИИ; государственный контроль в области обеспечения безопасности значимых объектов КИИ<sup>6</sup>. Вместе с тем ФСТЭК России не располагает отраслевой экспертизой применительно к специфике таможенных информационных систем и не участвует в разработке технических регламентов ЕАИС ТО.

Федеральная служба безопасности РФ осуществляет координацию деятельности по обеспечению безопасности КИИ (ст. 6 Федерального закона № 187-ФЗ), эксплуатирует Национальный координационный центр по компьютерным инцидентам (НКЦКИ) и осуществляет разведывательную деятельность применительно к иностранным киберугрозам. Применительно к таможенной инфраструктуре ФСБ России, помимо общей координирующей роли, осуществляет защиту сведений, составляющих государственную тайну (в части таможенной разведки, профилей рисков СУР, оперативной информации).

Министерство цифрового развития, связи и массовых коммуникаций РФ устанавливает требования к государственным информационным системам (ГИС) применительно к их архитектуре, использованию отечественного программного обеспечения и размещению данных на территории Российской Федерации. Данные требования распространяются на ЕАИС ТО в части, не регулируемой специальными нормами таможенного законодательства. Конфликт компетенций между

<sup>5</sup> Решение Коллегии ЕЭК от 27.01.2015 № 5 «Об утверждении Правил электронного обмена данными в интегрированной информационной системе внешней и взаимной торговли» // URL: <https://www.alt.ru/tamdoc/15kr0005/> (дата обращения: 09.05.2026).

<sup>6</sup> Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2018. № 9. Ст. 1393.



Минцифры и ФТС России периодически возникает применительно к требованиям об использовании российского программного обеспечения: ряд компонентов ЕАИС ТО исторически разработан на основе иностранных платформ.

Сама ФТС России обладает компетенцией в сфере кибербезопасности таможенной инфраструктуры в качестве ее оператора. Соответствующие функции осуществляются Главным управлением информационных технологий (ГУИТ) ФТС России совместно с Центральным информационно-техническим таможенным управлением (ЦИТТУ), являющимся правопреемником ГНИВЦ ФТС России — подведомственным учреждением, выступающим технологическим оператором ЕАИС ТО. Разграничение ответственности между ФТС России как субъектом КИИ и ЦИТТУ как техническим оператором в нормативных актах прямо не определено.

Описанная конфигурация субъектов регулирования характеризуется дублированием полномочий в одних аспектах (защита ГИС от несанкционированного доступа находится в сфере компетенции и ФСТЭК России, и ФСБ России, и Минцифры одновременно) при наличии значимых белых пятен в других (трансграничная кибербезопасность таможенных систем, защита данных в рамках интеграционных систем ЕАЭС).

Данные, обрабатываемые в ЕАИС ТО, характеризуются исключительной правовой сложностью с точки зрения режима их охраны. Они не являются однородной категорией — в составе таможенных данных одновременно присутствуют сведения, подпадающие под различные правовые режимы ограниченного доступа.

Первая категория — государственная тайна. К ней относятся сведения о профилях рисков СУР, содержащие методологию таможенной «разведки»; данные оперативных таможенных расследований; сведения, составляющие военную тайну, в части деклараций на товары военного и двойного назначения. Правовой режим данной категории определяется Законом РФ от 21.07.1993 № 5485-1 «О государственной тайне»<sup>7</sup> и является наиболее строгим.

Вторая категория — коммерческая тайна. Сведения, содержащиеся в таможенных декларациях (наименование товаров, их количество, стоимость, сведения о контрагентах), могут составлять коммерческую тайну декларантов. Режим защиты данной категории определяется Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне»<sup>8</sup>. Утечка данных сведений вследствие кибератаки нарушает права декларантов и может влечь гражданско-правовую ответственность оператора системы.

Третья категория — персональные данные. Декларации на товары содержат персональные данные физических лиц — грузополучателей, перевозчиков, представителей декларантов. Правовой режим защиты данной категории определяется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных

<sup>7</sup> Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.08.2024) «О государственной тайне» // СЗ РФ. 1997. № 41. Ст. 8220—8235 ; 2024. № 33 (ч. I). Ст. 4945.

<sup>8</sup> Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 08.08.2024) «О коммерческой тайне» // СЗ РФ. 2004. № 32. Ст. 3283 ; 2024. № 33 (ч. I). Ст. 4947.

данных»<sup>9</sup> и требованиями ФСТЭК России<sup>10</sup> по защите информационных систем, персональных данных.

Четвертая категория — открытые данные. Часть таможенной статистики подлежит обязательному публичному раскрытию. Вместе с тем грань между агрегированными данными, подлежащими публикации, и деперсонализированными данными, из которых при соответствующей обработке могут быть выделены персональные или коммерчески чувствительные сведения, нормативно не определена, что создает риск деанонимизации через открытые данные.

Сосуществование нескольких правовых режимов в рамках единой информационной системы создает принципиальную проблему: требования по защите, установленные для каждого режима в отдельности, разработаны применительно к «чистым» случаям, тогда как ЕАИС ТО объединяет в одной архитектуре данные всех перечисленных категорий. Это требует либо применения к системе в целом наиболее строгого из применимых режимов (что избыточно для части данных), либо технологического разделения данных по категориям (что технически сложно и нормативно не предусмотрено).

Трансграничный характер таможенной деятельности предопределяет необходимость интеграции ЕАИС ТО с информационными системами иностранных государств и международных организаций. Данная интеграция осуществляется по нескольким каналам:

- в рамках ЕАЭС — через ИИСВВТ, оператором которой является ЕЭК;
- в рамках двусторонних соглашений ФТС России с иностранными таможенными администрациями о взаимном признании и обмене предварительной информацией;
- в рамках международных программ (программа ВТамО SafeCargo, программы ВТО по упрощению процедур торговли).

Трансграничная интеграция создает уникальный класс киберугроз — угрозы, реализуемые через внешние информационные каналы. Компрометация информационной системы государства — партнера по обмену данными может создать вектор атаки на ЕАИС ТО через защищенные каналы межведомственного взаимодействия. Данный вектор принципиально отличается от традиционных внешних атак тем, что атакующий использует легитимные технические средства доступа.

Правовое регулирование трансграничной кибербезопасности таможенной инфраструктуры находится в зачаточном состоянии. Соглашения ФТС России с иностранными таможенными администрациями об обмене предварительной информацией, как правило, содержат общие положения о защите передаваемых данных, однако не устанавливают конкретных технических требований к кибербезопасности и не предусматривают механизмов ответственности за нарушение данных требований.

<sup>9</sup> Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451 ; 2025. № 26 (ч. I). Ст. 3486.

<sup>10</sup> Приказ ФСТЭК России от 11.04.2025 № 117 // URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117> (дата обращения: 09.05.2026).



На уровне ЕАЭС ситуация несколько лучше<sup>11</sup>. При этом к минусам относятся рекомендательный характер таких соглашений, а также тот факт, что они не охватывают специфику киберугроз применительно к таможенным данным.

Особую проблему представляет правовой режим данных ЕАИС ТО в ситуации кибератаки, осуществленной с территории иностранного государства. Российское законодательство о КИИ не содержит норм, регулирующих порядок ответных мер при установлении государственной принадлежности кибератаки, что является принципиальным пробелом с учетом тенденции к государственно спонсируемым кибератакам на инфраструктуру критически важных объектов.

Система административно-правовых санкций за нарушения в сфере кибербезопасности, применимых к таможенной инфраструктуре, характеризуется принципиальной неполнотой. КоАП РФ содержит ряд составов, потенциально применимых в данном контексте, однако они не формируют целостного механизма ответственности.

Статья 13.12 КоАП РФ предусматривает ответственность за нарушение правил защиты информации (штраф для юридических лиц от 15 000 до 25 000 рублей). Данный состав применим в случае нарушения оператором ЕАИС ТО требований ФСТЭК России по защите информации. Вместе с тем санкции данной статьи несопоставимо малы по отношению к масштабу возможного ущерба от нарушений в сфере таможенной кибербезопасности.

Статья 13.11 КоАП РФ устанавливает ответственность за нарушение законодательства о персональных данных. Применительно к ЕАИС ТО данный состав актуален в случае утечки персональных данных участников ВЭД вследствие кибератаки или ненадлежащей защиты системы. Однако специфика оператора ГИС (каковым является ФТС России) предполагает исключение из ряда обязанностей, установленных для операторов персональных данных в частном секторе.

Уголовно-правовая защита таможенной инфраструктуры обеспечивается гл. 28 УК РФ «Преступления в сфере компьютерной информации» (ст. 272—274.1). В части, специально посвященной объектам КИИ, ст. 274.1 УК РФ предусматривает ответственность за неправомерное воздействие на критическую информационную инфраструктуру. Применительно к таможенным системам данный состав является наиболее релевантным, однако его использование осложняется проблемой установления и доказывания государственной принадлежности кибератак.

Принципиальным пробелом является отсутствие механизма ответственности ФТС России как оператора ЕАИС ТО за ненадлежащее обеспечение кибербезопасности, повлекшее утечку данных или нарушение работоспособности системы. В данном случае участник ВЭД, пострадавший от утечки коммерческих данных вследствие кибератаки, реализовавшейся через недостаточно защищенную ЕАИС ТО, лишен эффективного правового средства защиты: иск к государству по ст. 1069 ГК РФ требует доказывания конкретного противоправного деяния должностного лица, тогда как системные недостатки защиты под данную конструкцию не подпадают.

Совокупность выявленных проблем обуславливает необходимость формирования специальной административно-правовой концепции, объединяющей

<sup>11</sup> Рекомендации Коллегии Евразийской экономической комиссии от 12.03.2019 № 9 «О перечне стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза» // URL: <https://www.garant.ru/products/ipo/prime/doc/72097708/> (дата обращения: 09.05.2026).

разрозненные требования к кибербезопасности таможенной инфраструктуры в системную правовую конструкцию. Автор предлагает концепцию таможенного киберсуверенитета как совокупности правовых механизмов, обеспечивающих суверенный контроль государства над цифровой таможенной инфраструктурой и обрабатываемыми в ней данными.

Таможенный киберсуверенитет как административно-правовая категория включает четыре компонента:

- 1) технологический суверенитет — обязательное использование при функционировании ЕАИС ТО сертифицированного российского программного обеспечения, отечественных средств криптографической защиты информации и размещение данных исключительно на серверах, физически находящихся на территории Российской Федерации. Данный компонент частично реализован через требования Минцифры России о переходе ГИС на российское ПО, однако применительно к ЕАИС ТО его реализация нормативно не закреплена;
- 2) информационный суверенитет — установление правовых ограничений на передачу данных ЕАИС ТО иностранным государствам и международным организациям, включая исчерпывающий перечень передаваемых категорий данных, порядок и условия их передачи, механизм приостановления обмена данными при возникновении угрозы кибератаки через каналы межведомственного взаимодействия;
- 3) операционный суверенитет — обязательная локализация всех процессов технической эксплуатации и обновления ЕАИС ТО на территории Российской Федерации, исключение привлечения иностранных специалистов или компаний к работам, дающим доступ к данным ЕАИС ТО, без специального разрешения ФСБ России. Данный компонент актуализирован с учетом практики санкционного давления, при котором иностранные поставщики ПО прекращали техническую поддержку государственных систем;
- 4) юрисдикционный суверенитет — установление исключительной юрисдикции российских органов власти над инцидентами в сфере кибербезопасности ЕАИС ТО, включая право ФСБ России проводить расследование кибератак без согласования с иностранными органами, даже если атака осуществлена с территории иностранного государства, с которым действует соглашение о правовой помощи по киберделам.

Концепция таможенного киберсуверенитета не означает изоляции таможенной инфраструктуры от международных систем обмена данными — она предполагает создание четких правовых рамок для такого обмена, обеспечивающих государственный контроль над его условиями и возможность оперативного ограничения в случае возникновения угроз.

Аналогичные концепции реализуются в ряде государств: Китай имплементировал систему контроля трансграничных потоков данных применительно к государственным инфраструктурным системам; ЕС разрабатывает концепцию цифрового суверенитета (Digital Sovereignty<sup>12</sup>) применительно к данным критической инфраструктуры.

<sup>12</sup> Digital sovereignty for Europe // URL: [https://www.europarl.europa.eu/thinktank/en/document/eprs\\_bri\(2020\)651992](https://www.europarl.europa.eu/thinktank/en/document/eprs_bri(2020)651992) (дата обращения: 09.05.2026).