на частную жизнь). Американские ученые предлагают даже более масштабную трактовку: в определенном смысле все права человека – это формы приватности. Такие широкие формулировки, на наш взгляд, излишне не определенны и не могут в полной мере отражать содержание этого сложного понятия. В толковом словаре Е.Н. Шагаловой встречается такое определение понятия «прайвеси»: «частная жизнь человека, неприкосновенность которой культивируется и охраняется в цивилизованных странах» (см.: Шагалова Е.Н. Самый новейший толковый словарь русского языка XXI века : ок. 1 500 слов. М., 2011. С. 413).

Определенный научный интерес заслуживает точка зрения, высказанная С. Кови в книге «Быть, а не казаться», в которой автор выделил три стороны жизни человека: публичную, частную и тайную. При этом под тайной жизнью понимается жизнь души, где скрыты истинные побуждения, самые заветные желания, мотивации, публичная жизнь – то, что видят и слышат коллеги, помощники и другие люди, частная жизнь – общение с супругами, членами семьи, близкими друзьями. Тайная жизнь – это составляющая первых двух.

Между тем, если категория «частная жизнь» в юридической литературе изучена, то научных разработок на тему тайной жизни и публичной жизни не встречается. В.И. Даль под прилагательным «публичный» понимал «всенародный, оглашенный, явный, известный». Н.Ю. Шведова толкует термин «публичный» как «осуществляемый в присутствии публики, открытый», Т.Ф. Ефремова – как «предназначенный для публики, находящийся в ее распоряжении; общественный, не частный».

Отсюда следует, что категория «публичный» по своей сути является противоположной категориям «частный» и «личный», т. е. публичная жизнь является жизнью открытой. Категория «тайная жизнь», по нашему мнению, также может иметь место в юридической науке как составляющая частной жизни и подлежит правовой регламентации только при уголовно-правовых правоотношениях (умысел на совершение преступления). В остальных случаях, с нашей точки зрения, тайная жизнь – это своего рода одно из проявлений свободы человека.

Таким образом, можно сделать вывод, что законодательство Республики Беларусь не раскрывает содержание категорий «личная жизнь» и «частная жизнь», «личная тайна», «семейная тайна», «сведения личного характера». Отсутствие нормативного определения указанных категорий создает пробел в праве и может привести к произвольному его толкованию правоприменителем, неоправданному ограничению или же расширению его смысла. Уяснение содержания этих категорий должно стать предметом более глубокого научного исследования.

УДК 327:004.056

О.А. Кучинский

КИБЕРУГРОЗЫ В ЭНЕРГЕТИЧЕСКОМ СЕКТОРЕ КАК ГЕОПОЛИТИЧЕСКОЕ ПОСЛЕДСТВИЕ ЭНЕРГЕТИЧЕСКОГО ПЕРЕХОДА

По мнению авторов экспертно-аналитического доклада «Цифровой переход в электроэнергетике России» (Центр стратегических разработок, 2017), облик электроэнергетики ближайшего будущего определяют следующие технологические и рыночные тренды: удешевление новых технологий для использования возобновляемых источников энергии (ВИЭ); глубокая децентрализация производства электроэнергии; распространение технологий и практики энергосбережения; распространение цифровых сетей и интеллектуальных систем управления; изменение модели поведения потребителей и появление просьюмеров; распространение новых финансовых технологий. Указанные тренды целесообразно рассматривать в более широком контексте энергетического перехода – процесса долговременных структурных изменений мировой энергетики, связанных с постепенным замещением ископаемых видов топлива (нефти, природного газа и угля) ВИЭ. Данный переход не сводится исключительно к замене одних источников энергии другими. Его ключевыми элементами, по мнению Международного агентства по возобновляемой энергии IRENA, являются энергетическая эффективность, ВИЭ, а также повышение потребления электроэнергии. Согласно Уставу Международного агентства по возобновляемой энергии IRENA (вступил в силу для Республики Беларусь 28 февраля 2011 г.) к возобновляемой энергии относят биоэнергию, геотермальную энергию, гидроэлектроэнергию, энергию океана, солнечную энергию и энергию ветра.

Указанная трансформация имеет не только глубокие социально-экономические, но и существенные геополитические последствия. К числу основных геополитических аспектов большинство исследователей относят кибербезопасность.

Энергетический сектор традиционно относится к объектам критической инфраструктуры, от бесперебойной работы которого зависит устойчивое функционирование государства. Экономические последствия аварий в энергосистеме могут быть очень значительны. Например, в совместном исследовании компании Lloyds и Кембриджского университета (2015) отмечается, что гипотетическая авария в США, вызванная кибератакой и затрагивающая 50 электростанций и 15 штатов, может обойтись в сумму от 243 млрд до 1 трлн долл. США.

Применительно к энергетике наиболее часто объектом кибератак становятся системы промышленного управления (ICS) и диспетчерского контроля и сбора данных (SCADA). К. Василеу выделяет следующие виды атак на энергетическую инфраструктуру:

вредоносное программное обеспечение (ПО) (malware) – файлы или программы, предназначенные для нанесения вреда устройствам или сетям (вирусы, черви, троянские кони, шпионское ПО и программы-вымогатели (ransomware));

распределенные атаки типа «отказ в обслуживании» (distributed denial of service, DDoS) – атаки на системы генерации и передачи энергии, которые делают услуги или ресурсы недоступными в результате перегрузки их бóльшим количеством запросов, чем они могут обработать;

социальная инженерия, или фишинг (social engineering), – методы, основанные на психологических особенностях личности и закономерностях человеческого мышления, обычно применяемые для несанкционированного доступа к сетям для кражи данных или кибершпионажа (часто атаки имеют вид электронных писем, поступающих из авторитетных источников, которые манипулируют пользователями с целью раскрытия конфиденциальной информации);

развитая устойчивая угроза (advanced persistent threat, APT), целевая (таргетированная) кибератака – атака с целью хищения защищенной информации из информационной системы конкретной компании, организации или государственной структуры, которая отличается комплексным характером используемых методов, большой продолжительностью, длительным и ресурсозатратным процессом подготовки.

Наиболее известные случаи кибератак в энергетическом секторе связаны с использованием вредоносного ПО Stuxnet (2010 г.), Shamoon (DistTrack) (2012) и BlackEnergy (2015).

По мнению журналистов американской газеты «Нью-Йорк таймс», вирус Stuxnet является разработкой спецслужб Израиля и США, направленной против ядерной программы Ирана. Вирус нарушил работу почти 1 000 центрифуг для обогащения уранового топлива в Нетензе. Примечательно, что иранские ядерные объекты были изолированы от сети Интернет, а заражение предположительно произошло через инфицированный USB-диск.

Вирус Shamoon, также известный как DistTrack, был впервые использован в 2012 г. против нефтяных компаний Aramco (Саудовская Аравия) и RasGas (Катар). Вирус уничтожил данные на более 30 000 компьютерах Aramco, в результате чего компания потратила две недели на восстановление их работоспособности. Вирус не затронул компьютеры, обеспечивавшие процессы бурения скважин и нефтепереработки. Таким образом, последствия кибератаки оказались ограниченными административными подразделениями компании.

В результате действия вируса BlackEnergy, поразившего в 2015 г. Прикарпатьеоблэнерго (г. Ивано-Франковск, Украина), были отключены 30 подстанций, более 230 тыс. человек оказались без света на период от одного до шести часов. Вирусная атака стала возможной ввиду наличия уязвимости в используемых на предприятии системах SCADA. В дальнейшем атаки на украинские энергообъекты продолжились при помощи вредоносного ПО GreyEnergy.

Следует отметить, что указанные инциденты являются лишь незначительной частью киберугроз, которым подвергается энергетическая инфраструктура в настоящее время. Так, по данным газеты «Энергетика и промышленность России» (2019), Россети – одна из крупнейших российских электроэнергетических компаний – ежегодно блокирует порядка 9 млн попыток хакерского проникновения в корпоративный периметр. Ежегодно компания тратит около 2 млрд р. на защиту от кибератак – около 10 % от всех расходов на процессы цифровизации и автоматизации. Только за 2019 г. 18 % российских энергокомпаний приступили к разработке проектов по реализации мер защиты критической информационной инфраструктуры.

С учетом отмеченных процессов развития ВИЭ, цифровизации и децентрализации энергетики можно предположить, что по мере трансформации мировой энергетики в направлении низкоуглеродных технологий значимость проблемы безопасности критической энергетической инфраструктуры будет только возрастать. Неслучайно в докладе IRENA, посвященном геополитике энергетической трансформации (2019), отмечены геополитические риски ВИЭ, связанные с киберугрозами. Например, преступные группы, террористы или службы безопасности враждебных стран могут взламывать цифровые системы, контролирующие работу электростанций и электрических сетей, в преступных целях, в том числе для военного или промышленного шпионажа. В наиболее экстремальных случаях киберпреступники могут попытаться совершить диверсию, прервав работу или разрушив промышленную инфраструктуру, включая энергетические установки. В этой связи очень показательным является отказ властей Австралии, Бельгии и Германии от приобретения китайской компанией State Grid акций ряда энергетических и электросетевых компаний по соображениям национальной безопасности.

Очевидно, что по мере увеличения количества производителей энергии из ВИЭ, поставляющих энергию в централизованную сеть, количество «слабых звеньев» будет пропорционально увеличиваться, так как небольшие предприятия, как правило, не обладают достаточными ресурсами для инвестиций в информационную безопасность. В этой связи очень важным представляется повышение требований по безопасности к установкам по использованию ВИЭ и сетевому оборудованию на уровне промышленных стандартов.

Несмотря на высокий потенциал белорусской IT-сферы, в глобальном рейтинге кибербезопасности за 2018 г., подготовленном Международным союзом электросвязи, Беларусь заняла 69-е место из 175. Необходимость дальнейшего решения имеющихся в данной сфере проблем потребовала принятия Концепции информационной безопасности Республики Беларусь (утверждена постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1). Хотя удельный вес возобновляемой энергетики в Беларуси в настоящее время не очень высок (7,1 % в валовом потреблении энергоресурсов и 2,47 % в производстве электроэнергии по данным Национального статистического комитета за 2019 г.), проблемы кибербезопасности, в том числе в энергетической сфере, для нашей страны остаются нерешенными.

УДК 336.34

С.Г. Луговский

ФИНАНСИРОВАНИЕ ГОСУДАРСТВЕННЫХ РАСХОДОВ ПУТЕМ УПЛАТЫ НАЛОГОВ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Конституционная обязанность граждан – принимать участие в финансировании государственных расходов путем уплаты налогов, пошлин и иных платежей. В Республике Беларусь с каждым годом наблюдается рост транспортных средств. В настоящее время зарегистрировано более 3,6 млн автомобилей, находящихся в собственности у юридических и физических лиц. Рост числа транспортных средств приводит к ухудшению состояния дорожной сети, следовательно увеличиваются затраты на ее содержание. В связи с этим необходимо изыскание дополнительных источников доходов. В 2014 г. Законом Республики Беларусь «О внесении изменений и дополнений в некоторые законы Республики Беларусь по вопросам предпринимательской деятельности и налогообложения»

была закреплена государственная пошлина за выдачу разрешения на допуск транспортного средства к участию в дорожном движении. Исходя из этого в 2014 г. появилась обязанность собственников автотранспортных средств оплачивать ее при выдаче разрешения на допуск транспортного средства к участию в дорожном движении.

Правовой основой уплаты государственной пошлины за выдачу разрешения на допуск транспортного средства к участию в дорожном движении в Республике Беларусь являются Конституция Республики Беларусь (ст. 56), Налоговый кодекс Республики Беларусь (п. 1.69 ст. 284), законодательные акты о республиканском бюджете.

Необходимо отметить, что целью введения названной государственной пошлины в Республике Беларусь стала необходимость финансирования строительства новых и ремонта существующих дорог. В связи с этим предусмотрено 50 % суммы от госпошлины направлять в республиканский и 50 % – в местные бюджеты. В свою очередь, ранее большинство собранных средств выделялось на строительство второй минской кольцевой автомобильной дороги. В бюджет 2018 г. было запланировано собрать 322 млн 750 тыс. р. дорожного налога, в бюджет 2019 г. – почти на 3 млн меньше. Согласно Закону Республики Беларусь от 16 декабря 2019 г. № 269-З «О республиканском бюджете на 2020 год» дорожный фонд в 2020 г. должен составить 560,5 млн р. Приведенные аргументы свидетельствуют о том, что большинство автовладельцев не платят транспортный налог и не проходят гостехосмотр. К такой категории граждан можно отнести тех, кто имеет в собственности несколько автомобилей, старый автомобиль, использует автомобиль редко или только в сезон. В связи с этим становится очевидным, что бюджет с каждым годом все больше недополучает данный вид обязательного платежа, а это, в свою очередь, существенно сказывается на обеспечении экономической безопасности Республики Беларусь. Вместе с тем немаловажной причиной неуплаты дорожного налога можно считать отсутствие в законодательстве Республики Беларусь понижающих коэффициентов для ветеранов Великой Отечественной войны, инвалидов I и II групп, граждан пенсионного возраста, членов многодетных семей и др.

Уплата пошлины является обязательным условием выдачи разрешения на допуск транспортного средства к участию в дорожном движении. Так, госпошлина для физических лиц за легковой автомобиль не более 1,5 т составляет 3 базовые величины; 1,5–2 т – 6 базовых величин; 2–3 т – 8 базовых величин; более 3 т – 11 базовых величин. За автомобили, проходящие техосмотр раз в два года, пошлина уплачивается однократно в