УДК 004.056 Вестник УрФО № 3(37) / 2020, с. 81–87

**Груздева Л. М.**

DOI: 10.14529/secur200309

# *ИССЛЕДОВАНИЕ ПРОБЛЕМ ЗАЩИТЫ ОБЪЕКТОВ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ ОТ УГРОЗ ХИЩЕНИЯ ИНФОРМАЦИИ*

*В статье отмечается, что чем быстрее происходит цифровизация транспортной отрасли, а, следовательно, возникновении новых уязвимостей и рисков, тем острее стоит вопрос о разработке новых и усовершенствовании уже используемых средств по обеспечению информационной безопасности транспортной инфраструктуры, защите информации ограниченного доступа. Автор приводит примеры инцидентов информационной безопасности на транспорте в России и мире с 2018 года. Статистический анализ позволил прийти к выводу, что основным мотивом злоумышленников при совершении информационных атак является хищение информации, в наибольшей степени персональные данных, в том числе из облачных хранилищ. Социальная инженерия и кибератаки с использованием вредоносного программного обеспечения, вероятнее всего, останутся самыми популярными и успешными методами проникновения в корпоративные информационные системы.*

***Ключевые слова:*** *транспортная инфраструктура, информационная безопасность, защита информации, инцидент информационной безопасности, информационная атака, утечка конфиденциальной информации.*

**Gruzdeva L.M.**

# *RESEARCH OF PROBLEMS OF PROTECTION OF TRANSPORT INFRASTRUCTURE OBJECTS FROM THREATS OF INFORMATION THEFT*

*The article notes that the faster the digitalization of the transport industry takes place, and, consequently, the emergence of new vulnerabilities and risks, the more acute is the question of developing new and improving the already used means to ensure information security of transport infrastructure, protect information of limited access. The author gives examples of infor-*

*mation security incidents in transport in Russia and worldwide since 2018. Statistical analysis made it possible to conclude that the main motive of cybercriminals in carrying out information attacks is information theft, mostly personal data, including from cloud storage. Social engineering and cyber-attacks using malicious software are likely to remain the most popular and successful methods of infiltrating corporate information systems.*

***Keywords:*** *transport infrastructure, information security, data protection, information security incident, information attack, leak of confidential information.*

Внедрение технологических инноваций позволяет транспортному комплексу соответствовать запросам цифровой экономики. Развитие электротранспорта и высокоскоростного железнодорожного движения [1, 2], использование автономного транспорта (AVRI) на основе роботизированных технологий призвано повысить экономические показатели, уменьшить экологический вред [3], а также улучшить качество жизни человека. Специалисты признают, что беспилотные технологии [4] могут принести человечеству огромную пользу, привести к значительному сокращению числа жертв автомобильных аварий, которые ежегодно забирают жизни 1,3 млн. человек, а также повысить доступность такого транспорта для людей с ограниченными возможностями.

Но стоит отметить, что с появлением новых технологий появляются и новые риски в области безопасности. В частности, компания Tesla имеет не только широкий модельный ряд автомобилей, но, и не менее обширный перечень аварий, приведших даже к гибели водителей, использовавших функцию автопилота. GPS-навигатор также неоднократно становился причиной дорожно-транспортных происшествий из-за помех в сигнале, получаемом от спутников по сети.

Транспортные информационные системы и сети, инфраструктура организаций построены по тем же принципам, что и в других отраслях. В связи с этим глобальные проблемы обеспечения информационной безопасности так же остро стоят перед компаниями транспортного комплекса [5, 6]. При этом транспортная инфраструктура, как правило, географически распределена, включает большое число объектов, что усложняет работу служб защиты информации.

Ежегодная доля информационных атак, совершаемых на объекты транспортной инфраструктуры, по данным компании Positive Technologies (PT) составляет 1%, но в III квартале 2019 г. было зафиксировано увеличение их числа до 3% [7]. В I квартале 2020 г. произошло увеличение доли атак, совершенных с использованием вредоносного программного обеспечения (ПО), способного обходить антивирусы, межсетевые экраны, IPS, почтовые и веб-шлюзы, в комбинации с методами социальной инженерией (рис. 1).

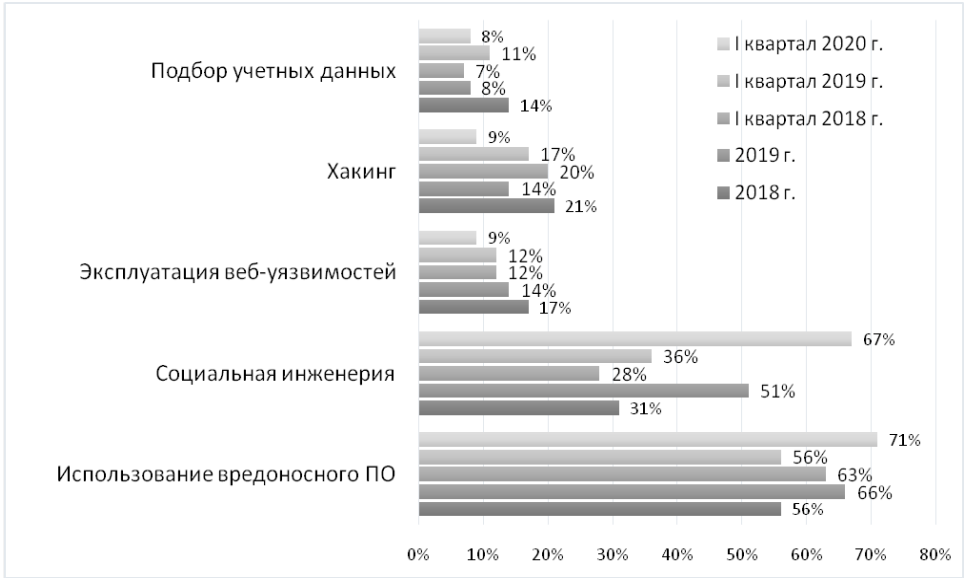


Рис. 1. Методы информационных атак (доля атак)

Так, например, на российские организации авиационно-космической отрасли была совершена APT-атака (advanced persistent threat - «развитая устойчивая угроза», целевая кибератака), в которой вредоносное ПО для удаленного управления (RAT) доставлялось путем рассылки писем с вредоносными документами в формате RTF [8].

Японский автопроизводитель Honda в июне 2020 г. заявил, что была совершена кибератака на сети промышленных систем управления, из-за которой возникли проблемы с доступом к внутренним серверам. Компания подтвердила, что работа на британском заводе была приостановлена наряду с приостановкой других операций в Северной Америке, Турции, Италии и Японии. Неизвестно, как злоумышленники проникли в компьютерную систему Honda, но исследования показывают, что все более распространенными становятся атаки с использованием информации о Covid-19, чтобы обманным путем заставить пользователей загружать на свои рабочие станции зараженные вредоносным ПО файлы.

В 2020 г. продолжился рост доли кибератак, совершаемых с целью хищения информации (рис. 2), при этом злоумышленников в 34% случаев интересовали персональные данные (ПДн), а в 19% - данные платежных карт.


Рис. 2. Мотивы злоумышленников

В 2018 г. злоумышленники похищали персональные данные в 30%, учетные данные в 24% и данные платежных карт в 14% случаев атак на информационные ресурсы. Например, из-за взлома системы бронирования British Airways в середине 2018 г., результатом которого стал доступ злоумышленников к тысячам номеров кредитных карт клиентов, британский информационный регулятор (Commissioner's Office, ICO) заявил, что намерен оштрафовать компанию на рекордные 183 млн. фунтов стерлингов (230 млн. долларов).

В середине марта 2018 г. программист Владимир Серов раскрыл самую крупную уязвимость в сервисе бесплатного Wi-Fi московского метро. Минимум год уязвимость позволяла злоумышленникам получать номера телефонов всех подключенных пассажиров поезда, а затем прочитать в незашифрованном виде цифровой портрет каждого.

По данным экспертно-аналитического центра компании InfoWatch, число утечек конфиденциальной информации в транспортных и логистических компаниях в 2019 г. выросло на 67%. Скомпрометировано около 59 млн. записей персональных данных клиентов и сотрудников, что почти в 6 раз больше, чем в 2018 г. [9]. При этом по статистике за 2019 г. в России существенно чаще, чем в мире «утекали» телефонные номера и паспортные данные (более чем в 30% утечек).

Европейская аэрокосмическая корпорация Airbus 30 января 2019 г. сообщила об обнаружении инцидента информационной безопасности, который привел к несанкционированному доступу к данным в информационных системах Airbus «Коммерческий авиационный бизнес». Нарушители получили доступ к личным данным, в основном, к профессиональным контактам и идентификационным данным некоторых сотрудников Airbus в Европе. Данный инцидент не повлиял на коммерческую деятельность корпорации.

Также в минувшем году крупную утечку персональных данных пассажиров пережила и китайская компания China Railway: из официальной системы бронирования могли быть похищены учетные записи до 5 млн. человек.

В России, как и в мире первое место по числу утечек ПДн занимает Интернет (браузер, cloud), на сеть приходится более 60% утечек. Бумажный документооборот в России продолжает функционировать наряду с электронным, поэтому злоумышленники в 22,7% случаев именно «бумагу» используют для хищения информации. Третье место в России занимают сервисы мгновенных сообщений (12,2%) [10].

С практической точки зрения для решения вопросов обеспечения информационной безопасности важно знать на сколько защищаемая информация подвержена деструктивному воздействию, т.е. «привлекательна» для злоумышленников. В России за 2018 г. было зафиксировано, что 60% утечек информации промышленных и транспортных компаний носило умышленный характер (рис. 3). В прошедшем году картина резко изменилась: было выявлено, что «привлекательность» для злоумышленников информации компаний данной отрасли являлась наименьшей, а доля умышленных утечек уменьшилась в 3 раза.

ции о путешествиях 9 млн. клиентов бюджетной британской авиакомпании EasyJet, но надо заметить, что при этом паспортные данные не были украдены. Интернет-издание Tom's Guide в июле 2020 г. сообщило об утечке персональных данных почти полумиллиона британских покупателей автомобилей BMW. Личные данные могут позволить злоумышленникам правдоподобно маскироваться под представителей автокомпании при реализации фишинговых атак на ее клиентов.

Из-за непрерывного роста спроса и предложений на рынке сервисов публичных облаков InfoWatch проявила интерес к проблеме обеспечения информационной безопасности от угроз хищения информации из баз данных. Согласно отчету Gartner, в 2019 г. объем данного рынка составил $227,8 млрд. (около 86 млрд. руб. приходится на Россию), а 2020 г. он может вырасти на +17%.

Эксперты зарегистрировали за 2019 г. в 3,5 раза больше, чем в 2018 г. случаев утечек конфиденциальной информации с хранилищ на незащищенных (свободно доступных из-за неверной конфигурации) серверах в облачных сервисах. При этом более половины всех выявленных случаев утечек конфиденциальной информации пришлось на две страны – США (27,5%) и Россию (26,7%). На первом ме-

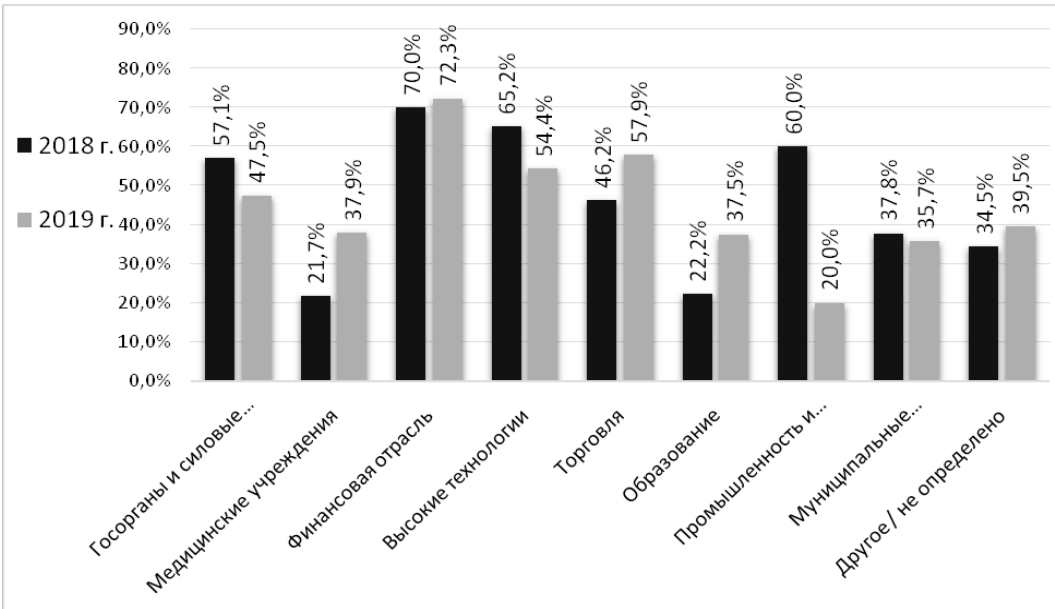


Рис. 3. Доля умышленных утечек ПДн и платежной информации по отраслям, Россия

В 2020 г. уже неоднократно фиксировались утечки ПДн из транспортных информационных систем. Например, в мае 2020 г. злоумышленники получили доступ к информа-

сте в мире и России по числу утечек находятся сервисы, на которых размещены данные высокотехнологичных компаний, например, телеком и электроника (рис. 4). При этом в

2019 г. в мире на +3,3% выросла доля утечек информации с промышленных и транспортных объектов, в России же зафиксировано число данных утечек на уровне 2018 г. - 7,2%.

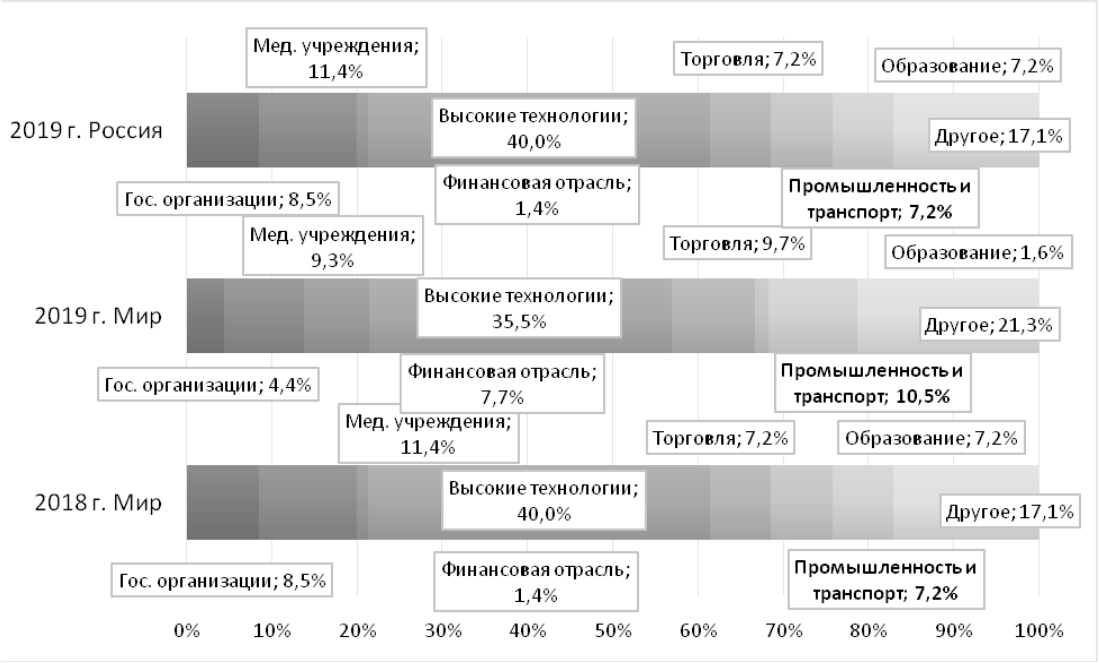


Рис. 4. Отраслевое распределение числа утечек из незащищенных хранилищ в облачных сервисах (Мир, 2018-2019 гг., Россия, 2019 г.)

В настоящее время на рынке облачных сервисов сохраняются многие проблемы в области информационной безопасности и защиты данных. Например, компьютерный справочный сайт Bleeping Computer сообщил, что на форумах распространяются базы (35 млн. записей персональных данных) участников программы лояльности и сведения из системы бронирования индонезийской авиакомпании Lion Air, при этом данные были скопированы с открытого облачного хранилища Amazon.

По мнению экспертов, International Data Corporation (IDC) к 2025 г. в облачных хранилищах будет обрабатываться почти половина всех мировых данных, в том числе и транспортной отрасли, в связи, с чем роль кибербезопасности будет только возрастать.

Около 10% утечек из транспортных и логистических компаний относятся к случаям компрометации информации категории «коммерческая тайна». Например, компания United Airlines была вынуждена принести извинения за утечку через Twitter внутренней информации, касающейся корпоративных расходов на авиабилеты среди крупнейших аккаунтов [9].

23 июля 2020 г. агентство Bloomberg сообщило об иске компании Tesla Inc. против Rivian Automotive Inc. в верховный суд штата Калифорнии, округ Санта-Клара (Сан-Хосе) о краже коммерческой тайны инсайдерами, которые перешли на работу к новому работодателю, что привело к внедрению интеллектуальной собственности Tesla в системы Rivian. Ранее Tesla уже подала в суд на бывших сотрудников за то, что они по сведениям компании передали ее коммерческие секреты китайскому производителю электромобилей Xpeng Motors и калифорнийскому разработчику беспилотного такси Zoox.

Издание The Register 10 апреля 2020 г. сообщило, что с помощью вируса-вымогателя DoppelPaymer для Windows был успешно атакован промышленный подрядчик Visser Precision. Конфиденциальные документы клиентов данной компании, в частности Tesla, Lockheed Martin, Boeing и SpaceX, были размещены злоумышленниками в открытом доступе в сети Интернет, так как Visser Precision не смогла выплатить выкуп за дешифратор зараженных файлов к сроку, установленному в марте.

Список инцидентов информационной безопасности на объектах транспортной инфраструктуры является далеко не полным, так как по мнению экспертов многие происшествия остаются не известны общественности. Компании стараются сохранить свою репутацию, стараются не подорвать доверие клиентов, поэтому не придают огласке случаи хищения инфор-

мации. Но каждая транспортная компания должна быть готова реагировать на информационные атаки и восстанавливаться путем создания киберустойчивости. Злоумышленники будут искать новые пути распространения вредоносного ПО и совершенствовать старые. Социальная инженерия, вероятно, останется основным путем распространения, однако в связи с ростом осведомленности о различных способах мошенничества преступники начнут разрабатывать более хитроумные схемы обмана пользователей. Стратегии защиты транспортных информационных систем должны быть сформулированы с учетом одного ключевого принципа: ни одна защита не является неприступной. Positive Technologies рекомендует заботиться не только об информационных ресурсах самих компаний, но и о безопасности их клиентов [7].

Анализ инцидентов информационной безопасности является одним из направлений оценки безопасности транспортных систем, которые в свою очередь являются объектами критической информационной инфраструктуры Российской Федерации [11]. Результаты проведенного исследования позволяют сделать вывод, что объекты транспортной инфраструктуры уязвимы и следует ожидать продолжение роста числа кибератак, совершаемых с целью хищения информации. В связи со сложностью и актуальностью задачи обеспечения информационной безопасности критической информационной инфраструктуры с 1 января 2018 г. на Федеральную службу безопасности Российской Федерации возложены функции по обеспечению функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ [12].

**Литература**


1. Розенберг Е. Н., Уманский В. И., Дзюба Ю. В. Цифровая экономика и цифровая железная дорога // Транспорт Российской Федерации. 2017. № 5 (72). – С. 45 – 49.

2. Уманский В. И., Павловский А. А, Дзюба Ю. В. Цифровая Железная Дорога. Технологический уровень // Перспективы Науки и Образования. 2018. № 1 (31). – С. 208 – 213.

3. Духно Н. А. Экологическая безопасность и транспорт // Транспортное право и безопасность. 2019. № 2(30). – С. 63 – 76.

4. Бойков В. Н., Скворцов А. В., Сарычев Д. С. Цифровая автомобильная дорога как отраслевой сегмент цифровой экономики // Транспорт Российской Федерации. 2018. № 2 (75) 2018. – С. 56 – 60.

5. Зворыкина Ю.В., Глущенко В.В. Обеспечение информационной безопасности на транспорте // Транспорт Российской Федерации. 2016. № 1 (62). – С. 6 – 9.

6. Груздева Л. М. Инциденты информационной безопасности на транспорте: виды, причины и негативные последствия // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. 2019. №6-2. – С. 57 – 60.

7. Актуальные киберугрозы. III квартал 2019 года [Электронный ресурс] ptsecurity.com. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q3/ (дата обращения 24.07.2020).

8. Актуальные киберугрозы. I квартал 2020 года [Электронный ресурс] ptsecurity.com. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/ (дата обращения 24.07.2020).

9. Транспорт: число утекших записей выросло в шесть раз [Электронный ресурс] infowatch.ru. – URL: https://www.infowatch.ru/analytics/digest/21801 (дата обращения 24.07.2020).

10. Исследование структуры утечек персональных данных: мир и Россия, 2019 год [Электронный ресурс] infowatch.ru. – URL: https://www.infowatch.ru/analytics/reports/26240 (дата обращения 24.07.2020).

11. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

12. Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».


**References**


1. Rozenberg E. N., Umanskij V. I., Dzjuba Ju. V. Cifrovaja jekonomika i cifrovaja zheleznaja doroga // Transport Rossijskoj Federacii. 2017. № 5 (72). – S. 45 – 49.

2. Umanskij V. I., Pavlovskij A. A, Dzjuba Ju. V. Cifrovaja Zhelez-naja Doroga. Tehnologicheskij uroven' // Perspektivy Nauki i Obrazovanija. 2018. № 1 (31). – S. 208 – 213.

3. Duhno N. A. Jekologicheskaja bezopasnost' i transport // Transportnoe pravo i bezopasnost'. 2019. № 2(30). – S. 63 – 76.

4. Bojkov V. N., Skvorcov A. V., Sarychev D. S. Cifrovaja avtomo-bil'naja doroga kak otraslevoj segment cifrovoj jekonomiki // Transport Rossijskoj Federacii. 2018. № 2 (75) 2018. – S. 56 – 60.

5. Zvorykina Ju.V., Glushhenko V.V. Obespechenie informacionnoj bezopasnosti na transporte // Transport Rossijskoj Federacii. 2016. № 1 (62). – S. 6 – 9.

6. Gruzdeva L. M. Incidenty informacionnoj bezopasnosti na transporte: vidy, prichiny i negativnye posledstvija // Sovremennaja nauka: aktual'nye problemy teorii i praktiki. Serija: Estestvennye i Tehnicheskie Nauki. 2019. №6-2. – S. 57 – 60.

7. Aktual'nye kiberugrozy. III kvartal 2019 goda [Jelektronnyj resurs] ptsecurity.com. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q3/ (data obrashhenija 24.07.2020).

8. Aktual'nye kiberugrozy. I kvartal 2020 goda [Jelektronnyj resurs] ptsecurity.com. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/ (data obrashhenija 24.07.2020).

9. Transport: chislo utekshih zapisej vyroslo v shest' raz [Jelektronnyj resurs] infowatch.ru. – URL: https://www.infowatch.ru/analytics/digest/21801 (data obrashhenija 24.07.2020).

10. Issledovanie struktury utechek personal'nyh dannyh: mir i Rossija, 2019 god [Jelektronnyj resurs] infowatch.ru. – URL: https://www.infowatch.ru/analytics/reports/26240 (data obrashhenija 24.07.2020).

11. Federal'nyj zakon ot 26.07.2017 № 187-FZ «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii».

12. Ukaz Prezidenta RF ot 22.12.2017 № 620 «O sovershenstvovanii gosdarstvennoj sistemy obnaruzhenija, preduprezhdenija i likvidacii posledstvij komp'juternyh atak na informacionnye resursy Rossijskoj Federacii».

---

**ГРУЗДЕВА Людмила Михайловна**, кандидат технических наук, доцент кафедры «Информационные технологии в юридической деятельности и документационное обеспечение управления», профессор Российской Академии Естествознания (РАЕ), Российский университет транспорта (МИИТ). 127994, г. Москва, ул. Образцова, д. 9, стр. 4. E-mail: docentglm@gmail.com

**GRUZDEVA Liudmila Mikhailovna,** Candidate of technical sciences, Associate professor of the department «Information Technologies in Legal Activity and Documentation Support of Management», Professor of the Russian Academy of natural Sciences (ANS), Russian University of Transport. 127994, Moscow, Obrastsova str., 9, bld. 9. E-mail: docentglm@gmail.com