

К вопросу о новых рисках в информационной сфере и реализации принципа «безопасность через развитие»

Макаров О. С.

Белорусский институт стратегических исследований, Республики Беларусь, г. Минск, Республика Беларусь; amakarovos@list.ru

РЕФЕРАТ

В статье на основе феноменологического анализа формирующихся общественных отношений в условиях «взрывной информатизации» рассматривается сущность и содержание информационной безопасности. Исходя из принципа «безопасность через развитие», приводятся результаты сравнительно-правового исследования законодательных новелл в сфере информационно-правовой трансформации Беларуси и России. Определяются стратегические направления дальнейшего правового регулирования, обеспечивающие упреждение новых рисков и вызовов.

Ключевые слова: безопасность, информационная безопасность, информационные риски, концепция информационной безопасности, правовое обеспечение информационной безопасности, взрывная информатизация

On the Issue of New Risks in the Information Sphere and Implementation of the Principle “Security through Development”

Oleg S. Makarov

Belarusian Institute for Strategic Studies of the Republic of Belarus, Minsk, Republic of Belarus; amakarovos@list.ru

ABSTRACT

The article considers the essence and content of information security based on a phenomenological analysis of emerging social relations in the context of “explosive informatization”. Based on the principle of “security through development”, the results of a comparative legal study of legislative innovations in the field of information and legal transformation of Belarus and Russia are presented. The strategic directions of further legal regulation are determined, ensuring the anticipation of new risks and challenges.

Keywords: security, information security, information risks, the concept of information security, legal support of information security, explosive informatization

Современное общество решительно осваивает информационное пространство, формируя новые объекты и формы отношений. Государства в стремлении не упустить интересы социума, а также занять доходные ниши торопят и подгоняют правовые системы, пытаясь «на марше» урегулировать формирующиеся общественные отношения. И это вызов для правового обеспечения информационных отношений, испытывающий реактивность и адаптивность правовых систем, прозорливость законодателя. В контексте информационной безопасности стремительное развитие названных правоотношений формирует возможность «отрыва» от традиционных и очевидных рисков и вызовов и одновременно столкновения с непознанными опасностями новых условий взаимодействия.

С позиций феноменологического подхода информационная безопасность представляется как явление, существующее за счет внутреннего противоречия: его сущностная составляющая «информационная...» тяготеет к развитию, так как может существовать только в динамических системах, а составляющая формы «...безопасность» требует статичности отношений и стремится к состоянию покоя: «...по своей

сути и содержанию задачи развития и обеспечения безопасности всегда имеют противоположную направленность. Развитие органически требует постоянного расширения, обновления, инноваций в тех или иных сферах деятельности общества. Безопасность же требует стабильности существующего положения, ограничения всякого рода новаций, особенно рискованных. Конечно, реальная взаимосвязь между развитием и безопасностью носит более сложный диалектический характер, поскольку эти две важнейшие функции жизнедеятельности общества тесно связаны между собой и раздельно осуществляться в принципе не могут, являясь как бы двумя сторонами одной медали» [6, с. 11]. Не вдаваясь в подробности известных теоретических подходов к пониманию информационной безопасности, отметим, что основные из них антагонистично разделены на «защитные» [9, с. 33–37] и «прогрессивные» [7, с. 115]. И. Л. Бачило полагает возможным синергию «защитного» и «прогрессивного» подходов, признает и поддерживает концепцию «безопасность через развитие» (особенно в области международной информационной безопасности) и полагает, что «...определение информационной безопасности через защищенность не противоречит формированию практики прогнозирования и стратегического планирования в области обеспечения национальной безопасности наряду с имеющимся подходом реагирования на опасности и угрозы...» [1, с. 367]. Для динамичной информационной сферы «прогрессивный» подход представляет значимый интерес, что позволяет рассмотреть его более подробно.

Специфика информационной безопасности заключается в том, что в информационной сфере формируются две категории интересов личности, общества и государства: «общечеловеческие» (закрепленные в конституции, реализуются посредством применения информационных технологий или в информационной среде) и «специальные», являющиеся средством достижения базовых («общечеловеческих») интересов (характерны только для информационной сферы, например, интерес к участию в информационном обмене, обеспечению безопасности информационной инфраструктуры). Особенность концептуальной архитектуры информационной безопасности (интересы — угрозы — меры) заключается в том, что основные угрозы не направлены непосредственно на «общечеловеческие» интересы, а воздействуют на способы их реализации (то есть «специальные» интересы). Таким образом, общей угрозой информационной безопасности может считаться недостижение «общечеловеческих» интересов или отставание в темпах приближения к ним. Следовательно, информационной безопасностью можно считать стабильную динамику развития информационных средств реализации базовых («общечеловеческих») интересов. Таким образом, в информационной сфере может быть внедрен принцип: «безопасность через развитие», при котором опережающие темпы роста являются гарантией безопасности, а задержка и отставание в развитии — угрозой безопасности. В таком случае функция подсистемы обеспечения безопасности смещается от противостояния совокупности угроз к их опережающему развитию (когда сфера интересов за счет динамики их развития не совпадает с точками реализации угроз). Данный принцип не следует путать с «иммунной» способностью базовой системы к выживанию в условиях реализации угроз.

Принцип «безопасность через развитие» в настоящее время претерпевает испытание на прочность в Республике Беларусь. Государство концептуально определило в числе основных угроз национальной безопасности «недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий» и «снижение или потерю конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента» [5]. По мнению заместителя директора Парка высоких технологий (ПВТ) [2] И. Жизневского, «чтобы государство было конкурентоспособным, его институты должны развиваться, используя самые современные технологии»¹. В целях реализации национальных интересов предприняты кардинальные меры обеспечения «ИТ-скачка», в первую очередь в области правового регулирования данной сферы. В частности, принят Декрет № 8 «О развитии цифровой экономики»² (далее — Декрет). Документ создает беспрецедентные условия для развития ИТ-отрасли и дает серьезные конкурентные преимущества стране в создании цифровой экономики³. Конкретные правовые гарантии, предоставленные Декретом, согласно оценке Д. Алейникова⁴, можно категорировать в следующем порядке:

упрощение документооборота (возможность заключать внешнеэкономические сделки путем обмена электронными и иными сообщениями посредством информационных систем; иностранные контрагенты резидента ПВТ могут не подписывать первичные учетные документы; законода-

¹ [Электронный ресурс]. URL: <http://www.pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2018/march/28171/> (дата обращения: 22.05.2018).

² Декрет Президента Республики Беларусь от 21.12.2017 № 8 / Национальный правовой интернет-портал Республики Беларусь. 27.12.2017. 1/17415.

³ [Электронный ресурс]. URL: <https://www.gb.by/izdaniya/glavnyi-bukhgalter/kommentarii-k-dekretu-8-ot-21-dekabrya-2> (дата обращения: 22.05.2018).

⁴ [Электронный ресурс]. URL: <http://bolshoi.by/persona/advokat-denis-aleynikov/> (дата обращения: 22.05.2018).

тельство Республики Беларусь о порядке проведения и контроля внешнеторговых операций не распространяется на внешнеторговые операции с участием резидентов ПБТ);

введение новых способов заключения договоров (посредством акцепта публичной оферты, размещенной в информационной сети; посредством обмена электронными сообщениями; посредством смарт-контракта);

имплементация отдельных институтов английского права (convertible loan — конвертируемый в доли [акции] заем (презюмирующий, что долг может быть конвертирован в доли [акции] и на договор не распространяются положения законодательства Республики Беларусь о преимущественном праве на приобретение долей [акций]); option agreements (put option, call option, including ESO) — опционные соглашения (Декрет предоставляет возможность сформировать опционный пул); indemnity — соглашение о возмещении имущественных потерь (предусматривается ответственность за ущерб, причиненный без нарушения договорных обязательств, что обеспечивает защиту интересов покупателя либо инвестора и упрощает процесс возмещения ущерба); warranties and representations — заверения об обстоятельствах (предусмотрены санкции за нарушение заверений, указанных в соглашении. Указанное положение остается в силе, даже если само соглашение признано недействительным); non-solicitation — соглашение о непереманивании, и non-competition — соглашение о неконкуренции (обеспечивают защиту интересов резидентов ПБТ путем ограничения прав ключевых сотрудников на трудоустройство в конкурирующие компании и создание конкурирующих компаний. Декрет позволяет предусмотреть санкции за нарушение этих соглашений); irrevocable power of attorney — безотзывная доверенность).

По мнению Д. Алейникова, «для привлечения иностранных венчурных инвестиций введены так называемые “институты английского права”: это позволит белорусским стартапам быть, что называется, on the same page с иностранными инвесторами и не уезжать на Кипр или в Делавэр. Такие юридические конструкции, как warranties and representations, indemnity и некоторые другие, защищают инвестора от возможных неблагоприятных последствий. А конвертируемый в доли (акции) заем — это классика венчурной индустрии США. Расширены виды деятельности: теперь в ПБТ можно заниматься еще и киберспортом, разработками в сфере медицинских и биотехнологий, аутсорсингом бизнес-процессов и любым бизнесом с использованием блокчейна»¹. Уже само принятие Декрета обусловило рекордный рост желающих вступить в Парк высоких технологий. Так, всего лишь за первый квартал 2018 г. число компаний-резидентов Парка увеличилось на четверть. Сфера их технологической компетенции — это в первую очередь искусственный интеллект, машинное обучение, интернет вещей, технологии дополненной реальности².

Несмотря на революционный характер белорусских правовых новелл, данная практика не является беспрецедентной. Метод «взрывной информатизации» выбрал в своем развитии целый ряд государств. Представляет интерес сравнительно-правовой анализ белорусского и российского подходов.

Министерство финансов Российской Федерации разработало схожий с Декретом Президента Республики Беларусь № 8 «О развитии цифровой экономики» проект закона «О цифровых финансовых активах». По мнению А. В. Шкирятова, по сравнению с российским аналогом «Декрет № 8 более либерален по отношению к физическим лицам, желающим заниматься майнингом, приобрести и разместить токены». В то же время, в отличие от Декрета, законопроект РФ «О цифровых финансовых активах» квалифицирует майнинг как предпринимательскую деятельность. В соответствии с Декретом токены подлежат обмену только на белорусские рубли, иностранную валюту, электронные деньги, токены / криптовалюту, в то время как, согласно законопроекту РФ, токены можно обменять в том числе и на иное имущество, но только через оператора цифровых финансовых активов, однако цифровые финансовые активы не являются законными средствами платежа на территории Российской Федерации, следовательно, ими нельзя выплачивать заработную плату, платить налоги, рассчитываться по кредитам, но, исходя из смысла законопроекта, цифровой актив можно обменивать на любые товары³.

По оценкам правового комитета Российской ассоциации криптовалюты и блокчейна (РАКИБ), сравнительный анализ Декрета и проекта Закона РФ «О цифровых финансовых активах» (далее — проект Закона) также показывает, что для деятельности физических лиц по майнингу цифровых ак-

¹ [Электронный ресурс]. URL: <https://forklog.com/vpered-i-planety-vsej-chto-predlagaet-belarus-kriptovalyutnomu-soobshhestvu/> (дата обращения: 22.05.2018).

² [Электронный ресурс]. URL: <http://www.park.by/post-1856/>. (дата обращения: 22.05.2018).

³ [Электронный ресурс]. URL: <https://www.kv.by/post/1053533-sravnitelnyy-pravovoy-analiz-dekreto-no-8-o-razvitiy-cifrovoy-ekonomiki-i-zakonoproekta> (дата обращения: 22.05.2018).

тивов в Беларуси созданы более либеральные условия, чем предполагается в России. Однако в проекте Закона более детально проработана процедура ICO и упрощен доступ к деятельности криптоплатформ, определено, что деятельность в криптовалютном пространстве будет доступна для всех субъектов хозяйствования. Проект Закона содержит ряд ограничений для исключения возможности использования цифровых активов в качестве инструмента для обслуживания нелегального бизнеса, а также легализации доходов, полученных преступным путем, и финансирования терроризма, а именно: установление порогового значения суммы сделок с токенами для неквалифицированных инвесторов, необходимость авторизации и прозрачности цифровых кошельков. В Беларуси операции с цифровыми активами будут опосредованы участием резидента ПВТ. Предполагается, что именно они станут своеобразным фильтром чистоты сделок¹.

IT-скачок, в соответствии с названной выше концепцией, позволяет избежать (а точнее, упредить) целый ряд рисков национальной безопасности в информационной и других сферах, таких как:

- отставание в темпах перехода экономики к передовым технологическим укладам от других государств;
- невысокий удельный вес высокотехнологичной наукоемкой продукции;
- неблагоприятные условия для привлечения иностранных инвестиций и кредитов;
- зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации;
- недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий.

В то же время отсутствие поступательности развития информационной сферы не позволяет спрогнозировать, а значит, и гарантировать безопасность национальных интересов уже для новых общественных отношений в новых социально-технологических условиях [3, с. 80]. Риски в данном случае в первую очередь порождаются применением передовых технологий и «опережающим» регулированием еще не сложившихся общественных отношений. В качестве наиболее прогнозируемых исследователи выделяют следующие риски.

1. Декрет вводит ряд элементов английского права. Однако белорусское право — это континентальная система, основанная на кодификации законов, а английское право основано на обычае и силе судебного прецедента. Пока непонятно, как нововведенные нормы будут исполняться на уровне белорусской судебной системы, поскольку судебной практики по применению таких норм просто не существует. Остается неясным, каким образом принятие Декрета скажется на привлечении инвестиций — захотят ли иностранные компании вкладывать средства в развитие своего присутствия в Беларуси или же будут пользоваться Декретом только для создания посреднических схем и финансовых транзакций. Есть опасность, что европейские, американские и иные регуляторы сочтут, что льготный налоговый режим ПВТ способствует созданию схем уклонения от уплаты налогов международными корпорациями. В сложившейся ситуации придется учитывать нормы иностранного законодательства, законодательства о противодействии террористической деятельности и отмыванию доходов, полученных незаконным путем, а также меры, принимаемые странами ОЭСР в рамках программы BEPS, направленной на борьбу с уклонением от налогов. Гарантия исполнения смарт-контрактов — это не только юридический, но и технический вызов, основанный на усложнении алгоритмов контрактов. Во многих отраслях смарт-контракты пока внедрить невозможно. Некоторые вопросы сейчас не вписываются в алгоритмы смарт-контрактов². **А. Воробей** указывает, что стороны, подписавшие смарт-контракт, понимают все его условия. Понятно, что обычное частное лицо или представитель субъекта хозяйствования едва ли умеют читать программный код. И в итоге легко могут стать жертвами мошенничества³.
2. В долгосрочной перспективе успехи IT-индустрии могут оказать влияние на социальное расслоение в обществе. По мнению экспертов Московского Центра Карнеги, Декрет может спровоцировать создание не только параллельной экономической реальности, но и новой социально-политической среды⁴.
3. По мнению Национального банка Республики Беларусь, операции с токенами по своей сути являются высокорисковыми и носят, как правило, спекулятивный характер. Риски связаны с отсутствием четкого и понятного механизма формирования их цены, надлежащих гарантий по защите

¹ [Электронный ресурс]. URL: <https://ilex.by/news/dekret-o-razvitiy-tsifrovoy-ekonomiki-vs-proekt-rossijskogo-zakona/> (дата обращения: 22.05.2018).

² [Электронный ресурс]. URL: <https://neg.by/novosti/otkrytiy/pravovye-vozmozhnosti-i-riski-dekreta-No-8> (дата обращения: 22.05.2018).

³ [Электронный ресурс]. URL: <https://neg.by/novosti/otkrytiy/dekret-No-8-chto-takoe-smart-kontrakt-i-zachem-ego-boyatsya> (дата обращения: 22.05.2018).

⁴ [Электронный ресурс]. URL: <http://nmbn.by/news/analytics/6545.html> (дата обращения: 22.05.2018).

прав и законных интересов держателей токенов, в частности, по погашению обязательств перед ними (в том числе при покупке токенов на зарубежных торговых площадках). Банкам следует повышать финансовую грамотность своих клиентов в данном вопросе, разъяснять им, что владельцы токенов берут на себя все возможные риски, совершая соответствующие операции¹.

4. Распространение на токены режима вещных прав является спорным с точки зрения классической доктрины гражданского права и теории вещных прав. Непонятно, в каком объеме нормы о вещных правах, в том числе о средствах защиты вещных прав, будут применяться к такого рода объектам. Вопросы, связанные с возможными коллизиями правового режима, применимого к праву, лежащему в основе токена и правового режима самого токена, будут возникать как в частном праве, так и в публичном. Многие из этих вопросов нельзя сейчас смоделировать или предвидеть, поэтому ответы придется искать уже в процессе реализации Декрета. Это неизбежная плата за попытку выработать регулирование отношений, которые находятся в стадии формирования и зависят от множества непредсказуемых факторов [8].
5. Деятельность оператора криптоплатформы в значительной степени построена на началах саморегулирования. В соответствии с Декретом, он сам разрабатывает и утверждает правила ICO: правила, регулирующие порядок торговли токенами; порядок допуска участников к торгам и исключения из числа участников торгов; правила допуска токенов к торгам (п. 4.3 Декрета). Вместе с тем успешная реализация такой высокой степени свободы в части регламентации процедуры ICO предполагает наличие неких стандартов, «лучших практик», которые служили бы ориентиром для операторов криптоплатформ².
6. Еще одной проблемой, которую необходимо будет решать белорусским регуляторам, станет идентификация участников операций с токенами (криптовалютами). Учитывая виртуальный характер соответствующих отношений, традиционные подходы к идентификации, основанные на личном присутствии и проверке документов, удостоверяющих личность, эффективно работать не будут. Будут нужны новые, надежные средства идентификации личности участников операций с токенами, возможно, с привлечением иных доверенных лиц, которые будут осуществлять такую идентификацию «как услугу»³.

Очевидно, что вышеназванные риски необходимо относить к разряду потенциальных. Трансформация их в реальные и деструктивное насыщение до уровня угроз национальной безопасности должно стать предметом мониторинга системы обеспечения безопасности. В соответствии с принципом «безопасность через развитие» в Республике Беларусь предпринимаются очередные шаги в информационной сфере. Так, Постановлением Совета Министров Республики Беларусь от 28 февраля 2018 г. № 167 создан Совет по развитию цифровой экономики, который будет координировать деятельность по реализации государственной политики в сфере цифровой трансформации экономики и развития информационно-коммуникационных технологий. В 2018 г. Президент Беларуси поддержал идею о создании Министерства цифровой экономики и поручил правительству внести соответствующее конкретное предложение по данному вопросу⁴. Для обеспечения национальной безопасности в информационной сфере в условиях активного развития информационных технологий, построения цифровой экономики и с учетом сопровождающих названные процессы рисков в соответствии с Указом Президента Республики Беларусь от 16.11.2017 № 413 «О Межведомственной комиссии по безопасности в информационной сфере» при Совете Безопасности Республики Беларусь создана Межведомственная комиссия по безопасности в информационной сфере, которая является постоянно действующим коллегиальным органом, осуществляющим координацию деятельности государственных органов и иных организаций по обеспечению национальной безопасности Республики Беларусь в информационной сфере⁵.

В Российской Федерации в целях формирования эффективной структуры федеральных органов исполнительной власти, в соответствии со ст. 112 Конституции Российской Федерации и Федеральным конституционным законом от 17.12.1997 № 2-ФКЗ «О Правительстве Российской Федерации», Министерство связи и массовых коммуникаций Российской Федерации переименовано в Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [4]. По словам

¹ [Электронный ресурс]. URL: <http://www.pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2018/february/27662/> (дата обращения: 22.05.2018).

² Там же.

³ Там же.

⁴ [Электронный ресурс]. URL: <http://www.belta.by/economics/view/ministerstvo-tsifrovoj-ekonomiki-mozhet-byt-sozdano-v-belarusi-uzhe-v-2018-godu-295871-2018/> (дата обращения: 22.05.2018).

⁵ [Электронный ресурс]. URL: http://kodeksy-by.com/norm_akt/source-%D0%9F%D1%80%D0%B5%D0%B7%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%20%D0%A0%D0%91/type-%D0%A3%D0%BA%D0%B0%D0%B7/413-16.11.2017.htm (дата обращения: 22.05.2018).

Д. Медведева, основной задачей обновленного министерства станет реализация «той самой цифровой повестки дня, которой занимается весь мир и которая является абсолютно актуальной и в нашей стране»¹.

Выводы. Изложенное позволяет сделать вывод, что современное состояние «IT-отрасли», да и информационной сферы в целом в интересах обеспечения национальной безопасности требует сосредоточения усилий на трех направлениях:

- учет потенциальных рисков при проектировании курса, темпов, конкретных шагов, правовых решений и технологических платформ информатизации;
- мониторинг состояния динамики угрожающих факторов в процессе реализации реформ и проектов;
- незамедлительное выстраивание адаптивной системы информационной безопасности в новых социально-технологических условиях.

Литература

1. Актуальные проблемы информационного права: учебник / коллектив авторов; под ред. И. Л. Бачило, М. А. Лапиной. М. : ЮСТИЦИЯ. 2016.
2. Декрет Президента Республики Беларусь от 22.09.2005 № 12 о создании Парка высоких технологий (ПВТ).
3. *Лопатин В. Н.* Риски информационной безопасности при переходе к цифровой экономике // Государство и право. 2018. № 3.
4. О структуре федеральных органов исполнительной власти. Указ Президента Российской Федерации от 15.05.2018.
5. Об утверждении Концепции национальной безопасности Республики Беларусь. Указ Президента Республики Беларусь от 09.11.2010 № 575.
6. Общая теория национальной безопасности: учебник / под общ. ред. А. А. Прохожева. Изд. 2. М. : Изд-во РАГС, 2005.
7. *Полякова Т. А.* Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. ... д-ра юрид. наук: 12.00.14. М., 2008.
8. *Савельев А. И.* Комментарий на положения о регулировании операций с криптовалютами и иных отношений, основанных на технологии «Блокчейн» Декрета Президента Республики Беларусь «О развитии цифровой экономики» № 8 от 21.12.2017 / ВШЭ НИУ. 2017. 22 с.
9. *Ліпкан В. А., Максименко Ю. Е., Желіховський В. М.* Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К. : КНТ, 2006.

Об авторе:

Макаров Олег Сергеевич, директор Белорусского института стратегических исследований (г. Минск, Республика Беларусь), доктор юридических наук, доцент; amakarovos@list.ru

About the author:

Oleg S. Makarov, Director of the Belarusian Institute for Strategic Studies (Minsk, Republic of Belarus), Doctor of Science (Jurisprudence), Associate Professor; amakarovos@list.ru

¹ [Электронный ресурс]. URL: <https://spbit.ru/news/n157334/> (дата обращения: 22.05.2018).