§4 АДМИНИСТРАТИВНОЕ И МУНИЦИПАЛЬНОЕ ПРАВО И БЕЗОПАСНОСТЬ

В.В. Мотин

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Транспорт в настоящее время составляет огромную часть мировой экономики. По оценке экспертов Организации экономического сотрудничества и развития, к 2030 г. инвестиционные потребности мировой транспортной инфраструктуры, включающей аэро и морские порты, железные дороги, а также трубопроводы, составят 11,3 трлн. долларов. Предполагается, что более 44% этого объема должны составить инвестиции в железнодорожную инфраструктуру (порядка 5 трлн. долларов).

По длине железных дорог и грузообороту железнодорожного транспорта Россия занимает второе место в мире после США. Протяженность железнодорожных путей в России составляет около 85 тыс. км., а грузооборот — около 2 трлн. т-км. против 230 тыс. км. железнодорожных путей и 2,3 трлн. т-км. грузооборота в США.

Оборот российского рынка транспортных услуг в 2014 г., включая доходы от перевалки грузов в портах и аэропортах, превысит 72 млрд. долларов.

Поскольку транспорт играет огромную роль в экономической деятельности любого государства, то неотъемлемым требованием к транспортной инфраструктуре является способность противостоять любым видам преступных посягательств. Это особенно важно, в первую очередь, для России. Протяженность ее территории и важность обеспечения безопасности транспортных коммуникаций во все времена вызвали необходимость наличия соответствующих силовых структур и нормативно-правовой базы, которая обеспечивала бы транспортную безопасность. Еще в начале XIX в. кроме городской и сельской полиции в России существовали специализированные полицейские органы на транспорте, которые действовали независимо от местной администрации, городской и сельской полиции. Задачей транспортной полиции являлось обеспечение безопасности на транспорте, сопровождение и предотвращение хищений грузов.

С появлением и дальнейшим развитием железнодорожного транспорта задача борьбы с преступностью на нем была возложена на жандармские полицейские управления железных дорог, входивших в состав Отдельного корпуса жандармов.

После революции вопросы обеспечения транспортной безопасности продолжали оставаться одними из ведущих. Были созданы специальные подразделения в составе всероссийской чрезвычайной комиссии — транспортные ЧК. В дальнейшем подразделения по обеспечению безопасности на транспорте не раз меняли свою ведомственную принадлежность, тем не менее, выполняемая ими задача оставалась весьма важной для обеспечения государственных интересов. В годы Великой Отечественной войны и почти до середины 50-х гг. XX в. порядок на транспорте обеспечивали структурные подразделения органов государственной безопасности, наряду с другими силовыми структурами и собственными вооруженными формированиями Министерства путей сообщения. В дальнейшем функции обеспечения безопасности на всех видах транспорта были переданы Министерству Внутренних дел, в настоящее время, в составе которого функционирует Главное Управление на транспорте.

Законодательная база обеспечения безопасности на транспорте включает в себя как уголовно-правовые, так и административно-правовые меры. Уголовный кодекс России включена специальная гл. 27 «Преступления против безопасности движения и эксплуатации железнодорожного, воздушного, морского и внутреннего водного транспорта и метрополитена». В Кодексе об административных правонарушениях также имеется соответствующая гл. 11 «Административные правонарушения

на транспорте». Реализация указанных правовых норм позволяет обеспечить транспортную безопасность. В то же время бурное развитие транспортного комплекса России ставит новые проблемы, связанные с обеспечением транспортной безопасности. Это обусловлено тем, что одновременно с ростом внутренних перевозок на всех видах транспорта, перед нашей страной встают новые задачи глобального масштаба: вступление России в ВТО, возрастание роли России как транспортного коридора между Европой и развитыми странами Дальнего Востока, регулярное судоходство по северному морскому пути, связанное с глобальным изменением климата и т.д. Все эти факторы оказывают значительное влияние на обеспечение транспортной безопасности, многократно усложняя задачи по ее реализации. Это связано, в первую очередь, с развитием информационных технологий. Цифровая эра подарила нам не только преимущество перед прошлыми поколениями, но и принесла новые проблемы — угрозы, с которыми может столкнуться или уже столкнулось человечество. Одной из таких опасностей являются кибервойны, которые представляют собой атаки на системы, критически важные для национальной и глобальной экономик, а также для национальной и глобальной безопасности, с целью ослабления военного потенциала, нанесения существенного урона деятельности государств, государственных учреждений, жизни населения, возможно, и без человеческих жертв[1].

Характерным примером ведения кибервойны на настоящий момент остается атака на Иран. Вирус Flame атаковал компьютеры иранских чиновников и собирал различные данные — главным образом документацию и чертежи, в том числе офисные документы, файлы PDF, AutoCAD. Специалисты по информационной безопасности, работающие в ведущих компаниях Symantec и Лаборатории Касперского, заявили, что есть прямая связь между Flame и вредоносной программой Stuxnet, которая в 2010 году спровоцировала технические сбои в оборудовании, установленном на ядерных объектах Ирана. По утверждениям СМИ разработка этого вируса велась специалистами США и Израиля. Цель запуска вредоносного приложения заключалась в том, чтобы помешать Ирану создать ядерное оружие. В результате иранская ядерная программа была отброшена в развитии на срок от полутора до двух лет[2].

В современном мире количество примеров подобных атак на инфраструктурные объекты отдельных государств постоянно увеличивается. Также заметно выросла угроза безопасности интернет-банкингу и системам промышленного управления. Эти угрозы усиливаются вследствие того что координация развития киберугроз зачастую осуществляется на государственном уровне. Например, Symantec регулярно проводит виртуальный конкурс среди сотрудников на лучший взлом внутрикорпоративного сервера. Задача — взломать определенные системы, достать определенные файлы. После этого отбираются 20 лучших команд и играют очный турнир, который проходит в США. Это мероприятие проводится при участии представителей Министерства обороны и соответствующих правительственных организаций. Это дало основание специалистам по информационной безопасности Китая считать, что первое место среди внешних источников кибератак занимает США[3]. В свою очередь союзник США — Южная Корея считает, что опасность для нее представляет Северная Корея. Эксперты по безопасности Южной Кореи, Северная Корея давно готовится к ведению войны в киберпространстве, имея в своем распоряжении подразделение из 3 тыс. элитных хакеров, которыми управляет сам лидер страны Ким Чен Ын. Южнокорейский генерал Бэй Диг-Си заявил, что хакеры из Северной Кореи уже давно активно атакуют информационные системы южных соседей с целью кражи военных секретов и выведения из строя компьютерных сетей[4].

Таким образом, целенаправленные кибератаки на ряд государств в современном мире стали объективной реальностью. В случае наличия политических разногласий кибератаки все чаще становятся аргументом в споре. И если в случае открытых военных конфликтов сдерживающим фактором, обеспечивающим стабильность, является ядерное оружие, то в случае с атаками на информационные сети понятия «ядерного паритета» не существует. Тем не менее, в случае возможного воздействия на инфраструктурные объекты нашей страны со стороны враждебно настроенных государств или террористических организаций. В условиях России, с ее протяженностью, одним из наиболее уязвимых мест инфраструктуры

---

[1] См.: От PIN-кода к кибервойне. Бизнесмен Евгений Касперский – о необходимости создания КиберМАГАТЭ // http://www.izvestia.ru/news/526680

[2] См.: США и Израиль обвинили в разработке «супервируса» // http://www.rg.ru/2012/06/20/virus-site.html

[3] См.: Китайский Интернет все больше подвергается внешним сетевым атакам // http://russian.people.com.cn/31521/7763896.html

[4] См.: Кибервойска Северной Кореи – 3 тысячи элитных хакеров // http://www.cnews.ru/top/2012/06/09/kibervoyska_severnoy_korei__3_tysyachi_elitnyh_hakerov_492597

является транспорт. Уровень опасностей резко возрастает в связи с развитием и внедрением информационных систем.

Так, ОАО «РЖД» уже сейчас занимается разработкой единой комплексной системы управления движением высокоскоростных (400 км/ч) поездов[5]. Достигнутый уровень информатизации на транспорте без должной защиты уже несет в себе потенциальные угрозы. Несложно себе представить результаты атаки на информационную сеть ОАО «РЖД». Результатом будет транспортный коллапс в масштабах всего государства.

Даже малейший сбой в системе реализации билетов на поезда в период сезона отпусков может вызвать большие проблемы в функционировании транспортной системы. Будет парализовано движение пассажирских поездов как ближнего, так и дальнего следования, что может отразиться на доставке товаров, корреспонденции, а также энергоносителей в ряд крайне зависимых от них регионов. Сложная, разветвленная, масштабная информационная сеть, которой обладают Российские железные дороги, должна быть надежно защищена на всех уровнях, поскольку от ее работы зависят миллионы людей, пользующихся услугами железной дороги, и даже малейшие сбои недопустимы. Потенциальную цель для кибератак представляет создание в Российских городах интеллектуальных систем управления транспортными и пешеходными потоками. В частности в Москве подобная система будет управлять не только светофорами, но и камерами, датчиками движения и различными информационными табло[6]. Подобные системы внедряются во многих российских городах, среди них Казань, Рязань, Санкт-Петербург и ряде других[7]. Интеллектуальные транспортные системы также могут явиться потенциальной мишенью для кибератак.

Вопросы безопасности киберпространства стали новым вызовом для национальной и международной безопасности. С появлением Интернета, национальная безопасность охватывает не только традиционные земельные площади, водное и воздушное пространство, но и «информационные границы». Транспортная безопасность, должна обеспечиваться и в информационных сетях объектов транспортной инфраструктуры, ввиду того, что даже замкнутая система, не имеющая доступа во внешнюю сеть, может стать объектом атаки. Это наглядно подтвердил факт проникновения компьютерного червя Stuxnet в сеть иранского ядерного объекта, несмотря на отсутствие физического подключения к глобальной сети[8]8. Стало ли его проникновение результатом халатности или целенаправленных злонамеренных действий отдельных сотрудников не так важно. Важно достижение атакующей стороной своей цели.

В настоящее время обеспечению безопасности объектов транспортной инфраструктуры от новых угроз связанных, прежде всего, с уязвимостью информационных систем не уделяется должного внимания. В частности в приказе Министерства транспорта «О порядке проведения оценки уязвимости объектов транспортной инфраструктуры и транспортных средств»[9] потенциальная уязвимость информационных систем не рассматривается в качестве объекта оценки. Однако ущерб от кибератаки может на несколько порядков превосходить ущерб от традиционного способа нападения. Все это делает данный аспект обеспечения безопасности на транспорте крайне актуальным как в организационном, так и законодательных аспектах. В состав гл. 28 уголовного кодекса России «Преступления в сфере компьютерной информации», включена ст. 273 «Создание, использование и распространение вредоносных компьютерных программ». В соответствии с указанной статей создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами — наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. Те же деяния, повлекшие по

---

[5] См.: Стратегические направления исследований и разработок на среднесрочную перспективу (2012-2015 гг.) // http://www.rzd-expo.ru/innovation/technology_platform_quot_high_intellectual_rail_transport_quot/Tehnologicheskaya_platforma_2012_2015.pdf

[6] В Москве исчезнут посты ДПС // http://www.buhgalteria.ru/news/n57561

[7] Московский международный конгресс по интеллектуальным транспортным системам // http://www.pibd.ru/2012its22/

[8] От PIN-кода к кибервойне. Бизнесмен Евгений Касперский – о необходимости создания КиберМАГАТЭ // http://www.izvestia.ru/news/526680

[9] См.: Приказ Министерства транспорта РФ (Минтранс России) от 12 апреля 2010 г. № 87 г. Москва «О порядке проведения оценки уязвимости объектов транспортной инфраструктуры и транспортных средств» // http://www.rg.ru/2010/06/02/ocenka-dok.html

неосторожности тяжкие последствия, — наказываются лишением свободы на срок от трех до семи лет. Под вредоносными программами в контексте данной статьи понимаются программы, специально созданные для нарушения нормального функционирования компьютерных программ. Проблема обеспечения транспортной безопасности в условиях современных информационных угроз носит многоаспектный характер. С технической точки зрения, прежде всего, необходимо создание и использование специальных программных комплексов направленных на обнаружение и нейтрализацию вредоносного программного кода. Примером может служить внедрение внедрении системы защиты (Kaspersky Total Space Security) для обеспечения антивирусной защиты корпоративной информационной сети Российских железных дорог[10]. Современное законодательство направлено, прежде всего, против умышленного создания и использования и распространения вредоносных программ. Оно достаточно эффективно против, прежде всего, отечественных создателей и распространителей вредоносных программ, хотя как мы уже отмечали выше, созданием таких программ все чаще занимаются правительства и спецслужбы различных государств. Естественно, что российское законодательство не в полной мере может противостоять таким внешним киберугрозам. Угрозы возникают также в связи с использованием так называемых «пиратских программ». С точки зрения потребителя применение таких программ экономически более выгодно, чем приобретение лицензионных, поскольку разница в цене может составлять несколько порядков, а с развитием интернета эта разница зачастую составляет всю стоимость программного обеспечения. Однако использование пиратских программ не может гарантировать того что они не заражены соответствующими вирусами, которые внешне могут себя не проявлять, а нанести ущерб спустя определенное время. По оценкам специалистов около четверти компьютеров, подключенных к Интернету во всем мире, может быть заражено и использоваться злоумышленниками в своих интересах[11]. Сами пользователи в большинстве случаев, об этом не догадываются. Усугубляет ситуацию то, что часто потребители не применяют специальные антивирусные программы.

С целью повышения уровня транспортной безопасности от новых видов угроз, связанных с развитием информационных технологий полагаю, что необходимо законодательно установить административную ответственность за неиспользование соответствующих антивирусных комплексов. С этой целью требуется внести соответствующие изменения в гл. 13 («Административные правонарушения в области связи и информации») кодекса об административных правонарушениях. Это позволит снизить угрозы для транспортной безопасности России.

Библиографический список:

1. От PIN-кода к кибервойне. Бизнесмен Евгений Касперский — о необходимости создания КиберМАГАТЭ. // http://www.izvestia.ru/news/526680
2. США и Израиль обвинили в разработке «супервируса» // http://www.rg.ru/2012/06/20/virus-site.html
3. Китайский интернет все больше подвергается внешним сетевым атакам // http://russian.people.com.cn/31521/7763896.html
4. Кибервойска Северной Кореи — 3 тысячи элитных хакеров // http://www.cnews.ru/top/2012/06/09/kibervoyska_severnoy_korei__3_tysyachi_elitnyh_hakerov_492597
5. Стратегические направления исследований и разработок на среднесрочную перспективу (2012-2015 гг.) // http://www.rzd-expo.ru/innovation/technology_platform_quot_high_intellectual_rail_transport_quot/Tehnologicheskaya_platforma_2012_2015.pdf
6. В Москве исчезнут посты ДПС // http://www.buhgalteria.ru/news/n57561
7. Московский международный конгресс по интеллектуальным транспортным системам // http://www.pibd.ru/2012its22/
8. От PIN-кода к кибервойне. Бизнесмен Евгений Касперский — о необходимости создания КиберМАГАТЭ. // http://www.izvestia.ru/news/526680
9. Приказ Министерства транспорта РФ (Минтранс России) от 12 апреля 2010 г. № 87 г. Москва «О порядке проведения оценки уязвимости объектов транспортной инфраструктуры и транспортных средств» // http://

[10] См.: Лаборатория Касперского» защищает Российские железные дороги от киберугроз // http://globalmsk.ru/firmnews/id/2835

[11] См.: Ботнет Великий и Ужасный // http://www.computerra.ru/focus/317787/

www.rg.ru/2010/06/02/ocenka-dok.html«Лаборатория Касперского» защищает Российские железные дороги от киберугроз // http://globalmsk.ru/firmnews/id/2835
10. Ботнет Великий и Ужасный // http://www.computerra.ru/focus/317787/

References (transliteration):

1. Ot PIN-koda k kibervoyne. Biznesmen Evgeniy Kasperskiy — o neobkhodimosti sozdaniya KiberMAGATE. // http://www.izvestia.ru/news/526680
2. SShA i Izrail' obvinili v razrabotke «supervirusa» // http://www.rg.ru/2012/06/20/virus-site.html
3. Kitayskiy internet vse bol'she podvergaetsya vneshnim setevym atakam // http://russian.people.com.cn/31521/7763896.html
4. Kibervoyska Severnoy Korei — 3 tysyachi elitnykh khakerov // http://www.cnews.ru/top/2012/06/09/kibervoyska_severnoy_korei__3_tysyachi_elitnyh_hakerov_492597
5. Strategicheskie napravleniya issledovaniy i razrabotok na srednesrochnuyu perspektivu (2012-2015 gg.) // http://www.rzd-expo.ru/innovation/technology_platform_quot_high_intellectual_rail_transport_quot/Tehnologicheskaya_platforma_2012_2015.pdf
6. V Moskve ischeznut posty DPS // http://www.buhgalteria.ru/news/n57561
7. Moskovskiy mezhdunarodnyy kongress po intellektual'nym transportnym sistemam // http://www.pibd.ru/2012its22/
8. Ot PIN-koda k kibervoyne. Biznesmen Evgeniy Kasperskiy — o neobkhodimosti sozdaniya KiberMAGATE. // http://www.izvestia.ru/news/526680
9. Prikaz Ministerstva transporta Rossiyskoy Federatsii (Mintrans Rossii) ot 12 aprelya 2010 g. N 87 g. Moskva «O poryadke provedeniya otsenki uyazvimosti ob'ektov transportnoy infrastruktury i transportnykh sredstv» // http://www.rg.ru/2010/06/02/ocenka-dok.html 10. «Laboratoriya Kasperskogo» zashchishchaet Rossiyskie zheleznye dorogi ot kiberugroz // http://globalmsk.ru/firmnews/id/2835
10. Botnet Velikiy i Uzhasnyy // http://www.computerra.ru/focus/317787