

УДК 34**Правовое регулирование компьютерных средств
информационной защиты и охраны систем обеспечения
транспортной безопасности****Лещов Геннадий Юрьевич**

Кандидат экономических наук,
директор научно-исследовательского центра экспертиз на транспорте,
Российский университет транспорта РУТ (МИИТ),
127994, Российская Федерация, Москва, ул. Образцова д.9/9;
e-mail: g-u-l@mail.ru

Мельникова Юлия Владимировна

Кандидат юридических наук,
доцент кафедры гражданско-правовых дисциплин,
Московский государственный университет технологий
и управления им. К.Г. Разумовского (Первый казачий университет),
109004, Российская Федерация, Москва, ул. Земляной Вал, 73;
e-mail: 84995016973@bk.ru

Аннотация

В статье анализируются современные проблемы теории и правоприменительной практики, связанные с применением информационно-компьютерных средств как средств информационной защиты и охраны систем обеспечения транспортной безопасности и технического прикрытия объектов инфраструктуры транспортного комплекса. Рассмотрены положения законодательства по данной проблеме, исследуются сильные и слабые стороны, формулируются авторские предложения по совершенствованию норм действующего законодательства в сфере применения информационно-компьютерных технологий, как средств информационной охраны и защиты транспортных систем. Выработано консенсусное решение о возможности применения комплексных технических и правовых средств охраны и защиты объектов инфраструктуры транспортного комплекса с помощью использования информационно-компьютерных средств. Отличием информационно-компьютерных средств от иных, реальных средств охраны и защиты в их искусственном характере. Данная виртуальная система возникла и развивается как совокупность технических средств и устройств, при этом еще принадлежащих в значительной степени частным лицам и взаимодействующих между собой на основе использования сети глобальных цифровых идентификаторов и системы протоколов обмена информацией между устройствами и средствами. Основным средством существования и развития информационно-компьютерных средств является предпринимательская деятельность частных лиц в области передачи, хранения и обработки информации, создания и развития, разработки и представления на рынок программных и технических продуктов.

Для цитирования в научных исследованиях

Лещов Г.Ю., Мельникова Ю.В. Правовое регулирование компьютерных средств информационной защиты и охраны систем обеспечения транспортной безопасности // Вопросы российского и международного права. 2024. Том 14. № 5А. С. 239-248.

Ключевые слова

Информационно-компьютерные технологии, информационно-компьютерные средства, средства информационной защиты и охраны, транспортная безопасность, техническое прикрытие, объекты инфраструктуры транспортного комплекса.

Введение

Одной из современных ключевых проблем современной России является правовое и техническое обеспечение развития информационной защиты систем транспортной безопасности и технического прикрытия объектов инфраструктуры транспортного комплекса.

На сегодняшний день несовершенство правовой базы в рассматриваемой сфере порой восполняется техническими мерами охраны и защиты информационных систем транспортной безопасности и технического прикрытия объектов инфраструктуры транспортного комплекса. Сейчас очень важно найти такие правовые механизмы, которые обеспечат правовую охрану и защиту транспортной системы с помощью информационно-компьютерных средств, не ограничивая возможности использования Интернета для передачи и получения необходимой информации.

Основное содержание

К числу актуальных направлений обеспечения транспортной безопасности Российской Федерации относится формирование национальной системы информационной безопасности [Об информации, информационных технологиях и о защите информации, [www...](http://www.fbi.ru)] и правовых средств охраны и защиты объектов инфраструктуры транспортного комплекса, обеспечивающих эффективное противодействие использованию информационных технологий в военно-политических целях, противоречащих международному праву, а также в террористически экстремистских, криминальных и иных противоправных целях.

Важным средством реализации данного направления государственной политики является совершенствование правового обеспечения транспортной безопасности (ТБ).

Количество работ российских и зарубежных авторов, посвященных различным аспектам данной проблемы, более чем значительно, однако проблема еще далека от своего решения.

Уже более 5 лет изучением проблем транспортной безопасности и технического прикрытия объектов инфраструктуры транспорта занимается группа ученых Научно – исследовательского центра экспертиз на транспорте Российского университета транспорта, в своей работе установлены ключевые аспекты влияния на национальную безопасность и необходимости применения в этой области специальных режимов государственного регулирования. На протяжении последних трех лет проведены следующие научно-исследовательские работы на тему «Исследование проблемных вопросов организации технического прикрытия и восстановления транспортных коммуникаций и подготовка предложений по их решению», Государственный контракт от 28 марта 2023 г., и «Актуализация методологических подходов по организации охраны наиболее важных объектов железнодорожного транспорта с учётом

современных тенденций изменения криминогенной обстановки, актуальных угроз совершения актов незаконного вмешательства», Государственный контракт от 23 августа 2021 г.

Важным итогом работы группы явилось консенсусное решение о возможности применения комплексных технических и правовых средств охраны и защиты объектов инфраструктуры транспортного комплекса с помощью использования информационно-компьютерных средств. В докладе группы было отмечено, что «право в целом применимо к данной области, однако необходимо выработать общее понимание того каким образом оно может применяться, а также в каком направлении в случае необходимости следует его адаптировать» [Паламарчук, 2010].

В настоящей статье сформулированы одни из причин возникновения проблем применимости информационно-компьютерных средств в сфере технического прикрытия и выработки правовых средств охраны и защиты объектов инфраструктуры транспортного комплекса, и возможные направления их решения.

Решение проблемы правомерного и законного использования информационно-компьютерных средств в интернет-пространстве волнует сегодня все мировое сообщество. Интернет переполнен материалами, нарушающими те или иные права граждан, юридических лиц, публично-правовых образований, государств. Во всемирной Сети сегодня можно найти практически любую интересующую информацию, размещенную иногда с нарушением прав.

Отличие нарушений прав с помощью информационно-компьютерных технологий состоит в том, что простота копирования и нематериальная сущность информации не позволяют также просто решить проблему обеспечения доказательств нарушений права. Проблема не в том, что информационно-компьютерными средствами невозможно обеспечить защиту системы технического прикрытия объектов инфраструктуры транспортного комплекса, а в том, что пока практически никто всерьез не пытался пресечь их нарушений имеющимися в распоряжении законодательства методами.

Внедрение информационно-телекоммуникационных сетей в различные сферы общественной жизнедеятельности актуализирует вопрос о надлежащем правовом обеспечении этого процесса, что, в свою очередь, ставит новые задачи для юриспруденции начала XXI в. Несмотря на то, что появление и распространение Интернета оказывает влияние практически на все сферы жизнедеятельности общества, а значит, на все отрасли права, все же именно для системы технического прикрытия объектов инфраструктуры транспортного комплекса это одна из самых острых проблем, прямо связанная с основами понимания и регулирования отношений с использованием информационно-компьютерных средств.

В настоящее время регулируемые правом отношения в электронной среде Интернет и/или с помощью информационно-компьютерных средств трактуются учеными в общем плане и довольно неопределенно, что сказывается на формировании общей концепции средств охраны и защиты и их особенностей в части применения в системе технического прикрытия объектов инфраструктуры транспортного комплекса. Реализация правоотношений предполагает здесь распространение сведений, данных в реальности, в виртуальном пространстве, их использование, информационную безопасность сетей собственников технических средств. Специфика применения информационно-компьютерных средств в системе технического прикрытия объектов инфраструктуры транспортного комплекса состоит в том, что для тех или иных управомоченных субъектов возникают права, а на других субъектов возлагаются обязанности, подразумевающие необходимое поведение, зафиксированное в источниках права и обеспеченное доброй волей сторон либо государственным принуждением.

Структура данных отношений включает следующие элементы: субъекты, объекты, субъективные права и обязанности. На них также оказывают влияние юридические факты, информация, технические средства и т.д.

Информация, используемая в системе технического прикрытия объектов инфраструктуры транспортного комплекса, разнообразна и разнородна. Информацию в системе технического прикрытия объектов инфраструктуры транспортного комплекса можно классифицировать по признакам: функционального назначения и характера информационных систем; типа связи с внешней средой; отношения к целевой функции; логического содержания информации; процедуре преобразования информации в компьютерных сетях; степени преобразования информации; совокупности информации, времени и периодичности возникновения, обработки и передачи информации.

В сфере технического прикрытия могут быть выделены и другие признаки классификации информации: способ передачи, вид преобразования, степень достоверности, участие в вычислительном процессе, алфавит и т.д.

Таким образом, система технического прикрытия объектов инфраструктуры транспортного комплекса охватывает довольно широкий круг отношений, причем многие из них разноплановые и четко не определены.

По мнению ученых, основной причиной порождающей сложности в обеспечении комплексной безопасности информационно-компьютерных средств в сфере транспортной безопасности и технического прикрытия объектов инфраструктуры транспортного комплекса являются, прежде всего, виртуальный характер данных средств.

Отличием информационно-компьютерных средств от иных, реальных средств охраны и защиты в их искусственном характере. Данная виртуальная система возникла и развивается как совокупность технических средств и устройств, при этом еще принадлежащих в значительной степени частным лицам и взаимодействующих между собой на основе использования сети глобальных цифровых идентификаторов и системы протоколов обмена информацией между устройствами и средствами.

Основным средством существования и развития информационно-компьютерных средств является предпринимательская деятельность частных лиц в области передачи, хранения и обработки информации, создания и развития, разработки и представления на рынок программных и технических продуктов.

Проблемы обеспечения информационной безопасности с использованием информационно-технических средств в системе технического прикрытия объектов инфраструктуры транспортного комплекса делится на два направления:

1. Защита компьютерного программного обеспечения;
2. Защита непосредственно информации из системы технического прикрытия объектов инфраструктуры транспортного.

Рассматривая защиту компьютерного программного обеспечения, следует, прежде всего, определиться в основных понятиях.

Под программой для ЭВМ принято понимать объективную форму предоставления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин и других компьютерных устройств с целью получения определенного результата. Это совокупность инструкций, при использовании которых электронное устройство должно достичь заданного результата. Под программой ЭВМ также подразумеваются подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

Существуют различные инструменты для подготовки программ. Теоретически программы можно писать с использованием символов, распознаваемых процессором, т.е. в двоичной форме. Однако такой подход к написанию программ, если и будет эффективным в плане достижения более высокой производительности вычислительной системы, но останется крайне

непрактичным с точки зрения скорости подготовки самой программы, поскольку любой символ, команда и т.д. будет представлять собой длинную цепочку единиц и нулей. Для написания программ используются специально разработанные языки программирования.

Весьма проблематичным остается выбор вида законодательной охраны компьютерных программ. Теоретически возможны 3 формы:

1. Охрана с помощью авторского права;
2. Охрана с помощью патентного права;
3. Охрана через положения, направленные против нарушений коммерческой тайны.

Споры о выборе рационального варианта охраны продолжались в нашей стране и за рубежом последние несколько десятков лет.

Авторское право защищает форму произведения, но не его содержание, следовательно, информация, содержащаяся в произведении, может беспрепятственно распространяться любыми лицами, не будет нарушения авторских прав и пересказ содержания произведения. Но и в области прав, защищающих содержательную сторону объекта, предоставление информации отступает на второй план.

База данных — это объективная форма представления и организации совокупности данных, систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Базы данных содержат в себе определенную информацию, под которой понимаются сообщения, осведомляющие о положении дел, о состоянии чего-нибудь. Это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Практически все общественное взаимодействие, так или иначе, основано на обмене информацией. Ограничение возможностей обмена информацией создало бы непреодолимые трудности для общественного развития.

Определенное регулирование предоставления и использования информации осуществляется с помощью ряда исключительных прав и отдельных специальных правовых институтов. Специального права на информацию не вводилось. Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивов, фондах, банках данных, других информационных системах) представляют собой информационные ресурсы. Фактически вместо права на информацию рассматриваются права на документы, в которых содержится информация либо на их совокупность. Только информация, выраженная в форме документа, может включаться в состав информационных ресурсов.

Возможно выделение разных видов информационных ресурсов. По принадлежности ресурсов соответствующим субъектам можно говорить о государственных и негосударственных информационных ресурсах.

По общему правилу государственные информационные ресурсы РФ являются открытыми и общедоступными, но определенная законом документированная информация может быть отнесена к категории ограниченного доступа. Любой иной собственник информационных ресурсов может также принять решение о придании определенным принадлежащим ему информационным ресурсам статуса открытых ресурсов либо определить, в каких случаях устанавливается ограниченный доступ к ресурсам. [Соглашение о создании единой системы технического прикрытия железных дорог государств — членов Организации Договора о коллективной безопасности, 2007; Соглашение о сотрудничестве государств - членов Организации Договора о коллективной безопасности в области перевозок воинских и других

формирований, их движимого имущества, а также продукции военного назначения].

Защита систем обеспечения транспортной безопасности и технического прикрытия объектов инфраструктуры транспортного комплекса ничем не отличается от традиционных способов защиты прав, но имеет ряд особенностей. Особенности определяются тем, что системы технического прикрытия объектов инфраструктуры транспортного комплекса носят, закрытый государственно важный характер и утечка информации будет наносить существенный вред охраняемым интересам Российской Федерации [Указ Президента Российской Федерации от 2 октября 1998 г. № 1175 «Об утверждении Положения о военно-транспортной обязанности»].

Рассматривая информационную защиту непосредственно системы обеспечения транспортной безопасности и технического прикрытия объектов инфраструктуры транспортного комплекса законодательство РФ предусматривает гражданско-правовую, административную и уголовную ответственность.

В отношении лиц, причастных к нарушениям требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, применяется административная ответственность по ст. 13.12.1. Этот вид ответственности распространяется на граждан и юридических лиц и влечет наложение административного штрафа.

Постепенно получает развитие и институт уголовно-правовой ответственности за нарушение не правомерного доступа к компьютерной информации (ст. 272 УК РФ) [Паламарчук, 2010; Шестаков, [www...](#)]. В Уголовном кодексе РФ предусмотрена ответственность за хищение охраняемой законом информации. При этом способ хищения может влиять на тяжесть совершенного преступления и его квалификацию. С точки зрения уголовного законодательства совсем не одно то же - простое копирование информации без согласия правообладателя посредством обычного сохранения с последующим незаконным ее использованием (ст. 146 УК РФ) и те же самые действия, но с несанкционированным доступом и с изменением существующих программ (ст. ст. 272, 273 УК РФ).

Таким образом, в настоящее время в России есть нормативно-правовая база для борьбы с «цифровым вторжением и хищением», постепенно нарабатывается практика правоприменения, но есть и проблемы, присущие правовым системам большинства стран.

Современные «компьютерные преступники» активно используют пробелы национального законодательства и создают новые технологические способы хищения, передачи, вторжения, распространения информации в сфере безопасности.

В этой связи назрела необходимость установления в национальном законодательстве дополнительных механизмов привлечения к ответственности за попытки нарушения информационной целостности транспортных коммуникаций, так как их модификация может привести к существенным нарушениям функционирования системы и значительным человеческим жертвам.

Более эффективной защитой системы технического прикрытия объектов инфраструктуры транспортного комплекса с помощью информационно-компьютерных средств будет служить введение норм о привлечении к ответственности и владельцев сайтов, предоставляющих возможность получать или осуществлять передачу такой информации.

Отдельно следует сказать о роли прокуратуры в процессах обеспечения информационной защиты системы транспортной безопасности и технического прикрытия объектов инфраструктуры транспортного комплекса. Прокурорам необходимо включиться в работу по

созданию интегрированной системы управления безопасностью на объектах инфраструктуры транспортного комплекса, используя предоставленные законом полномочия [Лещов, 2019].

Прежде всего, для профилактики подобного рода нарушений целесообразно объявлять предостережения о недопустимости нарушения закона юридическим лицам, специализирующимся на размещении информации в сети Интернет.

В ходе соответствующих проверок при выявлении признаков уголовно наказуемого деяния (ст. 146 УК РФ) прокурор должен оперативно вынести постановление о передаче материалов в органы, уполномоченные на проведение проверки в соответствии со ст. ст. 144, 145 УПК.

При осуществлении надзорной работы прокурорам целесообразно наладить взаимодействие с общественными правозащитными организациями, которые могут предоставить информацию о нарушениях системы обеспечения транспортной безопасности и технического прикрытия объектов инфраструктуры транспортного комплекса и дальнейшей незаконной передачи с помощью сети Интернет и иных информационно-технических средств.

Информационная защита системы обеспечения транспортной безопасности и технического прикрытия объектов инфраструктуры транспортного комплекса, с использованием информационно-технических средств, предполагает под собой не только юридические, но и технические направления деятельности. В настоящее время контролировать использование информационно-технических средств в Интернете очень сложно, в связи с чем, самые удачные нормы права не смогут работать в полную силу без применения дополнительных, нерегулируемых методов защиты. Перспективы развития законодательства применительно к информационно-техническим средствам в значительной степени зависят от того, будут ли созданы технические средства, позволяющие ограничивать и отслеживать использование информации в сфере обеспечения транспортной безопасности и технического прикрытия объектов транспортной инфраструктуры.

Как и любую глобальную систему, систему технического прикрытия и систему правовых средств охраны и защиты объектов инфраструктуры транспортного комплекса можно рассматривать как совокупность технических и правовых институтов, призванных регулировать деятельность различных институтов, взаимодействующих на единой платформе во имя единой цели.

Заключение

Таким образом, можно сделать вывод, что информационная охрана и защита систем обеспечения транспортной безопасности и технического прикрытия объектов инфраструктуры транспортного комплекса с помощью информационно-компьютерных средств возможна и существует, однако необходимо соблюдать установленные требования. Нарушения лучше предотвратить, чем разбираться с их последствиями. В целом же представляется, что не отношения в среде Интернета нуждаются в особом правовом регулировании, а нормы самых разных законодательных актов (в том числе по вопросам безопасности) нуждаются в уточнении с учетом специфики отношений, складывающихся благодаря развитию новых средств коммуникации в цифровой среде.

Библиография

1. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: Федеральный закон № 149-ФЗ от 27.07.2006. Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 19.07.2024).

2. Паламарчук А.В. Защита исключительных прав на результаты интеллектуальной деятельности в сети Интернет // Законность. 2010, № 7. Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 19.07.2024).
3. Шестаков Е. Охрана контента в Интернете // <http://www.pcweek.ru/themes/detail.php?ID=111573>. Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 10.07.2024).
4. Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс]: № 174-ФЗ от 18.12.2001. Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 12.07.2024).
5. Постановление Правительства Российской Федерации от 17 февраля 2007 г. № 100-4 «Об утверждении Положения о техническом прикрытии инфраструктуры железнодорожного транспорта общего пользования Российской Федерации».
6. Указ Президента Российской Федерации от 2 октября 1998 г. № 1175 «Об утверждении Положения о военно-транспортной обязанности».
7. Указ Президента Российской Федерации от 21 сентября 2022 г. № 647 «Об объявлении частичной мобилизации в Российской Федерации».
8. Соглашение о создании единой системы технического прикрытия железных дорог государств — членов Организации Договора о коллективной безопасности (подписано в Душанбе 28 апреля 2003 г., ратифицировано Федеральным законом от 19 июля 2007 г. № 137-ФЗ, вступило в силу для Российской Федерации 13 августа 2007 г.)
9. Соглашение о сотрудничестве государств - членов Организации Договора о коллективной безопасности в области перевозок воинских и других формирований, их движимого имущества, а также продукции военного назначения (Заключено в г. Душанбе 15.09.2015)
10. Соглашение об использовании и развитии сети транспортных коммуникаций для нужд экономики, воинских и гуманитарных перевозок государств-участников Содружества Независимых Государств (подписано в Минске 31 мая 2001 г.)
11. Введенский И.А. Стратегическое управление и процессный подход // Известия РГПУ им. А.И. Герцена. 2009. №117.
12. Воробьев И, Киселёв В. Перспективы тактики в XXI веке // Армейский сборник: — 2008. — Февраль (т. 164, № 02). — С. 18-22.;
13. Ключевые моменты подготовки и организации технического прикрытия транспортных коммуникаций в Российской Федерации
14. Лещов Г.Ю. Проблемные вопросы материально-технического обеспечения группировок войск (сил) в специальной военной операции: сборник материалов отраслевой научно-практической конференции (30 ноября 2023 г.). Кн. 1. -СПб.: НИИ (ВСИ МТО ВС РФ) ВА МТО, 2023 г., с. 547-554
15. Исследование организации технического прикрытия транспортных коммуникаций для восстановления движения в военное время и разработка предложений по совершенствованию системы планирования технического прикрытия транспортных коммуникаций
16. Лещов Г.Ю. Сборник научных статей по материалам VII межведомственной научно-практической конференции «Актуальные вопросы обеспечения обороноспособности и безопасности государства в новых экономических условиях» (10.04.2024) / под редакцией д.э.н., проф. Хачатуряна А.А. – М.: ВУ МО РФ, 2024. – 1 эл. Опт. Диск (CD-ROM) уч. №837с
17. Лещов Г.Ю. О контроле качества подготовки сил обеспечения транспортной безопасности В сборнике: Прокурорский надзор за исполнением законодательства о транспортной безопасности. Сборник материалов круглого стола. Под общей редакцией Т.А. Дикановой. 2019. С. 102-106.

Legal regulation of computer means of information protection and security of transport security systems

Gennadii Yu. Leshchov

PhD in Economics,
Director of the Scientific Research Center for Transport
Expertise of the Russian University of Transport RUT (MIIT)
127994 , 9/9,Obraztsova ul., Moscow, Russian Federation;
e-mail: g-u-l@mail.ru

Yuliya V. Mel'nikova

PhD in Law

Associate Professor of the Chair of Civil Law Disciplines,
Moscow State University of Technology and Management
named after K.G. Razumovsky (First Cossack University)
109004, 73, Moscow, Zemlyanoy Val, Russian Federation;
e-mail: 84995016973@bk.ru

Abstract

The article analyzes modern problems of theory and law enforcement practice related to the use of information and computer tools as means of information protection and protection of transport security systems and technical cover of transport infrastructure facilities. The provisions of legislation on this issue are considered, strengths and weaknesses are explored, author's proposals are formulated to improve the norms of current legislation in the field of information and computer technologies as means of information security and protection of transport systems. A consensus decision has been developed on the possibility of using complex technical and legal means of protection and protection of infrastructure facilities of the transport complex through the use of information and computer tools. The difference between information and computer tools from other, real means of protection and protection in their artificial nature. This virtual system originated and is developing as a set of technical means and devices, while still largely owned by private individuals and interacting with each other through the use of a network of global digital identifiers and a system of protocols for information exchange between devices and means. The main means of existence and development of information and computer facilities is the entrepreneurial activity of individuals in the field of transmission, storage and processing of information, creation and development, development and presentation of software and technical products to the market.

For citation

Leshchov G.Yu., Mel'nikova Yu.V. (2024) *Pravovoe regulirovanie komp'yuternykh sredstv informatsionnoi zashchity i okhrany sistem obespecheniya transportnoi bezopasnosti* [Legal regulation of computer means of information protection and security of transport security systems]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (5A), pp. 239-248.

Keywords

Information and computer technologies, information and computer tools, means of information protection and security, transport security, technical cover, infrastructure facilities of the transport complex.

References

1. On Information, information Technologies and information Protection [Electronic resource]: Federal Law No. 149-FZ of 07/27/2006. Access from the help.-legal system "Consultant Plus" (date of application: 07/19/2024).
2. Palamarchuk A.V. Protection of exclusive rights to the results of intellectual activity on the Internet // *Legality*. 2010, No. 7. Access from the help.- legal system "Consultant Plus" (date of application: 07/19/2024).
3. Shestakov E. Protection of content on the Internet // [http://www.pcweek.ru / themes/ detail.php?ID=111573](http://www.pcweek.ru/themes/detail.php?ID=111573). Access from the help.-the legal system "Consultant Plus" (date of application: 07/10/2024).

4. The Criminal Procedure Code of the Russian Federation [Electronic resource]: No. 174-FZ dated 12/18/2001. Access from the help.-the legal system "Consultant Plus" (date of application: 07/12/2024).
5. Resolution of the Government of the Russian Federation No. 100-4 dated February 17, 2007 "On Approval of the Regulations on the Technical Cover of the infrastructure of Public Railway Transport of the Russian Federation".
6. Decree of the President of the Russian Federation No. 1175 dated October 2, 1998 "On Approval of the Regulations on Military Transport Duties".
7. Decree of the President of the Russian Federation No. 647 dated September 21, 2022 "On the announcement of partial mobilization in the Russian Federation".
8. Agreement on the creation of a unified system of technical cover for Railways of the Member States of the Collective Security Treaty Organization (signed in Dushanbe on April 28, 2003, ratified by Federal Law No. 137—FZ of July 19, 2007, entered into force for the Russian Federation on August 13, 2007)
9. Agreement on cooperation of the member States of the Collective Security Treaty Organization in the field of transportation of military and other formations, their movable property, as well as military products (Concluded in Dushanbe on 09/15/2015)
10. Agreement on the use and development of a network of transport communications for the needs of the economy, military and humanitarian transportation of the member States of the Commonwealth of Independent States States (signed in Minsk on May 31, 2001)
11. Vvedensky I.A. Strategic management and process approach // *Izvestiya RSPU named after A.I. Herzen*. 2009. №117.
12. Vorobyov And Kiselyov V. Prospects of tactics in the XXI century // *Army collection*: — 2008. — February (vol. 164, No. 02). — pp. 18-22.;
13. Key points of preparation and organization of technical cover of transport communications in the Russian Federation
14. Leshchov G.Y. Problematic issues of logistical support for groups of troops (forces) in a special military operation: a collection of materials from the branch scientific and practical conference (November 30, 2023). Book 1. -St. Petersburg: Research Institute (VSI MTO of the Armed Forces of the Russian Federation) VA MTO, 2023, pp. 547-554
15. Research on the organization of technical cover of transport communications for the restoration of traffic in wartime and the development of proposals for improving the planning system of technical cover of transport communications
16. Leshchov G.Y. Collection of scientific articles based on the materials of the VII interdepartmental scientific and practical conference "Topical issues of ensuring the defense capability and security of the state in new economic conditions" (04/10/2024) / edited by Doctor of Economics, Professor. Khachatryan A.A. – M.: VU of the Ministry of Defense of the Russian Federation, 2024. – 1 electronic Opt. Disc (CD-ROM) uch. No.837c
17. Leshchov G.Y. In the collection: Prosecutor's supervision of the implementation of legislation on transport security. Collection of materials of the round table. Under the general editorship of T.A. Dikanova. 2019. pp. 102-106.