Обеспечение информационной безопасности на транспорте

Ю. В. Зворыкина,
д-р экон. наук, советник Постпредства России при Евросоюзе (ЕС)

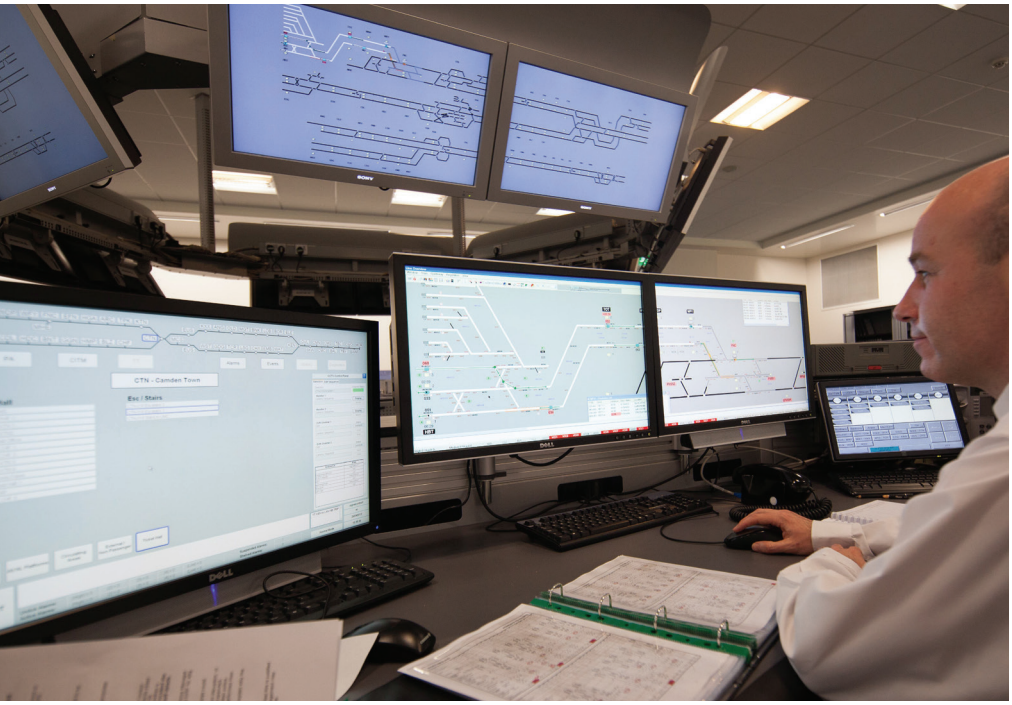
В. В. Глущенко,
советник Постпредства России при ЕС

При широком внедрении цифровых технологий в транспортной отрасли проблема информационной защиты вошла в число приоритетов обеспечения безопасности на транспорте. Защита информационных транспортных систем – серьезная задача для любого развитого государства.

Подходы к укреплению информационной безопасности

В январе 2013 г. Президент России Владимир Путин поручил ФСБ разработать систему по прогнозу и предотвращению кибератак, а в конце июля 2013 г. утвердил «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». В документе, ориентированном на устранение внешних угроз, к сожалению, не заложены основы взаимодействия всех участников цифрового сообщества внутри России.

Указанный документ стал ответом на принятую в 2011 г. США «Международную стратегию по действиям в киберпространстве». В ней компьютерные атаки приравнены к форме военных действий, что дает право применять в ответ любое оружие, вплоть до ядерного, прописаны цели и задачи, очерчены направления и механизмы реализации внешней политики.



Проблема информационной безопасности носит трансграничный характер, но это не исключает разработки свода правил, применяемых внутри страны. Более того, изучение зарубежного опыта может оказаться весьма полезным для формирования национальных подходов в этой сфере.

Национальные стратегии безопасности в киберпространстве появились сравнительно недавно: в США в 2003 г., во Франции в 2011 г. Единая стратегия для Евросоюза (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace) была опубликована только 7 февраля 2013 г.

В 2014 г. произошло смещение акцентов в стратегиях нового поколения. Если раньше государство ориентировалось на защиту граждан и организаций, то теперь – на общество и институты в целом. Это связано с увеличением значения Интернета в экономике и госуправлении, а также с потенциальными угрозами от других государств. Иными словами, уровень проблем кибербезопасности за пару десятков лет поднялся от частного до межгосударственного. Поэтому поощряется как межведомственное взаимодействие и государственно-частное партнерство внутри стран, так и межгосударственное сотрудничество.

Особое внимание мировое сообщество уделяет применению информационных технологий для обеспечения безопасности на транспорте. Например, в ноябре 2015 г. на Всемирной конференции по радиосвязи в Женеве (Швейцария) было достигнуто согласие о распределении радиочастотного спектра для глобального слежения за рейсами гражданской авиации. Это решение было принято после исчезновения в марте 2014 г. самолета Boeing 777, рейс MH 370 Малазийских авиалиний, с 239 людьми на борту.

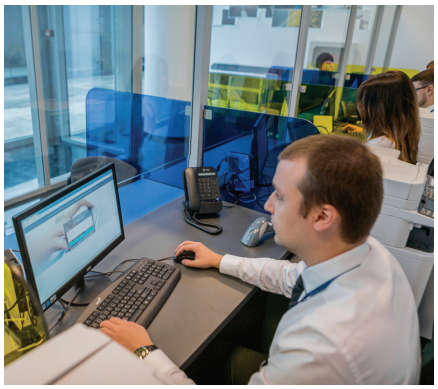
Информационно-коммуникационные технологии и кибербезопасность в Евросоюзе

Роль информационно-коммуникационных технологий (ИКТ) можно сравнить с функцией нервной системы: передача импульсов и сигналов, необходимых для корректной работы не только экономики, но и всего общественного организма. Тезис о том, что внедрение информационных технологий на транспорте формирует внутриполитическую повестку дня, недавно получил подтверждение: водители большегрузных автомобилей выступили против цифровой системы сбора платы за проезд по федеральным трассам «Платон». Отметим, что во многих странах действуют аналогичные системы сбора платы с автомобилей за пользование автодорогами. Например, в Евросоюзе все больше стран (с 1 января 2016 г. к ним присоединились Бельгия и Германия) взимают подобным образом плату за использование дорог. Устройства, аналогичные «Платону», используются на территории нескольких стран, что позволяет снизить административные расходы. Один из аналогов – сервисы и решения, предлагаемые компанией «Multi Service Tolls» (Нидерланды) в 18 европейских странах. Гарантийный депозит составляет 135 евро, средний расход на оплату дорог за проезд для одного грузовика – около 15 тыс. евро.

Остановимся подробнее на совершенствовании систем информационной безопасности. В Евросоюзе уделяется самое пристальное внимание развитию собственного потенциала обеспечения надежной защиты критически важных объектов инфраструктуры ЕС и его государств-членов от киберугроз. Особую обеспокоенность Евросоюза вызывает стремительный рост количества преступлений в киберпространстве и степень их тяжести.

Придавая большое значение укреплению кибербезопасности, Еврокомиссия и другие институты ЕС наращивают усилия в этом направлении как внутри Евросоюза, так и на международной арене. Постоянно совершенствуется нормативно-правовая база ЕС в области кибербезопасности. Ключевой концептуальный документ, определяющий приоритетные направления, цели и основные задачи деятельности органов ЕС и государств-членов, – Стратегия кибербезопасности ЕС. Согласно Стратегии, основные усилия ЕС сосредоточены на решении пяти приоритетных задач:

ФОТО С САЙТА WWW.PLATON.RU



Система «Платон»

1) повышении устойчивости информационно-коммуникационных систем и критически важных объектов инфраструктуры к кибератакам;

2) кардинальном снижении уровня киберпреступности;

3) развитии политики ЕС в области кибероборонны;

4) создании производственной и научно-исследовательской базы обеспечения кибербезопасности;

5) участии в формировании международной политики информационной безопасности и продвижении интересов ЕС в этой области на мировой арене.

В настоящее время предприняты конкретные шаги по реализации Стратегии. В ЕС создан экспертный форум по сетевой и информационной безопасности (Network and Information Security Platform) и сформированы три профильные рабочие группы:

1) по кризисному управлению в сфере кибербезопасности;

2) по обмену информацией и технологиями между заинтересованными субъектами ЕС;

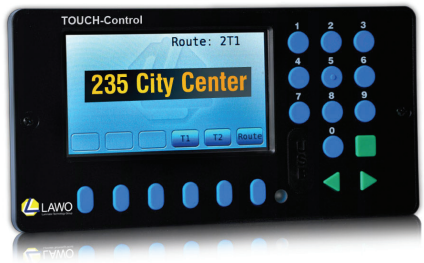
3) по координации подходов к проведению научно-исследовательских работ и опытно-конструкторских разработок, внедрению инноваций в сфере ИКТ и кибербезопасности.

Еврокомиссия при поддержке ведущих европейских университетов и профильных неправительственных организаций регулярно проводит конференции, семинары и заседания в формате «круглого стола» по актуальным проблемам кибербезопасности с широким привлечением общественности, экспертного сообщества и средств массовой информации. Предпринимаются шаги по развитию единых стандартов кибербезопасности, схем сертификации защиты информации в облачных базах данных.

Важнейшим элементом Стратегии станет директива о сетевой и информационной безопасности (Network and Information Security (NIS) Directive). 7 декабря 2015 г. Совет ЕС и Европарламент достигли политического соглашения по проекту директивы. С целью создания единой высокоэффективной системы защиты от угроз в киберпространстве положения документа будут юридически обязывающими не только для компетентных органов ЕС и государств-членов, но и для частных компаний, работающих в критически важных отраслях (энергетике, транспорте, водоснабжении, здравоохранении, в банковском и финансовом секторах), а также для ряда поставщиков цифровых услуг. К последней категории директива относит торговые площадки в сети Интернет, провайдеров облачных услуг и поисковые сервисы. Компетентным органам будут даны полномочия применять меры относительно недобросовестных компаний. Отметим, что на малые предприятия это требование не распространяется.

Главные задачи новых правил – повышение эффективности систем кибербезопасности стран-членов, усиление сотрудничества между ними. Компании должны быть готовы к принятию эффективных мер по обеспечению кибербезопасности. Об отмеченных инцидентах необходимо сообщать компетентным национальным органам.

В соответствии с директивой страны-члены должны принять национальные стратегии в области сетевой и информационной безопасности, определяющие цели и необходимые политические и регулятивные меры, установить компетентный орган, отвечающий за исполнение директивы, создать группы быстрого реагирования на компьютерные инциденты (CSIRT) для противо-



действия им, а также для предотвращения рисков.

Директива предусматривает создание межгосударственной группы по сотрудничеству для стратегического взаимодействия и обмена информацией. Оперативное сотрудничество по координированному реагированию на трансграничные инциденты и обмену информацией о рисках будет осуществляться с помощью создаваемой общей сети CSIRT.

Итоговый текст директивы будет в ближайшее время формально утвержден Европарламентом и Советом ЕС. В течение 21 месяца после вступления Директивы в силу страны-члены должны интегрировать ее положения в национальное законодательство, а еще через шесть месяцев – составить список компаний-операторов критически важных объектов инфраструктуры.

Немалые усилия предпринимаются ЕС и на международной арене. Запущены так называемые кибердиалоги со стратегическими партнерами: США, Японией, Южной Кореей, а также с Индией и Китаем. Наиболее интенсивный диалог ведется с Министерством внутренней безопасности и с Агентством национальной безопасности США. Признавая очевидное отставание от США в области развития ИКТ, Евросоюз проводит курс на усиление своих позиций. Так, Еврокомиссия предпринимает шаги по созданию в ЕС мощной научно-исследовательской и технологической базы для развития микро- и наноэлектроники, для создания новых материалов и передового программного обеспечения. В рамках запущенной 1 января 2014 г. программы исследований и инноваций ЕС «Горизонт 2020» ведутся разработки по двум направлениям:

1) информационно-коммуникационные комплексы, системы и сети с высокой степенью защиты от несанкционированного доступа;

2) технологии и средства криптографической защиты данных.

На финансирование этих исследований из фонда программы на 2014–2015 гг. было выделено 658,5 млн евро. При отборе проектов основное внимание уделялось предложениям по разработке передовых технологий, систем и средств, в полной мере соответствующих принятым в ЕС нормам безопасности и конфиденциальности и предоставляющих более высокий уровень защиты данных, чем аналогичные решения за пределами Евросоюза.

Далеко не все страны ЕС имеют технические возможности для эффективного противодействия киберпреступности. Поэтому в ЕС уделяется большое внимание оснащению национальных правоохранительных органов современным оборудованием и организации профессиональной переподготовки и повышению квалификации специалистов. Известно также о глобальных планах ЕС по увеличению объемов финансирования проектов и программ борьбы с киберпреступностью и киберугрозами.

После известных разоблачений Э. Сноудена Брюссель признал, что нет реальной возможности ограничить разведывательную деятельность Агентства национальной безопасности США на территории ЕС. Было принято решение сосредоточить основные усилия на организации «джентльменского» противодействия ближайшим «союзникам»: создать надежную инфраструктуру организационной и технической защиты информационных сетей органов ЕС и государств-членов от несанкционированного доступа.

Кроме того, проводится работа с коммерческими компаниями, прежде всего, по концентрации усилий государства и бизнеса в сфере защиты критически важных объектов инфраструктуры, в том числе интеллектуальных транспортных систем, от несанкционированного доступа.

Непосредственное отношение к транспорту имеет и такой вопрос обеспечения информационной безопасности, как защита персональных данных (ПД). Это предмет острых дискуссий на международных площадках. Политики разных стран пытаются найти компромисс между обеспечением защиты прав граждан на неприкосновенность частной жизни и необходимостью активизировать борьбу с террором и тяжкими преступлениями.

Защита персональных данных пассажиров

С 20 июля 2015 г. Евросоюз обсуждает проект директивы по использованию ПД пассажиров в целях предупреждения, выявления, расследования террористических актов и особо тяжких преступлений, а также уголовного преследования виновных (Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime), так называемой «полицейской директивы». Большая часть положений документа, относящихся к работе авиационного транспорта, уже согласована. Так, данные о пассажирах будут передаваться в период 48–24 ч до вылета. Создания Единого центра ЕС по сбору, обработке и хранению данных passenger name record (PNR) не предполагается. Каждая страна – член ЕС сформирует для этих целей собственное национальное подразделение (Passenger Information Unit, PIU).

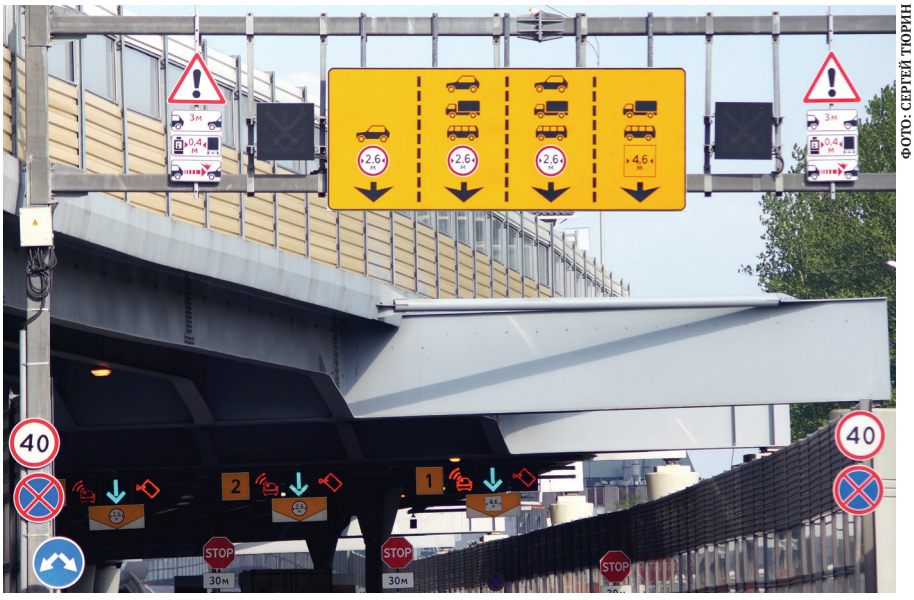


ФОТО: СЕРГЕЙ ТЮРИН

Как работает Global Distribution System, GDS

Террористическая атака на российский самолет А321 в Египте и октябрьские теракты в Париже заставили политиков ЕС ускорить работу по согласованию положений директивы. Представители стран – членов ЕС, не сомневаются в необходимости сбора PNR-информации для внутренних рейсов и согласны увеличить срок хранения данных до двух лет. Франция и Бельгия объявили, что они не намерены ждать, пока другие страны – члены ЕС «созреют» до стадии сбора и обмена данными, и введут в действие национальные системы немедленно, по мере готовности технической части.

Предполагается, что анализ данных PNR станет одним из ключевых элементов борьбы с терроризмом в ЕС. Представители Европарламента, Совета ЕС и Еврокомиссии рассчитывают, что директива будет утверждена в 2016 г. В настоящее время авиакомпании, зарегистрированные в ЕС, могут передавать данные только при наличии соответствующих двусторонних соглашений. Евросоюз заключил такие соглашения с США и Австралией. Аналогичный документ был подписан с Канадой, но на уровне Еврокомиссии, поэтому его легитимность была оспорена в Суде ЕС.

После того как Мексика ввела штрафы в размере 30 тыс. долл. США с каждого рейса за отказ авиакомпании предоставлять данные PNR, в июле 2015 г. ЕС начал переговоры о соглашении с Мексикой. Этот документ будет регулировать передачу данных PNR в Мексику и условия обработки данных мексиканскими властями. С 2012 г. мексиканское законодательство обязывает авиакомпании передавать данные PNR с целью выявления пассажиров, вовлеченных в оборот наркотиков, оружия и другую противозаконную деятельность. Международные пассажирские транспортные компании, осуществляющие воздушные, железнодорожные и морские перевозки, должны передавать таможенным органам данные пассажиров и членов экипажа до прибытия транспортного средства в место назначения.

Знаковым проектом в области внедрения информационных технологий на транспорте можно считать создание сервиса единого билета ЕС. В начале 2016 г. в большинстве крупных городов ЕС частично запущено обобщенное расписание муниципального транспорта, в середине года к сети подключат междугородные перевозки, а с января 2017 г. сервис единого билета охватит и международные перевозки на всех видах транспорта. Отметим, что система единого билета в Евросоюзе, несмотря на попытки Еврокомиссии ускорить бюрократические процедуры, реально начнет работать не раньше 2019–2020 гг. вследствие длительного согласования деталей проекта со всеми странами – членами ЕС.

Технологической платформой для создания так называемой глобальной системы резервирования (Global Distribution System, GDS) – основы концепции единого билета, станет испанская компания «AMADEUS», известная пользователям по авиатранспорту. Финансовые сервисы системы поручено реализовать компании «MasterCard Europe». Предполагается, что при использовании сервиса единого билета пассажир самостоятельно формирует и оплачивает через Интернет маршрут поездки «от двери до двери», включая муниципальный транспорт, с получением альтернативных предложений по времени в пути и цене. Создание сервиса единого билета – один из практических шагов, предпринимаемых руководством ЕС на международной арене.

Перспективы системы информационной безопасности на транспорте в России

Сегодня у России есть возможность опередить конкурентов и разработать свой сервис единого билета на все виды транспорта, заняв лидирующие позиции в европейском пространстве. Опираясь на требования законодательства о хранении персональных данных россиян с использованием баз данных, находящихся на территории России, предлагается создать российский GDS на основе информационных ресурсов системы «Сирена» ОАО «РЖД».

Инициатива создания российского единого билета может стать системообразующим проектом в области импортозамещения программного обеспечения и преодоления глобальной монополии США в сфере информационных технологий. Российская GDS станет ключевым звеном формирования международного сотрудничества, поскольку, несомненно, найдет понимание и поддержку в странах, стремящихся потеснить американцев в секторе информационных технологий.

Новая сфера обеспечения информационной безопасности на транспорте – использование автономных транспортных средств, прежде всего беспилотных летательных аппаратов. Согласно экспертным оценкам международные стандарты регулирования и технические платформы управления автономными транспортными средствами будут сформированы к 2020 г. Работа в этом направлении ведется отечественными учеными уже несколько лет. Российские наработки существенно опережают зарубежные аналоги, что позволит продвигать нашу продукцию на международные рынки.

Информационная безопасность давно играет ключевую роль в операционной деятельности крупных российских компаний, и борьбе с киберугрозами уделяется самое пристальное внимание. Проблема обеспечения информационной безопасности и цифрового суверенитета России остается актуальной, особенно в свете обострения отношений с Западом и антироссийскими санкциями. Таким образом, становится очевидным приоритет информационной безопасности критически важных объектов инфраструктуры, прежде всего, транспорта.