BSI Consulting и TT Club Отчёт о хищениях грузов за 2024 год

Апрель 2025

bsi Your partner in progress

TT

Содержание

Введение

BSI Consulting и TT Клуб совместно подготовили ежегодный отчёт о хищениях грузов, цель которого — представить анализ глобальных данных, который демонстрирует новые угрозы для цепочек поставок и особенности преступной активности. Анализируя данные, собранные в течение года, мы предлагаем посмотреть, как изменяющийся характер рисков влияет на логистическую отрасль.

Профиль рисков в цепочке поставок постоянно меняется под воздействием макроэкономических и географических факторов, цен на сырьё, экономической политики отдельных стран и колебаний объёмов перевозок. При этом преступные группы быстро адаптируют свои подходы к хищениям грузов, действуя более скоординированно, применяя глубокие знания логистики, современные технологии и продуманные схемы обхода мер безопасности. Надеемся, что данный отчёт станет для вас полезным источником практической информации, которая поможет укрепить безопасность вашего бизнеса и глобальных цепочек поставок.

Глобальные тенденции хищений грузов

Данные за 2024 год свидетельствуют о стремительных изменениях в характере краж грузов, вызванных развитием преступных методов и появлением новых целей. Наиболее часто похищаемой категорией грузов стали продукты питания и напитки — на них пришлось 22% всех инцидентов. Далее следуют сельскохозяйственная продукция (10%), электроника (9%) и топливо (7%). В 76% случаев хищения были связаны с автомобильным транспортом. По видам преступлений лидируют захваты транспортных средств (21%), за ними следуют угоны самих транспортных средств (20%), хищения с объектов (16%) и хищения из транспортных средств (14%).

Большинство краж (41%) произошло в пути. Ещё 21% инцидентов связан со складами, а остальные приходятся на производственные объекты, точки доставки, стоянки и прочие места. Географически наибольшая преступная активность отмечена в Бразилии, Мексике, Индии, США, Германии, Чили и Южной Африке. Наибольшее количество инцидентов было зафиксировано в первом и четвёртом кварталах года.

Одной из наиболее заметных тенденций года стал рост так называемых стратегических хищений, на долю которых в США приходится уже 18% всех инцидентов. Этот вид краж связан с обманом, мошенничеством и тщательной предварительной подготовкой. Преступники прибегают к таким методам, как подделка документов, выдача себя за других лиц, а также используют технологии искусственного интеллекта для фальсификации коносаментов и дистанционного вмешательства в онлайн-операции. Подобные схемы свидетельствуют о растущей степени организованности преступных группировок и их понимании слабых мест в цепочках поставок. Наибольшую уязвимость по-прежнему представляют склады и транзитные пункты, которые подвергаются хорошо скоординированным атакам.

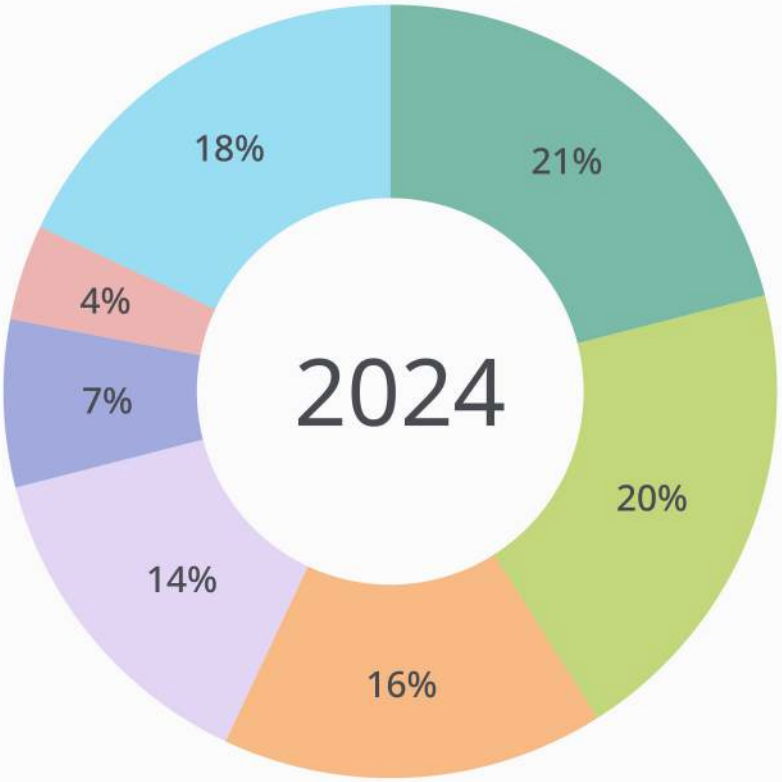
Кроме того, всё чаще фиксируются преступления с использованием интернет-технологий. Преступники применяют искусственный интеллект (ИИ) для создания фишинговых писем, дипфейков и вредоносных программ, которые открывают доступ к конфиденциальной информации о грузах. Участившиеся атаки на облачные хранилища данных говорят о том, что злоумышленники быстро адаптировались к современным технологиям. Увеличение доли стратегических и интернет-хищений приводит к необходимости инвестиций в передовые меры безопасности и эффективные практики управления рисками, позволяющие защитить операционную деятельность компаний.

Глобальные тенденции 2024 года

На основе последних данных об инцидентах, собранных в рамках сотрудничества и партнёрства с правоохранительными органами, государственными и негосударственными структурами, коммерческими организациями, отраслевыми ассоциациями, открытыми источниками, а также на основании информации от консультантов BSI и приглашённых экспертов.

Виды хищений

- Нападение на ТС
- Кража ТС
- Кража со склада
- Кража изТС
- Кража из контейнера/прицепа
- Кража сотрудником
- Другое



Наиболее часто похищаемые категории грузов

22%	10%	9%	7%	5%	5%	42%
Продукты питания и напитки	Сельхоз-продукция	Электроника	Топливо	Автомобили	Стройматериалы	Другое

Страны с наибольшим числом хищений

Хищения в разных сегментах транспортировки

Глобальные тенденции 2023 vs. 2024

На основе последних данных об инцидентах, собранных в рамках сотрудничества и партнёрства с правоохранительными органами, государственными и негосударственными структурами, коммерческими организациями, отраслевыми ассоциациями, открытыми источниками, а также на основании информации от консультантов BSI и приглашённых экспертов.

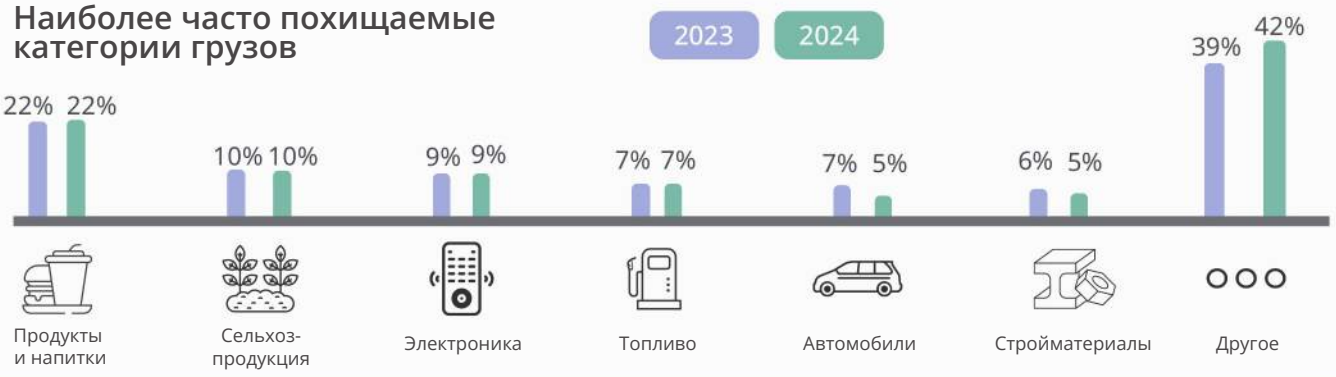
Виды хищений

Сегменты транспортировки

- Авто
- Склады
- Море
- Обработка
- Ж/д
- Другое

						Другое
2023	68%	26%	2%	2%	1%	1%
2024	76%	18%	2%	1%	2%	1%

Наиболее часто похищаемые категории грузов



Стратегические хищения и кризис в США

Тенденции хищений грузов в США имеют уникальный и вызывающий тревогу характер по сравнению с другими регионами. Это обусловлено широким распространением стратегических методов хищения, уязвимостью технологической инфраструктуры, участием инсайдеров и нацеленностью на высокоценные категории товаров, такие как электроника, фармацевтическая продукция и товары народного потребления. Эти факторы подчёркивают серьёзные трудности, с которыми сталкиваются участники цепочек поставок при обеспечении безопасности на фоне всё более сложных преступных схем.

Электроника лидирует среди похищаемых товаров в США, составляя 19% от общего числа инцидентов. Далее по частоте хищений идут продукты питания и напитки, алкоголь и почтовые отправления. 79% краж происходит во время транспортировки грузов, 13% краж приходится на инциденты на складах во время хранения и обработки.

В последние годы в США наблюдается рост стратегических хищений грузов — они составляют сейчас около 18% всех зафиксированных случаев. Подобные преступления основаны на мошеннических действиях и использовании высокотехнологичных инструментов, с помощью которых реализуются сложные и хорошо организованные схемы. Высоколиквидные грузы, такие как электроника, одежда и фармацевтика, особенно уязвимы перед этими методами, поскольку организованные преступные группы продолжают совершенствовать средства проникновения в уязвимые участки логистических процессов.

Изначально эпицентром стратегических хищений в США была Калифорния, однако постепенно проблема распространилась по всей стране. Сообщения о подобных инцидентах поступают из Иллинойса, Индианы, Огайо, Кентукки, Луизианы и Пенсильвании. Расширение географии подобных краж отражает рост влияния организованных преступных сетей и появление новых игроков, использующих мошеннические технологии. Разные секторы — от пищевой и металлургической промышленности до потребительских товаров и текстиля — уже столкнулись с последствиями стратегических хищений.

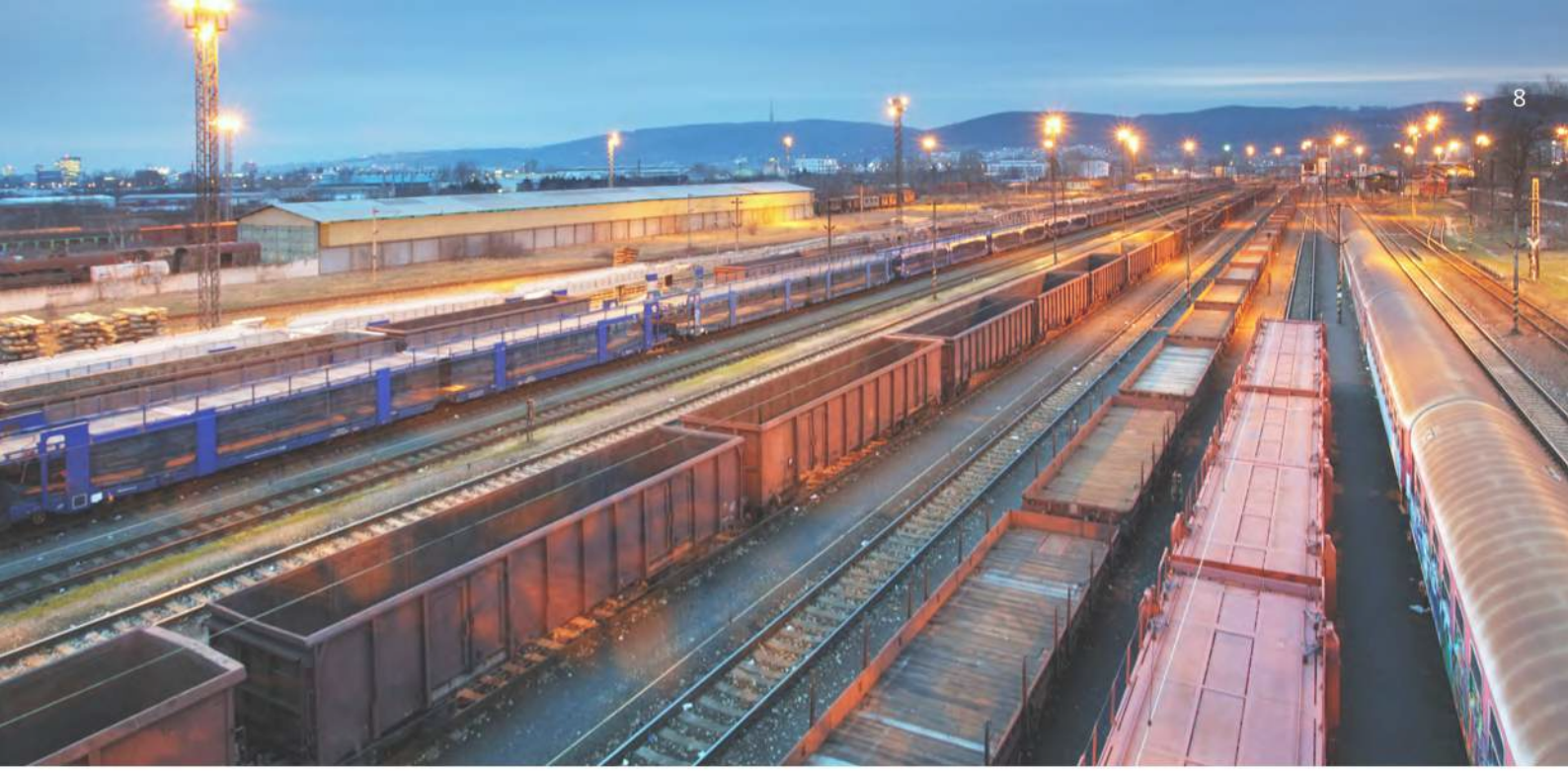
Проблема усугубляется участием инсайдеров: преступники используют доступ к конфиденциальной информации для выявления и перехвата особо ценных грузов. Существенную роль в современных схемах хищений играет и киберпреступность, позволяющая злоумышленникам использовать слабые места в технологических системах. Совокупность всех этих факторов указывает на то, что хищение грузов становится всё более сложным и непредсказуемым риском для логистики.

Кейс: рост угрозы мошенничества в цепочках поставок

За последние годы уровень мошенничества значительно возрос. Пандемия COVID-19 ускорила переход к цифровизации, что привело к резкому росту онлайн-покупок, банковских операций и других транзакций онлайн. Преступники постоянно улучшают схемы атак на цепочки поставок. По некоторым оценкам,онлайн-мошенничество превратилось в индустрию с глобальным оборотом около 500 млрд долларов США, что сопоставимо с масштабом незаконного оборота наркотиков.

Преступления, связанные с использованием компьютерных технологий, включают несанкционированный доступ к системам и данным. Цепочки поставок в значительной степени зависят от эффективной и безопасной работы ИТ-систем — будь то системы управления транспортировкой, складские системы или каналы внутренней связи. Это создаёт множество источников информации, к которым преступники стремятся получить доступ, чтобы завладеть грузом. Этот вид мошенничества крайне рентабелен: достаточно телефонной линии и подключения к интернету, чтобы действовать в глобальном масштабе без физических ограничений. Порог входа в эту преступную деятельность низкий, а потенциальная выгода высока.

Даже простая стратегия «остановись и оцени» может помочь своевременно выявить попытку мошенничества.



Кражи на железной дороге в США

Доля краж с железнодорожного транспорта в США выросла с 3 % в 2023 году до 6 % в 2024-м, что свидетельствует о нарастающем характере проблемы. Преступники демонстрируют возрастающую тактическую осведомлённость: в Калифорнии группировки планируют свои действия с учётом расписаний движения поездов и графиков смен, что значительно повышает успешность их операций.

Хищения в разных сегментах транспортировки в США

- Грузовик
- Склад/терминал
- Ж/д
- Фургон
- Море

2023	79%	14%	3%	3%	1%
2024	79%	13%	6%	2%	0%

Южная Калифорния, куда поступает значительный объём грузов через региональные порты, особенно уязвима. Медленно движущиеся поезда в таких городах, как Лос-Анджелес, становятся лёгкой мишенью, особенно из-за нехватки охранного персонала и устаревших замков. Однако проблема уже вышла за границы одного региона: высокий уровень риска сохраняется также в Иллинойсе и Теннесси, где терминалы и сортировочные станции часто становятся объектами нападений. Здесь контейнеры могут стоять без движения длительное время, а меры безопасности нередко недостаточны. В отличие от автоперевозок, где грузы обычно находятся под присмотром водителей или охраны, железнодорожные перевозки часто не контролируются на протяжении всего маршрута, что даёт преступникам возможности для хищений.

Наиболее привлекательными для похитителей остаются ценные грузы: в первую очередь электроника, затем — автозапчасти и обувь. Компании постепенно внедряют различные технологии снижения рисков: от систем отслеживания груза в реальном времени и пломб, соответствующих стандарту ISO, до мобильных охранных групп. Эти решения позволяют точечно усиливать защиту конкретных объектов и видов грузов, стараясь опережать всё более организованных и изобретательных преступников.

Кейс: организованные преступные группы, нападающие на поезда в пути следования в Калифорнии и Аризоне

По данным правоохранительных органов, организованная преступная группа, действующая из Синалоа (Мексика), совершает хищения с грузовых поездов, следующих через малонаселённые районы Калифорнии в сторону Аризоны. Преступники выбирают момент, когда поезд останавливается в сортировочной зоне, и взбираются на подвижной состав. Зафиксированы случаи вмешательства в работу тормозной системы и сигнальных устройств, в результате чего поезд вынужденно останавливается. Такая тактика не только наносит физический ущерб поезду, но и создаёт угрозу безопасности локомотивных бригад. Одновременно с этим другие участники группы следуют за составом на автомобилях, в которых вывозят похищенные товары.

Характер хищений указывает на высокий уровень организации: преступники обладают информацией о грузе, замках и других средствах защиты, что позволяет им целенаправленно охотиться за ценными товарами, включая электронику, обувь и инструменты. Смещение фокуса на сельские районы очевидно связан для преступников с меньшим риском обнаружения. Даже в тех случаях, когда сотрудники железной дороги становятся свидетелями краж, внутренние инструкции запрещают им вмешиваться, чтобы избежать возможных травм — особенно если злоумышленники вооружены.

Хищения грузов в Южной Африке

Южная Африка входит в число стран с наибольшим количеством хищений грузов в мире и занимает первое место на континенте, что серьёзно влияет на экономику региона. Автоперевозки остаются зоной самого высокого риска, с самый арспростарненный вид краж — угоны грузовиков с грузом. Зачастую насильственные нападения совершают хорошо организованные группы, нередко выдающие себя за полицейские патрули. Помимо угонов фиксируются кражи со складов, при железнодорожных и авиаперевозках. В 2024 году лидировали регионы Гаутенг, Квазулу-Натал, Восточный Кейп, Мпумаланга и Западный Кейп. Особую опасность представляет внутренняя угроза: коррумпированные сотрудники могут участвовать в хищениях или передавать информацию о маршрутах и мерах безопасности. Известны случаи имитации угонов и участия охранников. Чаще всего в 2024 году похищали продукты питания и напитки, посылки, животных, алкоголь и топливо.

Для противодействия угрозам необходимо действовать проактивно: проверять персонал, усиливать меры безопасности и инвестировать в современные технологии.

Кейс: кражи металлов в Южной Африке

На протяжении последних лет фиксируются кражи различных металлов — как правило, это ценные грузы, на которые преступники нацеливаются на этапе автомобильной перевозки к порту отправки. Чаще всего такие партии перевозятся в контейнерах на большие расстояния, нередко нападения сопровождаются захватом транспортных средств с применением силы.

Особую обеспокоенность вызвал недавний инцидент с участием инсайдеров, предоставивших доступ к грузу. Отправка включала процедуру взвешивания под контролем независимой стороны, однако девять контейнеров, вышедших с объекта в разные дни, так и не прибыли в порт. Расследование показало, что кражи здесь происходили и раньше: слабые места в управлении запасами, в частности возможность ручного ввода данных, приводили к задержкам сверки и позволяли вывозить груз без немедленного обнаружения. Кроме того, не проводились проверки надёжности перевозчиков, забирающих груз.

Низкий уровень охраны изначально позволял совершать мелкие хищения, которые переросли в организованную деятельность. Участники группы предлагали сотрудникам деньги за информацию и доступ к грузу, в результате девять грузовиков получили разрешение на вывоз контейнеров, которые впоследствии исчезли.

Тенденции хищений грузов в Европе

Уровень краж грузов в Европе в целом остался стабильным по сравнению с предыдущими годами. Чаще всего целью становились товары высокого спроса: продукты питания и напитки (12%), электроника (12%), металлы (9%) и алкоголь (7%). Рост числа инцидентов указывает на слабые места в цепочках поставок по всему региону. Организованные преступные группы продолжают охоту на грузы, которые легко реализовать, что подчёркивает необходимость усиления безопасности на всех этапах транспортировки.

Склады оказались наиболее уязвимыми объектами — на них приходится 41% всех инцидентов. Много краж также произошло на стоянках, в зонах отдыха и на обочинах. Основные методы: кражи с объектов, из контейнеров и прицепов, угоны и тактика «режь и хватай» (slash-and-grab).

Наибольшее число краж зафиксировано в Германии, Великобритании, Италии, Испании и Франции. Основные цели преступников — припаркованные транспортные средства на неохраняемых площадках и плохо защищённые склады. Также мы отмечаем рост технологически сложных преступлений, как в США. Так, в Австрии груз медных болтов, направлявшийся во Францию, был перенаправлен с помощью поддельных инструкций по доставке, что привело к ущербу в размере шестизначной суммы долларов США.

Высоким остаётся риск для водителей. В окрестностях Милана была арестована группа, нападавшая на водителей во время обязательных перерывов. Использовались разные тактики: разрезание тентов на полуприцепах, взлом замков и насильственные действия, включая похищения.

Эти инциденты демонстрируют растущую сложность и опасность краж грузов в Европе и подчёркивают необходимость срочного усиления мер безопасности, обучения водителей, создания защищённых зон отдыха и инвестиций в технологии для защиты имущества и персонала.

Кейс: кражи с движущихся транспортных средств в Европе

На протяжении последних лет в Европе и за её пределами фиксируются случаи, когда преступники проникают в грузовой отсек грузовиков прямо во время движения. Из всех вмешательств в цепочку поставок этот вид краж представляет наибольший риск как для водителей, так и для самих злоумышленников.

Узнайте больше о кражах с движущихся ТС

За последние 12 месяцев подобные инциденты отмечены в ряде стран Европы и Великобритании. Помимо очевидной опасности, такие преступления особенно трудно расследовать: записи водителя и данные маршрута обычно не фиксируют несанкционированную остановку, поэтому невозможно точно установить момент хищения. Кража обнаруживается лишь в пункте доставки, часто спустя несколько дней, когда груз и преступники уже далеко.

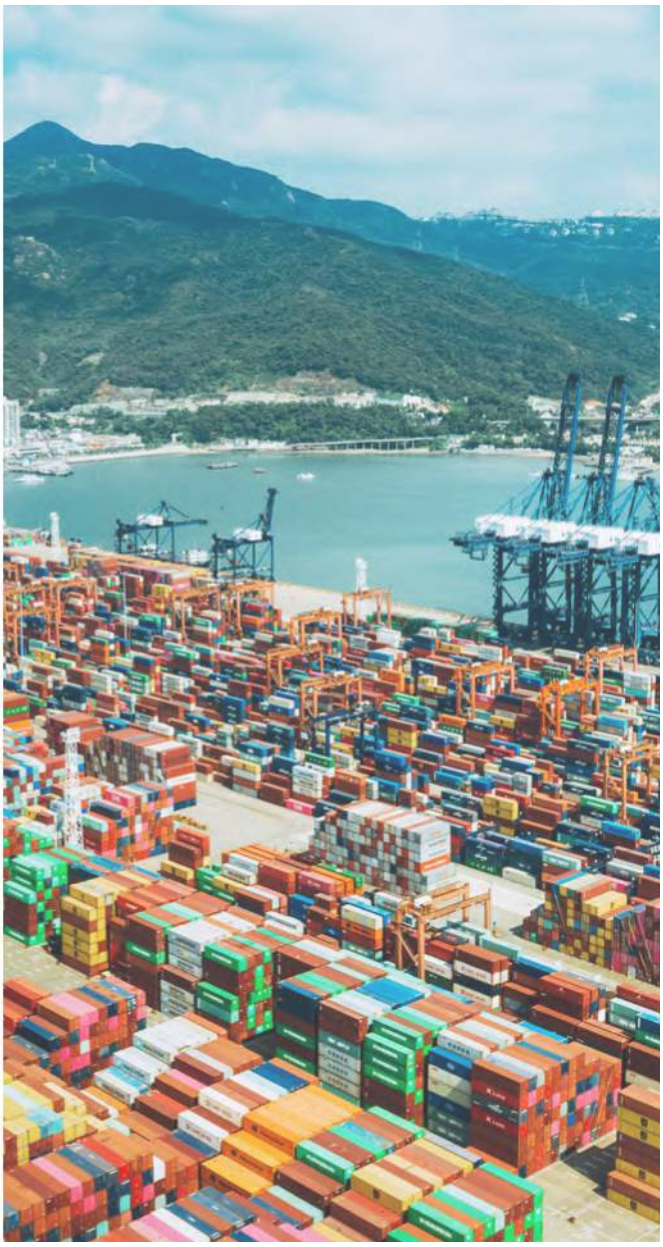
Нападения тщательно планируются. Преступники выбирают только те транспортные средства и грузы, которые оправдывают риск. Часто они прибегают к помощи инсайдеров — сотрудников складов, закрепляющих GPS-устройства, диспетчеров, подтверждающих наличие груза, или даже водителей, которые сознательно меньше сопротивляются нападению.

Риски можно снизить на нескольких уровнях. Ключевые меры:

- повышение осведомлённости о внутренней угрозе и проведение тренингов;
- надёжное управление информацией и контроль доступа;
- обучение водителей методам распознавания угроз и реагирования на подозрительные ситуации.

Мелкие кражи, участие инсайдеров и хищение фармацевтической продукции в Индии

Грузоперевозки по территории Индии сопряжены с множеством рисков. По итогам прошлого года наибольшее число краж зафиксировано в штатах Уттар-Прадеш, Мадхья-Прадеш, Раджастхан, Харьяна и Бихар. Цепочки поставок сталкиваются с инсайдерской угрозой, спонтанными мелкими кражами и целенаправленным хищением ценных грузов, включая фармацевтическую продукцию.



Согласно данным BSI Consulting, не менее 26 % краж грузов в Индии в 2024 году сопровождались участием инсайдеров. Коррумпированные сотрудники складов взаимодействуют с организованными группами, передавая им информацию о протоколах безопасности и помогая обходить охранные системы. Они также могут вступать в сговор с водителями, загружая дополнительный груз и подделывая документы. Подобные схемы приводят к системным хищениям и значительным убыткам. Вмешательство инсайдеров делает логистику более уязвимой и серьёзно подрывает безопасность цепочек поставок. В сочетании со случаями нападений на водителей такие схемы иллюстрируют сложный характер риска и подчёркивают необходимость усиленного контроля персонала.

Мелкие хищения также остаются актуальной угрозой. Их распространённости способствует слабая защита груза, например, использование тентов. В 2024 году чаще всего похищали продукты питания, напитки, сельхозпродукцию и электронику. Особенно уязвимы грузы, оставленные на ночных стоянках у заправок, где воры берут то, что проще украсть. Дополнительный фактор риска в Индии — неудовлетворительное состояние дорог и опасная манера вождения: перевернувшиеся или замедлившиеся транспортные средства становятся лёгкой добычей.

Как один из крупнейших мировых производителей фармацевтической продукции, Индия сталкивается с особыми рисками в этом сегменте. Хотя такие кражи случаются относительно редко, их последствия крайне серьёзны. В декабре 2024 года зафиксированы три инцидента: два нападения на грузовики в пути и один случай с припаркованным автомобилем. Эти события демонстрируют уязвимость транспортных процессов, особенно при слабой физической защите и неохраняемых стоянках. Ситуацию осложняют коррумпированные водители, инсценирующие нападения, что затрудняет оценку масштабов проблемы.

Учитывая значимость фармацевтических поставок для глобальных цепочек жизнеобеспечения, устранение этих рисков остаётся задачей первостепенной важности.

Нападения на водителей и захваты транспортных средств в Южной Америке

В 2024 году страны Южной Америки столкнулись с серьёзной проблемой хищения грузов. Наибольшее количество инцидентов зафиксировано в Бразилии, на долю которой пришлось 68 % всех случаев. За ней следуют Аргентина, Чили и Перу, при этом Аргентина занимает второе место (12 %). Наиболее распространённым способом хищения остаётся угон транспортного средства — 33 % случаев. Преступления нередко сопровождаются насилием: водителей запугивают, избивают, похищают и даже убивают.

Развитие технологий стало одновременно инструментом и ареной противостояния. Системы GPS и блокировки двигателя позволяют отслеживать автомобили и при необходимости останавливать их, что способствует возврату похищенных грузов. Однако преступные группы адаптируются, используя глушители GPS-сигнала и взламывая аккаунты перевозчиков для фиктивных заявок на забор груза. В 2024 году в Бразилии зафиксировано несколько подобных случаев.

Экономические трудности и проблемы с инфраструктурой лишь усугубляют ситуацию. Плохое состояние дорог в Бразилии, Аргентине и Чили приводит к частым опрокидываниям грузовиков, что провоцирует мелкие хищения со стороны местных жителей. Экономический кризис в Аргентине также способствует росту преступности: безработица и низкий кровень жизни трудоустройства толкают людей к незаконным действиям. Влияние наркокартелей в Эквадоре усугубляет ситуацию и провоцирует рост преступлений, среди которых и кражи грузов.

В такой обстановке компаниям важно сохранять бдительность и постоянно обновлять меры защиты своих поставок.

Стратегии снижения рисков от BSI Consulting и TT Клуба

BSI Consulting и TT Club подготовили настоящий отчёт для анализа новых тенденций и угроз в цепочках поставок в 2024–2025 годах. Мы предлагаем подходы к снижению рисков, чтобы помочь организациям лучше понимать угрозы и формировать устойчивую логистику.

Рекомендуемые меры по снижению рисков хищений

- **Для пользователей онлайн-платформ и бирж перевозок:**

Продуманно публикуйте информацию — она может быть интересна злоумышленникам. Будьте осторожны с «выгодными» предложениями. Тщательно проверяйте перевозчиков, работающих вне платформы.

- **Для водителей и перевозчиков:**

Заранее планируйте маршрут с безопасными местами для остановки. В приоритете — охраняемые, освещённые площадки с ограждением и контролируемым въездом. Выявляйте зоны повышенного риска и исключайте остановки в них.

- **Управление информацией и оценка рисков:**

Определите, какие данные наиболее ценны для преступников, и защитите их. Информация о маршрутах и GPS-координатах особенно опасна в случае утечки и должна распространяться только по принципу «необходимости знания».

- **Для электронной почты:**

Не открывайте письма и вложения от неизвестных отправителей. Компании должны обучать сотрудников распознаванию фишинга. Помните: адрес отправителя может быть подделан. Если письмо от партнёра содержит просьбу ответить на другой адрес — это тревожный сигнал.

- **Управление складскими запасами:**

Чтобы снизить риск мелких хищений, необходим строгий контроль запасов. Эффективны выборочные проверки, ограничение доступа к учётной системе и разграничение прав пользователей.

- **Принятие грузов:**

Проверяйте, соответствует ли накладная фактическому объёму. Подделка документов может обеспечить длительный несанкционированный доступ к грузу. Все поступления должны сканироваться и учитываться поштучно, а не партиями.

Оценка операционных рисков

«Если предложение выглядит слишком выгодным, чтобы быть правдой — скорее всего, это обман»

Оценка операционной деятельности
Отправной точкой для оценки является понимание собственных операционных потребностей. Например:

- средний объём перевозимых грузов
- типичные точки загрузки и выгрузки
- сезонные колебания спроса (периоды пиков и спадов)
- среднее количество доступных перевозчиков
- размещение заказов на онлайн-биржах (следует использовать с осторожностью)
- подтверждённая стоимость груза должна соответствовать или быть ниже лимитов, установленных в контракте с клиентом, ещё до принятия груза к перевозке и назначения перевозчика.

Понимание этих параметров позволяет провести оценку рисков и выстроить устойчивую стратегию. Такая оценка уникальна для каждого участника цепочки поставок и ведёт к формированию индивидуальных требований к безопасности.

Анализ операционной нагрузки помогает определить, какие процессы целесообразно выполнять вручную, а какие — автоматизировать. Несмотря на начальные и постоянные затраты, связанные с внедрением автоматизированных решений, их применение может быть оправданным при сравнении с затратами рабочего времени персонала на выполнение тех же задач вручную, а также при оценке надёжности ручных процессов. Процесс оценки подрядчиков в зависимости от характера и объёма текущей операционной загрузки можно также частично или полностью передать на аутсорсинг.

В отдельных случаях следует сузить круг проверенных перевозчиков, с которыми компания работает на постоянной основе. Проводить тщательную проверку тысяч подрядчиков гораздо сложнее, чем проверять несколько сотен. Кроме того, заметить изменения в поведении перевозчика, с которым компания работает нерегулярно, гораздо труднее, чем при работе с постоянными партнёрами.

Надлежащая проверка контрагентов (Должная осмотрительность)

После выработки стратегии управления рисками необходимо внедрить процедуры проверки благонадёжности подрядчиков. Они зависят от размера компании и уровня выявленных рисков, но должны соблюдаться неукоснительно. Поскольку аномалии неизбежны, важно назначить ограниченный круг уполномоченных лиц с правом оперативных решений. Также необходима чёткая процедура эскалации инцидентов с учётом пиковых периодов, выходных и праздников, чтобы обеспечить круглосуточное реагирование.

Проверка и фильтрация партнёров и подрядчиков. Проверку можно проводить вручную силами компании, полностью передавать на аутсорсинг или реализовать гибридный формат, когда сторонний поставщик услуг взаимодействует с компанией для достижения результата.

Централизованные базы данных (central databases). Существуют специализированные базы, такие как Registry Monitoring Insurance Services (RMIS) и Федеральная администрация автотранспортных перевозок США (FMCSA / Safer), которые используют для получения сведений о потенциальных рисках.

Процедуры и технологии безопасности перевозчиков. Необходимо оценивать меры безопасности и цифровые инструменты, применяемые подрядчиком. Например, использование электронных регистраторов маршрутов (ELD) требует предварительной юридической консультации и закрепления требований в договорных документах.

Стандартные операционные процедуры. Перевозчики могут заранее предоставлять список VIN-номеров используемых тягачей. Эти данные помогают проверить водителя, прибывшего за грузом, и убедиться, что выдача осуществляется уполномоченному лицу. Если VIN недоступен, минимальный набор сведений включает регистрационный номер, марку, год выпуска тягача и номер прицепа.

Подход, основанный на правилах. На основе анализа внешних баз можно выстроить критерии фильтрации, например, требование, чтобы перевозчик работал не менее года и не менял регистрационные данные на сайте FMCSA в течение последних шести месяцев. Такой подход позволяет отсеивать фиктивные компании и мошенников.

Мониторинг и реагирование. На рынке существует множество решений для отслеживания и мониторинга, которые могут служить дополнительным уровнем защиты. Однако компания должна определить, кто отвечает за анализ информации и какое реагирование считается адекватным. Злоумышленники нередко «тестируют» системы безопасности, и если сигнал тревоги остаётся без ответа, они продолжают действовать, игнорируя наличие технологий.

Киберпреступность и интернет-мошенничесвто

Использование деловой электронной почты в мошеннических целях остаётся серьёзной проблемой для компаний. Методы преступников эффективны, особенно там, где нет базового уровня осведомлённости и технической защиты. Существует ряд стратегий, позволяющих снизить такие риски.

Бдительность. Автоматизированные решения могут быть слишком дорогими для небольших компаний, поэтому важно выстраивать чёткие процедуры ручной проверки входящих писем, поиска несоответствий и отклонений от условий. Сотрудники, отвечающие за заказы на перевозки, должны пройти обучение по информационной безопасности и знать порядок действий при выявлении подозрительных признаков. Любой сигнал должен передаваться назначенному ответственному лицу.

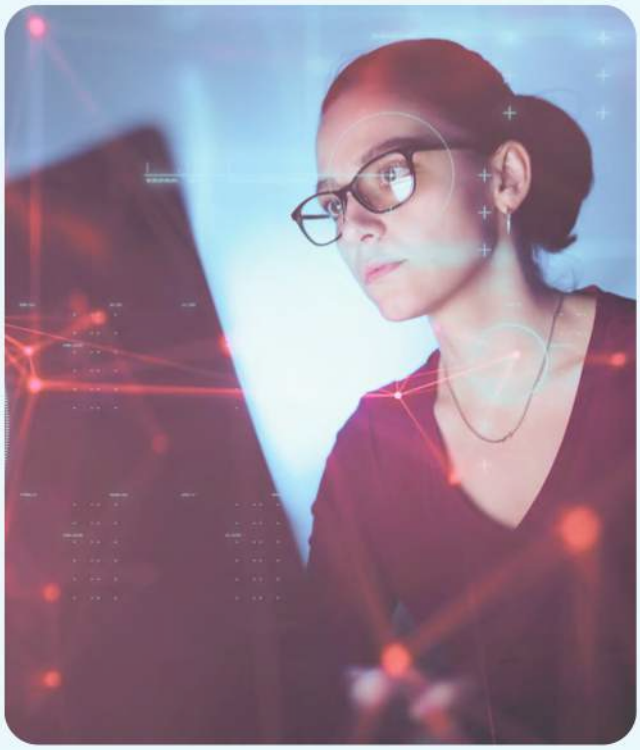
Онлайн-биржи грузоперевозок представляют интерес для злоумышленников. Необходимо критически относиться к объёму и характеру публикуемой информации, которая может быть использована в преступных целях. Следует настороженно относиться к подозрительно выгодным предложениям и высокой пропускной способности, заявленной от одного источника. Перевозчики, работающие вне платформы, должны проходить тщательную проверку.

ИТ-решения. Существуют специализированные программные решения, которые обеспечивают высокий уровень защиты для бизнеса. Такие системы можно интегрировать в стандартные офисные пакеты, например Microsoft 365, — они работают параллельно и обеспечивают защиту от широкого спектра угроз, настраиваемых в соответствии с потребностями компании. Эти решения способны автоматически сигнализировать в следующих случаях:

- **Опечатки в именах доменов.** Преступники рассчитывают, что незначительное изменение известного адреса почты изменение останется незамеченным, и они смогут вести переписку от имени, например, перевозчика.
- **Создание фальшивых доменов.** Суть метода — создание нового электронного домена для маскировки под контрагента. Злоумышленники выбирают цель, регистрируют новый домен, через который ведётся переписка. После совершения хищения этот домен закрывается.
- **Блокировка IP-адресов.** Поскольку многие атаки ведутся из-за рубежа, можно ограничить приём электронной почты только с IP-адресов стран, с которыми компания реально взаимодействует, и блокировать всю остальную входящую корреспонденцию.
- **Аутентификация домена (DMARC — Domain-based Message Authentication, Reporting and Conformance).** Этот протокол помогает предотвратить подмену доменных имён в электронных письмах.
- **Фишинг, спарфишинг, компрометация деловой переписки.** С применением технологий на основе искусственного интеллекта возможно распознавание стилевых особенностей переписки, идентификация сторон и проверка наличия предыдущих контактов, что позволяет обнаружить подмену отправителя.

Цифровые реестры. Доступ преступников к централизованным реестрам с возможностью изменения данных — отдельный риск. Его можно снижать регулярной проверкой: срок присутствия перевозчика в базе, внесённые правки и др.

Как и в случае с процедурами проверки благонадёжности, ИТ-системы и сопутствующие процессы должны предусматривать наличие сигналов тревоги, запрет на дальнейшие действия (hard stop) и чётких индикаторов при любых изменениях в оригинальной информации о перевозчике, даже на один символ. Ключевое значение имеет наличие регламента эскалации и понимание того, кто в компании уполномочен принимать решения на уровне бизнеса при необходимости отклонения от стандартной процедуры.



Red flags

Не существует универсального решения для предотвращения стратегических и мошеннических хищений. Ниже приведены факторы риска на основе страховых случаев 2024 года. Эти индикаторы можно интегрировать в систему управления безопасностью как критерии настороженности:

- **Бесплатные почтовые сервисы**
- **Только мобильный телефон, без стационарного**
- **Отсутствие веб-сайта**
- **История коммерческих споров**
- **Длинные маршруты перевозок**
- **Разовые контракты**
- **Двойное брокерство без согласования**
- **Экономический спад в регионе**
- **Грузы повышенного риска**

Наши услуги

BSI Connect Screen

Интегрированная платформа, использующая основанный на оценке рисков подход к управлению рисками в цепочках поставок. Она помогает противостоять крупнейшим глобальным угрозам в цепочках поставок, выстраивать доверительные отношения с подрядчиками и повышать устойчивость на основе анализа данных. Платформа включает крупнейшую в мире частную базу данных по рискам в цепочках поставок, содержащую информацию более чем о 20 типах рисков в более чем 200 странах.

BSI Connect Screen предлагает сервисы и решения, которые ускоряют понимание рисков в цепочках поставок и предоставляют аналитическую информацию, необходимую для принятия обоснованных решений и повышения устойчивости цепочки поставок.

Услуги включают:

- Индивидуальные аналитические отчёты
- Интерактивные карты рисков
- Ежедневные обновления и уведомления
- Конструктор индивидуальных отчётов
- Базу данных инцидентов в цепочках поставок
- Систему аудита Connect Screen
- Консультационные услуги

BSI Connect Screen's Intelligence Analysts

Свяжитесь с нашими специалистами:

Jason Willoughby
Jason.Willoughby@bsigroup.com

Anna Lee Robbins
AnnaLee.Robbins@bsigroup.com

Stephanie Phillips
Stephanie.Phillips@bsigroup.com

Heather Mullen
Heather.Mullen@bsigroup.com

Millena Kiros
Millena.Kiros@bsigroup.com

Emily Lewis
Emily.Lewis@bsigroup.com

ТТ Клуб — признанный независимый лидер рынка в сфере взаимного страхования и сопутствующих услуг по управлению рисками для международной транспортной и логистической отрасли. Основная цель ТТ Клуба — способствовать повышению безопасности и защищённости отрасли. Команда по управлению рисками ТТ Клуба активно готовит рекомендации и информационные материалы, поддерживающие достижение этой цели.

Задачи ТТ Клуба в области предотвращения убытков:

- Поддержка в снижении вероятности возникновения страховых случаев.
- Продвижение возможностей внедрения лучших практик.
- Содействие в улучшении оценки рисков, их минимизации и контроле.

Хищения грузов остаются в пятёрке крупнейших категорий убытков по результатам глобального анализа страховых случаев ТТ Клуба. Анализ инцидентов, расширение соглашений об обмене данными, партнёрские инициативы и широкое распространение результатов исследований способствуют более глубокому пониманию корневых причин рисков.

Настоящий отчёт отражает общую цель ТТ Клуба и BSI Consulting — просвещать представителей логистической отрасли о меняющихся рисках хищений грузов по всему миру и рассказывать об эффективных мерах предотвращения убытков.

HIGHLIGHTING RISK, REDUCING EXPOSURE. ADVISING INSUREDS, SERVING THE INDUSTRY.

Michael Yarwood
Managing Director, Loss Prevention
michael.yarwood@thomasmiller.com

Josh Finch
Logistics Risk Manager
joshua.finch@thomasmiller.com

Your partner
in progress