

СИСТЕМЫ ФИКСАЦИИ И РАСПОЗНАВАНИЯ НЕСАНКЦИОНИРОВАННОГО ПРОНИКНОВЕНИЯ В ОХРАНЯЕМУЮ ЗОНУ КАК ЭЛЕМЕНТ ЭФФЕКТИВНОЙ БЕЗОПАСНОСТИ ОБЪЕКТА ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ

DOI 10.24411/2072-8735-2018-10086

Кузьмина Наталья Александровна,
Дальневосточный государственный университет
путей сообщения (ДВГУПС), г. Хабаровск, Россия,
Kuznimsprepodavatel@mail.ru

Ключевые слова: транспортная безопасность,
акт незаконного вмешательства, объект
транспортной инфраструктуры, система
безопасности, охрана объекта, нарушитель,
датчики, извещатели.

Ввиду специфики работы транспорт сам по себе является потенциальным источником опасности. А если вторгнуться в его сферу незаконными, агрессивными действиями, опасность становится реальной, грозящей тяжелейшими последствиями. Статистика последних 10-15 лет показывает, что от 50 до 70% совершаемых террористических актов связано с транспортом. Какими-то отдельными мерами обеспечить транспортную безопасность невозможно. К этой проблеме надо подходить комплексно и системно. От обеспечения транспортной безопасности существенно зависит национальная безопасность Российской Федерации. Федеральный закон "О транспортной безопасности" от 9 февраля 2007 г. № 16-ФЗ впервые в отечественной практике поставил вопрос об обеспечении безопасности всей транспортной отрасли Российской Федерации, установил правовые основы деятельности по обеспечению безопасности объектов транспортной инфраструктуры и транспортных средств от актов незаконного вмешательства, в том числе террористической направленности. Впервые предусматривается единый для всех видов транспорта системный подход к антитеррористической защите. Транспорт – весьма уязвимый объект для террористических атак. Имеются в виду сами транспортные средства, транспортные коммуникации, помещения вокзалов, транспортные средства с опасными грузами. Уязвимость транспорта связана с возможностью повреждения средств сигнализации, устройств автоматики и связи, охрана которых с учетом масштабов и протяженности, железных дорог РФ затруднена. Несмотря на проблемные вопросы и объективные трудности в законодательных вопросах при реализации мер по обеспечению транспортной безопасности, работники железных дорог РФ прилагают усилия для обеспечения защищенности ОТИ и ТС от актов незаконного вмешательства. Незамедлительно реагируя на другие вызовы и угрозы, обеспечивают надежное функционирование работы транспортного комплекса, сохраняя тем самым спокойствие и безопасность наших граждан. Рассмотрены вопросы эффективной системы безопасности объектов транспортной инфраструктуры. Большая роль отводится системам, позволяющим зафиксировать факт проникновения посторонних лиц в охраняемую зону объекта.

Информация об авторе:

Кузьмина Наталья Александровна, к.п.н., старший преподаватель кафедры: "Организация перевозок и безопасность на транспорте"
Дальневосточный государственный университет путей сообщения (ДВГУПС), г. Хабаровск, Россия

Для цитирования:

Кузьмина Н.А. Системы фиксации и распознавания несанкционированного проникновения в охраняемую зону как элемент эффективной безопасности объекта транспортной инфраструктуры // Т-Comm: Телекоммуникации и транспорт. 2018. Том 12. №5. С. 47-52.

For citation:

Kuzmina N.A. (2018). Fixing systems and recognition of unauthorized penetration in the protected zone as an element of effective safety of the transport infrastructure object. T-Comm, vol. 12, no.5, pp. 47-52. (in Russian)

Подавляющее большинство совершенных за последние годы террористических актов проведено на объектах транспорта или с использованием транспортных средств. Сегодня уже и простые граждане все чаще говорят о необходимости усиления мер безопасности на транспорте. Здесь речь идет не о безопасности движения, не о техническом и технологическом состоянии объектов транспортной инфраструктуры и транспортных средств. Прежде всего, речь идет об укреплении мер обеспечения транспортной безопасности.

Бесперебойность функционирования транспортного комплекса для любой страны является одним из базовых условий развития экономики, а значит и всего государства. Для нашей страны – это условие возрастает многократно [1].

Несмотря на принимаемые меры субъектами транспортной инфраструктуры и перевозчиками по повышению уровня защищенности транспортного комплекса, угроза совершения актов незаконного вмешательства (АНВ) остается. Сухая статистика констатирует, что, к сожалению, пока полностью исключить возможность совершения АНВ не представляется возможным. В этой связи первоочередной задачей является максимально затруднить попытки совершения АНВ в деятельность объектов транспортной инфраструктуры и транспортных средств и нарушить коварные планы нарушителей.

Федеральный закон №16-ФЗ «О транспортной безопасности» обязывает защищать объекты транспортной инфраструктуры от актов незаконного вмешательства [2].

В условиях экономического кризиса применение Федерального закона ФЗ-16 «О Транспортной безопасности» становится все более затруднительно, тем не менее, пути решения проблем необходимо находить в том числе путем налаживания диалога между органами государственной власти и субъектами транспортной инфраструктуры. Такой подход не предусматривает оценку эффективности принятых мер и способности всей системы противостоять реальным угрозам. И нет никакой гарантии того, что в нештатной ситуации реагирование на нее будет своевременным и корректным [3].

Какой должны быть эффективная система безопасности объекта и как обеспечить их защищенность? Этот вопрос актуален сегодня для многих субъектов транспортной инфраструктуры, перед которыми стоит непростая задача обеспечения транспортной безопасности.

Почему объекты транспортной инфраструктуры – одни из привлекательных мишеней для террористов? Ответ прост – да потому, что в основном цель террора (вытекает из латинских его корней «terroro» – страх, ужас) – посеять панику, запугать, вселить ужас. Внезапная гибель большого количества ни в чем неповинных граждан – что может быть страшнее для простого обывателя? Эксперты признаются, что проблемы транспортной безопасности на железнодорожном транспорте до сих пор остаются не до конца разрешенными, а потому эта транспортная ветвь является главной целью террористов. В этой связи представляется необходимым обеспечить должный уровень защищенности таких объектов от актов незаконного вмешательства (АНВ).

В настоящее время угрозы совершения АНВ в деятельность транспортного комплекса сохраняются, возникают все новые вызовы и способы их осуществления. В этой связи повышение степени защищенности объектов транспортной инфраструктуры железнодорожного транспорта является

задачей комплексной и требует комплексного подхода. В условиях повышения качества услуг железнодорожных перевозок обеспечение гарантированной безопасности, в том числе и транспортной, является стратегическим направлением работы ОАО «РЖД» [4].

При комплексном подходе к обеспечению безопасности на объектах транспортной инфраструктуры причины, повлекшие возможность совершения террористического акта, должны рассматриваться как симптомы неудовлетворительной организации эксплуатации данных объектов, на совершенствование которой требуется направлять основные усилия, людские и материальные ресурсы. Согласно предложению профессором Колорадского университета (США) Д. Питерсоном теории множественности причин возникновения любой нештатной ситуации, можно не только спрогнозировать возможность её возникновения, но и выявить обстоятельства, сделавшие возможным её появление. Следовательно, безопасностью, в том числе и транспортной, не только можно, но и необходимо управлять так же, как и любой другой областью транспортной системы. Обеспечение транспортной безопасности должно представлять собой одну из неотъемлемых, ежедневных функций руководящих и оперативно-управленческих работников различного уровня, такую же, как снижение стоимости, обеспечение требуемого объёма и качества перевозок грузов и пассажиров.

При решении задачи обеспечения безопасности на объектах транспортной инфраструктуры большая роль отводится системам, позволяющим зафиксировать факт проникновения посторонних лиц в охраняемую зону объекта. Для этой цели используются различные системы пультовой охраны, решающие задачи оповещения о факте проникновения на объект с указанием места и времени нарушения границы объекта. Данные системы обеспечивают сбор информации с датчиков, контролирующих места возможного проникновения на объект, фиксацию факта несанкционированного проникновения и передачу сигнала тревоги на пульт управления системой. Системы пультовой охраны часто интегрируются с системами пожарной сигнализации и имеют во многом схожую с ними архитектуру.

В состав системы охраны объекта входит оборудование централизованного управления, приёмно-контрольные приборы (ПКП) или панели (ПКН) и датчики контроля охраняемого объекта. Централизованное управление системой обеспечивает компьютер или заменяющая его в небольших системах специальная панель управления.

Приёмно-контрольные приборы осуществляют питание шлейфов с устанавливаемыми на объекте датчиками, принимают и анализируют передаваемые датчиками сообщения, формируют и передают сигнал тревоги на пункт централизованного управления, управляют оповестительными устройствами и другими системами обеспечения безопасности объекта. На небольших объектах управление всеми системами может осуществляться непосредственно ПКП без передачи информации на пункт централизованного управления.

В системах пультовой охраны для контроля возможных мест проникновения на охраняемый объект используются различные, отличающиеся по типу и принципу действия и решаемой задаче, датчики-извещатели, такие как: магнитные, вибрационные, фотоэлектрические, микроволновые,

ультразвуковые датчики, шлейфы, датчики разбития стекла, датчики движения.

Наиболее простыми, дешёвыми и широко используемыми являются *магнитоконтактные датчики*, устанавливаемые на окна, двери охраняемого объекта. Данные датчики состоят из закрепляемого на подвижной части окна или двери магнитоуправляемого контакта – геркона и постоянного магнита, закрепляемого на раме окна или дверной коробке.

Примером такого датчика может служить накладной малогабаритный магнитоконтактный охранный извещатель ИО-102-14 (СМК-14, геркон), используемый для защиты дверей и окон (рис. 1, а).

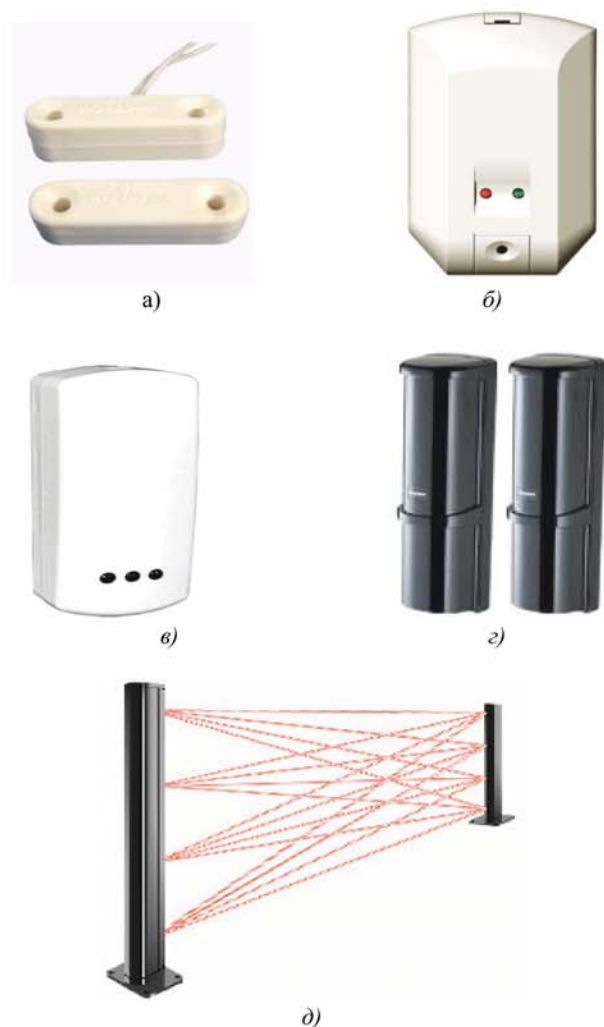


Рис. 1. Охранные извещатели: а – извещатель охранный магнитоконтактный ИО-102-14 (СМК-14, геркон); б – датчик разбития стёкол ИО329-3 Арфа; в – извещатель охранный поверхностный вибрационный «Шорох-2» (ИО-313-5/1); г – четырёхлучевой датчик-барьер инфракрасных лучей NR110QS; д – схема использования лучевых датчиков

Датчики разбития стекла (рис. 1, б) реагируют на звук бьющегося стекла и предназначены для защиты окон охраняемого объекта. Принцип работы датчика основан на анализе спектра фиксируемого шума и его сравнении с запи-

санными в память датчика эталонными звуковыми сигналами. Наиболее совершенные типы датчиков формируют сигнал тревоги при наличии двух факторов: удара по стеклу и звука бьющегося стекла.

Вибрационные датчики (рис. 1, в) фиксируют наличие вибрации и ударов, возникающих при попытке разрушения защищаемого объекта. Принцип действия таких датчиков основан на использовании пьезоэлектрического эффекта или электромагнитной индукции для преобразования сигналов вибрации, подвергающихся разрушению, в анализируемые электрические сигналы.

Фотоэлектрические (лучевые) датчики инфракрасного (ИК) излучения (рис. 1, г, д) используют для защиты коридоров, лестничных пролётов, ворот и входных дверей, а также в системе периметральной охраны объекта.

Действие датчиков основано на образовании барьера из формируемых специальными излучателями для защиты охраняемой зоны объекта системы модулированных инфракрасных лучей. При попадании нарушителя в зону действия барьера выдаётся сигнал тревоги.

Шлейфы систем охранной сигнализации представляют собой наклеиваемую на защищаемый элемент конструкции (стекло, дверь и т. п.) ленту из алюминиевой фольги, включённую в цепь охранной сигнализации. При разрушении конструкции вместе с лентой разрывается цепь охранной сигнализации и формируется сигнал тревоги.

Датчики движения позволяют распознать движение в охраняемой зоне по изменению уровня инфракрасного излучения при перемещении излучающего тепло объекта в зоне чувствительности датчика. По мере движения объекта ИК-излучение попадает на разные сегменты оптической системы, что приводит к формированию ряда импульсных сигналов, фиксируемых электронной системой датчика. Для защиты от ложных срабатываний в современных датчиках движения используется микропроцессорная обработка фиксируемых сигналов. В качестве примера датчиков движения представлены два типа инфракрасных пассивных извещателя семейства «Фотон» (рис. 2).

Наряду с рассмотренными выше типами извещателей для охранной сигнализации также могут использоваться радиоволновые, ультразвуковые, микроволновые, ёмкостные и другие датчики, принцип действия которых основан на анализе отражённого от объекта сигнала или изменения поля и ёмкости охраняемого объекта. Однако означенные датчики получили гораздо меньшее распространение, так как весьма критичны к влиянию изменений окружающей среды, типу охраняемого объекта и наличию различных дестабилизирующих факторов.

От извещателей информация передаётся в другую обязательную структурную составляющую любой охранной системы, роль которой выполняют приёмно-контрольные приборы, а на небольших объектах – приёмно-контрольные панели.

Задачей ПКП является проверка исправной работы оборудования, сбор и анализ поступающей от извещателей информации, передача сигнала тревоги на пульт охраны, управление световой и звуковой оповестительной и пожарной сигнализацией, а также другими техническими устройствами и системами обеспечения безопасности объекта.



Рис. 2. Датчики движения: а – извещатель инфракрасный пассивный «Фотон-9»; б – охранный оптико-электронный извещатель потолочной установки «Фотон-21»

В ПКП обычно совмещаются функции охранной и пожарной сигнализации. Примером ПКП могут служить приёмно-контрольные охранно-пожарные приборы «Кварц», «Радиус», «Сигнал», «Риф» и т. п.

Прибор «Кварц» (рис. 3,а) является довольно простым ПКП и позволяет обеспечить питание и контроль одного шлейфа с включёнными в него охранными или пожарными извещателями.

Прибор также управляет оповещателями и передаёт на пульт центрального наблюдения сигнал тревоги.

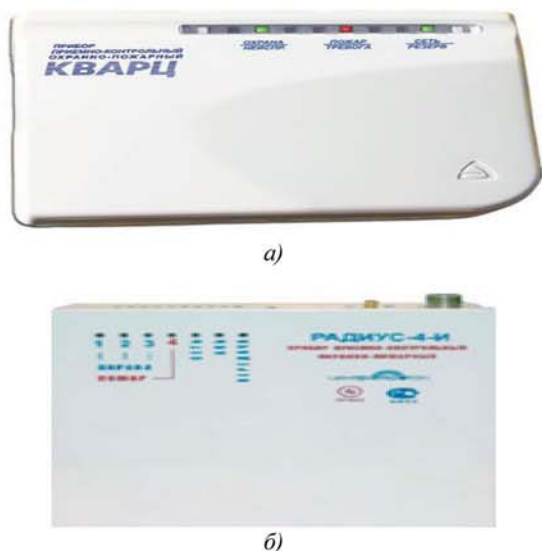


Рис. 3. Приёмно-контрольные приборы: а – «Кварц», б – «Радиус-4И»

Применяемые на железнодорожном транспорте приёмно-контрольные охранно-пожарные приборы «Радиус-4И» (рис. 3) и «Радиус-6И», могут использоваться как при централизованной, так и при автономной охране объектов от несанкционированного доступа и пожаров.

Прибор «Радиус-4И» обеспечивает возможность контроля четырёх, а «Радиус-6И» шести шлейфов с включёнными в них охранными и пожарными извещателями. При получении сигнала от любого из извещателей устройство по каналам связи передаёт сигнал тревоги, а также сигнализирует о проникновении на объект или пожаре световыми и звуковыми сигналами.

В обоих приборах предусмотрена индикация состояния шлейфов с использованием светодиодов. Диапазон рабочих температур прибора составляет от минус 10 до плюс 50°C, что обеспечивает возможность его широкого использования при охране различных объектов.

Для охраны распределённых по территории стационарных объектов используют системы радиоохраны с передачей извещения о проникновении на объект или пожаре по радиоканалу. Одним из примеров такой системы является «Риф Стринг-202». Данная система включает в себя размещаемую в центре охраны базовую станцию, пульт наблюдения и компьютер, а также размещаемые на объектах приёмно-контрольные приборы с передающим устройством. Система позволяет контролировать с одного пульта до 600 устанавливаемых на объектах передающих устройств мощностью 10 мВт.

В зависимости от местности система обеспечивает дальность связи от 25 до 50 и более километров, что достигается использованием сверхвысокочастотных каналов связи и помехоустойчивого кодирования. В системе применена цифровая фильтрация и одновременная, параллельная обработка всех принятых по различным каналам связи сигналов от контролируемых объектов. Передача каждого нового сообщения с объектного приёмно-контрольного прибора осуществляется на новой частоте, случайным образом выбираемой из 1024 заранее запрограммированных частот связи.

Для проверки исправности оборудования каждый объектный передатчик один раз в минуту передаёт на базовую станцию контрольные сигналы. Благодаря использованию лицензируемых частот и передатчиков малой мощности эксплуатация системы «Риф Стринг-202» не предусматривает получения разрешительных документов.

Для полного контроля больших территорий используют системы радиоохраны, также обеспечивающие сбор информации с распределённых по территории объекта датчиков с радиоизвещением. Датчики в данном случае располагаются по всей территории охраняемого объекта таким образом, чтобы расстояние между ними не превышало радиуса действия датчика, при котором обеспечивается обнаружение постороннего объекта и не образуются так называемые мёртвые зоны. При попадании в зону действия датчика человека или постороннего предмета датчик фиксирует факт возникновения нештатной ситуации и посылает по радиоканалу на пульт управления системой сигнал тревоги.

Во многих случаях для обеспечения безопасности любой территории достаточно надёжно контролировать только её периметральные границы, чтобы полностью исключить факт несанкционированного проникновения на данную территорию.

Такие системы получили название периметральных. Данные системы просто незаменимы при охране объектов с большими защищаемыми территориями, таких как аэродромы, базы, транспортные логистические терминалы, а также объектов с большой протяжённостью, таких как железные и автомобильные дороги, трубопроводы и т. п.

Периметральные системы позволяют зафиксировать нарушение границы охраняемой территории и выдать сигнал тревоги намного раньше, чем нарушитель попадёт на расположенные на данной территории особо важные объекты. Данные системы довольно часто конструктивно связаны с физическим ограждением охраняемого объекта, поэтому их работа напрямую зависит от физических характеристик ограждения, его параметров, наличия вибраций, используемого материала, а также от выбора места установки оборудования, качества выполнения монтажных работ и ряда других факторов.

Для надёжной охраны объекта периметральные системы должны отвечать определённым требованиям, таким как:

- полный контроль всего периметра охраняемого объекта и отсутствие «мёртвых зон»;
- высокая чувствительность обнаружения нарушителя;
- низкая вероятность ложных срабатываний;
- надёжная работа в условиях электромагнитных помех от работающего оборудования и расположенных вблизи промышленных объектов;
- надёжная работа в различных климатических условиях.

В настоящее время для обеспечения безопасности объектов наиболее часто используются лучевые, радиоволновые и ёмкостные периметральные системы. Данные системы имеют высокую эффективность обнаружения и позволяют надёжно защитить охраняемую территорию. Однако лучевые системы, например, инфракрасные барьеры, могут эффективно контролировать только прямолинейные участки периметра. Радиоволновые системы критичны к рельефу местности и плохо работают при наличии в охраняемой зоне деревьев или кустарников, что часто имеет место вблизи железных и автомобильных дорог. Ёмкостные системы требуют наличия физического ограждения объекта, так как фиксируют изменение электрического поля и ёмкости при приближении или прикосновении нарушителя к данному ограждению.

Для охраны протяжённых объектов также могут использоваться проводно-радиоволновые системы, представляющие собой два расположенных по охраняемому периметру параллельных фидера. Один фидер выполняет роль приёмной, а другой передающей антенны. При попадании в зону действия поля данных фидеров постороннего предмета происходит возмущение поля, сопровождающееся изменением параметров принимаемого сигнала, постоянно фиксируемых соответствующим оборудованием.

Рассматриваемые системы радиоохраны обычно интегрируются с системами видеонаблюдения, так как требуют идентификации нарушителя, пытающегося проникнуть на охраняемый объект.

Конечно, только человек остается центром принятия решения в системе безопасности. Он следит за состоянием технических средств, получает тревожные сигналы, управляет силами реагирования. Несмотря на четкий и понятный алгоритм действий, неукоснительное соблюдение требований по обеспечению транспортной безопасности на ОТИ и ТС железнодорожного транспорта в нестандартной ситуации может сработать естественный человеческий фактор: утомляемость, усталость, растерянность и даже халатность. И тогда ценой ошибки или промедления в реагировании на угрозы может стать человеческая жизнь [5].

Вполне естественным для руководителей является желание достичь высокого качества систем безопасности и при этом получить максимальный эффект от вложенных средств. Решение существует. Эффективная система управления безопасностью – как хороший солдат и в мирное и в боевое время отвечает за точное и своевременное исполнение возложенных обязанностей и задач. При этом позволяет видеть ситуацию цельно и максимально снижает вероятность ошибки.

Сегодня транспортная система России – важнейшая составляющая инфраструктуры, а ее развитие и обслуживание – одна из приоритетных задач государственной политики [6].

Литература

1. Корниенко А.А. Нормативная правовая база транспортной безопасности // Транспортная безопасность и технологии № 2, 2016. С. 20-24.
2. Федеральный закон №16-ФЗ от 09.02.2007 г. «О транспортной безопасности».
3. Старовойтов А.В. Защищенность объектов транспорта необходимо поддерживать // Транспортная безопасность и технологии. № 2, 2017. С. 100-101.
4. Стратегия развития холдинга ОАО «РЖД» до 2030 года: <http://doc.rzd.ru>. Дата обращения 18.01.2018 г.
5. Постановление правительства РФ от 26.04.2017 г. №495 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищенности объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств железнодорожного транспорта».
6. Поминов И.А. Инфраструктурные проекты в сфере транспорта: Инновации и перспективы // Транспортная безопасность и технологии № 3, 2017. С. 23-25.

FIXING SYSTEMS AND RECOGNITION OF UNAUTHORIZED PENETRATION IN THE PROTECTED ZONE AS AN ELEMENT OF EFFECTIVE SAFETY OF THE TRANSPORT INFRASTRUCTURE OBJECT

Natalia A. Kuzmina,

Far Eastern State Transport University (DVGUPS), Khabarovsk, Russia, Kuznimsprepodavatel@mail.ru

Abstract

Due to the nature of the work, transport itself is a potential source of danger. And if you invade his sphere with illegal, aggressive actions, the danger becomes real, threatening grave consequences. The statistics of the last 10-15 years show that from 50 to 70% of the terrorist acts committed are connected with transport. It is impossible to ensure transport security by any single measures. This problem should be approached in a comprehensive and systemic way. The national security of the Russian Federation depends substantially on ensuring transport security. The Federal Law "On Transport Security" of February 9, 2007, No. 16-FZ, for the first time in the domestic practice raised the issue of ensuring the security of the entire transport industry of the Russian Federation, established the legal framework for ensuring the safety of transport infrastructure and vehicles from acts of unlawful interference, including terrorist orientation. For the first time, a uniform approach for all types of transport to antiterrorist protection is envisaged. Transport is a very vulnerable target for terrorist attacks. Means of transport means, transport communications, premises of stations, vehicles with dangerous cargoes are meant. Vulnerability of transport is associated with the possibility of damage to signaling devices, automation and communication devices, whose protection, given the scale and extent, is difficult for the railways of the Russian Federation. Among other modes of transport, rail transport, as in many industrialized countries, takes a leading place.

A considerable number of terrorist acts committed in recent years have been committed at transport facilities or using vehicles. Dry statistics are inexorable and international and domestic sources testify to this. Therefore, the protection of transport infrastructure (OTI) objects and vehicles (TC) from acts of unlawful interference (ANV), especially committed intentionally, in the form of terrorist acts and sabotage, has become one of the most pressing problems in the world in recent years. Transportation facilities are most attractive to terrorists, as are other places of large crowds. Terrorist threats and attacks on transport have a great public resonance and bear serious consequences, violating the rhythm of the transport complex, affect the livelihoods of many people, cities and even countries. Today, even ordinary citizens are increasingly talking about the need to strengthen security measures for transport. Here, first of all, we are talking about strengthening the state system of measures to ensure transport security.

Despite the problematic issues and objective difficulties in legislative matters in the implementation of measures to ensure transport security, Russian railways employees make efforts to ensure the protection of the OTI and the TC against acts of unlawful interference. Immediately responding to other challenges and threats, ensure the reliable functioning of the transport complex, thereby preserving the peace and security of our citizens. This article discusses the issues of an effective security system for transport infrastructure facilities. A large role is assigned to systems that allow to detect the fact of penetration of unauthorized persons into the protected area of the facility.

Keywords: *transport security, act of unlawful interference, object of transport infrastructure, security system, object protection, intruder, sensors, detectors.*

References

1. Kornienko A.A. (2016). Normative legal basis of transport safety. *Journal Transport safety and technology*, vol. 145, no. 2, pp. 20-24.
2. Federal Law No. 16-FZ of 09.02.2007 "On Transport Security". Date of circulation 22.12.2017.
3. The development strategy of JSCO "Russian Railways" holding until 2030 y.e. Date of circulation 18.01.2018.
4. Decree of the Government of the Russian Federation of April 26, 2017 No. 495 On approval of requirements for ensuring transport security, including requirements for antiterrorist protection of facilities (territories) that take into account the security levels for various categories of transport infrastructure and transport vehicles.
5. Pominov I.A. (2017). Infrastructural projects in the sphere of transport: Innovations and prospects. *Journal Transport safety and technology*, no. 3, pp. 23-25.

Information about author:

Natalia A. Kuzmina, *Candidate of pedagogical sciences, senior lecturer of the department: "Organization of transport and transport safety" of the Far Eastern State Transport University (Khabarovsk, Russia). Far Eastern State Transport University (DVGUPS), Khabarovsk, Russia.*