[16] О применении арбитражными судами статей 140 и 317 ГК РФ: Информационное письмо Президиума высшего Арбитражного Суда РФ от 4 ноября 2002 г. № 70 // Вестник ВАС РФ. – 2003. - № 1.

[17] Постановление Пленума Верховного Суда РФ и Пленума Высшего Арбитражного Суда РФ от 12 ноября и 15 ноября 2001 г. № 15/18 «О некоторых вопросах, связанных с применением норм Гражданского кодекса РФ об исковой давности» // Российская газета. – 2001. – 8 декабря. П. 25

PROBLEMS OF REAL EXECUTION OF OBLIGATIONS FOR PAYMENT OF INTEREST ON LOAN AGREEMENT

© 2019 Dashin Alexey Viktorovich
Doctor of Law, Professor Samara State University of Economics
E-mail: avdashin@mail.ru

A systematic analysis was carried out on the problem of the actual fulfillment of the obligation to pay interest on the loan agreement, which allowed to identify problematic aspects and outline the best ways to resolve them.

Keywords: loan agreement, interest rate, bank interest, refinancing, statute of limitations.

УДК 343.10.77.01

ЦИФРОВАЯ ЭКОНОМИКА, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И РОССИЙСКОЕ УГОЛОВНОЕ ПРАВО

© 2019 Денисова Анна Васильевна
Доктор юридических наук, доцент, главный научный сотрудник
отдела научного обеспечения прокурорского надзора и укрепления законности
в сфере уголовно-правового регулирования, исполнения уголовных наказаний
и иных мер уголовно-правового характера
Университет прокуратуры Российской Федерации, г. Москва
E-mail: anden2012@yandex.ru

Все отрасли права постоянно находятся под воздействием окружающей социальной среды, в особенности национальной политики и экономики, в связи с чем автором в работе поставлена цель исследования влияния процессов развития цифровой экономики Российской Федерации на отрасль российского уголовного права, на обеспечение информационной безопасности. На основании проведенного анализа выявляется перечень проблем, препятствующих в настоящее время развитию цифровой экономики России, которые могут быть разрешены с использованием уголовно-правовых средств. Исследуются вопросы пробельности российского уголовного законодательства относительно ряда общественно опасных деяний, совершаемых с использованием современных информационных технологий.

***Ключевые слова*:** цифровая экономика; экономическое уголовное право; киберпреступления; информационные экономические преступления; уголовно-правовое обеспечение информационной безопасности.

Уже давно доказано, что право, являясь социальной подсистемой, постоянно испытывает на себе направляющее воздействие окружающей социальной среды, в особенности национальных политической и экономической систем. Если вспомнить основные постулаты теории К. Маркса, то право как часть политической надстройки имеет своим базисом экономику, и поэтому не может не ощущать на себе первоочередного влияния экономических процессов, происходящих в обществе. Все те же самые правила актуальны и для российского уголовного права - следовательно, содержание российского уголовного права напрямую или опосредованно зависит от состояния национальной экономики, направлений внешней и внутренней политики государства, от уровня правосознания населения, количественных и качественных характеристик преступности, правоохранительной деятельности, уровня развития юридической науки, нравственности и религии и т.д. То есть изучение межсистемных связей между уголовным правом и вышеназванными социальными явлениями позволит в определенной степени управлять ими с учётом их зависимого поведения в социальной среде.

На наш взгляд, именно национальная политика является доминирующим, определяющим явлением в процессе уголовного правотворчества и правоприменения, опутывает отрасль права своими сильными и жесткими связями. Поэтому так важно на сегодняшний день учитывать ее приоритетные направления, связанные со все более активным внедрением информационных и коммуникационных технологий, развитием информационного общества в Российской Федерации и формированием национальной цифровой экономики[1].

Учитывая то обстоятельство, что уголовно-правовое регулирование является частью государственного управления, а отраслевые средства выступают инструментами управленческой деятельности государства, с помощью которых разрешаются сложные оперативно-тактические и стратегические задачи руководства обществом, не вызывает сомнений тот факт, что возможности отрасли уголовного права будут востребованы и при решении ряда злободневных проблем, препятствующих в настоящее время развитию цифровой экономики России. К таковым следует отнести проблемы обеспечения прав человека в цифровом мире, в том числе при идентификации (соотнесении человека с его цифровым образом), сохранности цифровых данных пользователя, а также проблемы обеспечения доверия граждан к цифровой среде; рост масштабов компьютерной преступности, в том числе международной; новые угрозы личности, бизнесу и государству, связанные с тенденциями к построению сложных иерархических информационно-телекоммуникационных систем, широко использующих виртуализацию, удаленные (облачные) хранилища данных, а также разнородные технологии связи и оконечные устройства; наращивание возможностей внешнего информационно-технического воздействия на информационную инфраструктуру, в том числе на критическую информационную инфраструктуру. Часть этих проблем с очевидностью относятся к юрисдикции российского уголовного права и подлежат разрешению с использованием арсенала соответствующих отраслевых средств.

Но право (и уголовное право в частности) никогда не бывает всего лишь инструментом в руках государства, оно по сути должно нести некий «высший план» общественного развития, предначертанный правопорядок, по отношению к которому государство и его управление, в свою очередь, выступают в инструментальной роли. Управляющее воздействие на отрасль уголовного права развивает ее систему, поддерживает и оптимизирует системные характеристики отрасли, производит упорядочивающий в отношении нее эффект. Так, модернизация отечественной экономической системы остро поставила вопрос о совершенствовании мер по обеспечению информационной безопасности во всех секторах экономики. По мнению опрошенных представителей российского бизнеса, количество преступлений в цифровой среде за 3 последних года возросло на 75 процентов, и оно будет только увеличиваться в связи с проводящейся цифровизацией экономики страны[2].

В Доктрине информационной безопасности Российской Федерации указывается, что в настоящее время на территории России возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий[3]. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее. Кроме того, наблюдается увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры Российской Федерации, нарастают угрозы применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации. Поэтому в качестве одной из стратегических целей обеспечения информационной безопасности Российской Федерации указано повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям. Однако конкретные средства реализации данной цели нигде не указаны, и как их будет разрабатывать и внедрять ответственное ведомство (в данном случае - Министерство внутренних дел РФ), и как это скажется на отрасли уголовного права в целом - остается загадкой.

В связи с этим в Национальной программе «Цифровая экономика Российской Федерации» 2019 года[4] акцентируются вопросы уголовно-правового обеспечения защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности в условиях цифровой экономики. В п.1.17 указывается на необходимость криминализации новых типов общественно опасных деяний, совершенных с использованием современных информационных технологий; в п. 4.1 - необходимость определения на законодательном уровне состава сведений, составляющих банковскую тайну, тайну связи, врачебную тайну, коммерческую тайну и иные виды тайн, и порядка их передачи третьим лицам, что крайне важно для реализации на практике ряда статей Уголовного кодекса РФ (ст. 137, 138, 183 и пр.) и их предупредительного потенциала.

Вышеуказанная обязанность по разработке проектов новых составов преступлений, совершаемых с использованием информационных технологий, возложена на

Министерство внутренних дел РФ и подлежит исполнению в срок до 30 июня 2020 года. Представляется, что для успешного выполнения данного поручения было бы целесообразно обратиться к опыту зарубежных стран, в законодательстве которых т.н. «информационные экономические преступления» появились еще несколько десятилетий назад (например, в США Computer Fraud and Abuse Act был принят в 1984 году, в Великобритании Computer Misuse Act - в 1990 году).

Отметим, что в большинстве зарубежных стран, имеющих серьезный опыт противодействия «информационным экономическим преступлениям», криминализированы следующие виды общественно опасных деяний: незаконный доступ к компьютерной системе; незаконные действия, связанные с входом в части компьютерной системы или в компьютерную систему целиком без разрешения или правомерного основания; хакерство; незаконное вмешательство в компьютерную систему; незаконные действия, создающие препятствия для работы компьютерной системы; атака типа "отказ в обслуживании", повреждение компьютерной системы; незаконное вмешательство в компьютерные данные (действия, связанные с повреждением, удалением, ухудшением, изменением или блокировкой компьютерных данных без разрешения или основания; удаление файлов компьютерных систем без разрешения); незаконный перехват компьютерных данных или доступ к ним (незаконные действия, связанные с получением доступа к компьютерным данным без разрешения или основания, включая получение данных во время процесса передачи, которая не рассчитана на то, чтобы быть публичной, а также получение компьютерных данных (такое, как копирование данных) без разрешения; запись передачи данных без права на это в беспроводной сети; копирование компьютерных файлов без разрешения и другие.

Так, согласно статье 202 Уголовного кодекса Германии незаконное получение лицом компьютерных данных, которые предназначались не для него, находящихся под специальной защитой от неправомочного доступа, с целью извлечения выгоды для себя или для третьего лица влечет лишение свободы сроком до трех лет. Наказанию в виде штрафа или заключения сроком до двух лет подлежат стирание, уничтожение, приведение в негодность, изменение компьютерных данных или попытки произвести такие действия.

Пункт "b" статьи 303 этого же кодекса предусматривает ответственность за т.н. «DNS-атаки» (компьютерный саботаж) и создание вредоносных программ. Под компьютерным саботажем понимается вмешательство в обработку данных, которое может причинить существенный вред предприятию, государственному органу или ведению бизнеса. Соответствующее деяние может быть осуществлено путем уничтожения, повреждения, приведения в негодность, изменения компьютерной системы, или вмешательства в передачу данных.

В Нидерландах криминализовано умышленное, с целью извлечения выгоды для себя или для третьего лица использование лицом технических устройств для перехвата или записи данных, из телекоммуникационных систем или присоединенного оборудования, если данные не предназначаются только для соответствующего лица (статья 139с УК). Отдельный состав предусмотрен и для пособников данному преступлению - подлежат уголовной ответственности лица, снабжающие средствами для незаконного перехвата и записи данных, идущих по телекоммуникационным или автоматизирован-

ным системам (статья 139d). А также для лиц, прикосновенных к вышеуказанным преступлениям - а именно обладающих данными, о которых он знает или должен знать, что они были получены в результате незаконного прослушивания, записи или перехвата данных автоматизированных систем или телекоммуникационных систем (статья 139e). Также к компьютерным преступлениям по голландскому законодательству относятся: несанкционированный доступ в компьютерные сети; несанкционированное копирование данных; компьютерный саботаж; распространение вирусов; компьютерный шпионаж. В ряд статей УК Голландии, предусматривающих ответственность за совершение «общеуголовных» преступлений (вымогательство, мошенничество, подлог и др.), были внесены дополнения и разъяснения, позволяющие использовать данные составы и для борьбы с компьютерными преступлениями.

Отметим, что в абсолютном большинстве случаев как в России, так и за рубежом «кибероружие» используется в сфере экономической деятельности хозяйствующих субъектов для извлечения материальной выгоды для злоумышленников или других лиц, либо для причинения имущественного вреда потерпевшим - добросовестным пользователям информационных и коммуникационных технологий. Учитывая также, что данные преступления опасны не только для граждан, общества, бизнеса и государства, но и подрывают инфраструктуру безопасности цифровой экономики России, представляется целесообразным признать их именно информационными экономическими преступлениями[5]. Данная группа преступлений, находясь на стыке институтов экономических и компьютерных преступлений, безусловно, имеет непосредственное отношение к зарождающейся в системе российского уголовного права «молодой» подотрасли «экономического/хозяйственного уголовного права», призванной защитить инвестиции, кредитные отношения, потребительский рынок и снизить экономические издержки, делая рынок более эффективным[6]. Представляется, что становление данной подотрасли в российском уголовном праве обусловлено помимо всего прочего и необходимостью обеспечения развития национальной цифровой экономики, создания благоприятных условий для честных участников рынка и минимизации криминальных рисков и угроз их информационной безопасности.

Подводя итоги, отметим, что качество связей российского уголовного права с национальной экономикой, особенностями ее развития на современном этапе и их учет в процессе реформирования законодательства - это важное условие обеспечения эффективности отрасли уголовного права, и в то же самое время необходимое условие для достижения состояния защищенности личности, бизнеса и государственных интересов при взаимодействиях в условиях цифровой экономики.

---

[1] Указ Президента РФ от 09 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

[2] Распоряжение Правительства РФ от 28 июля 2017 года № 1632-р «Об утверждении Программы "Цифровая экономика Российской Федерации"» (утратило силу)) // Собрание законодательства РФ. 2017. № 32. Ст. 5138.

[3] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

[4] Паспорт национального проекта Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7). Available at: https://digital.gov.ru/uploaded/files/natsionalnaya-programma-tsifrovaya-ekonomika-rossijskoj-federatsii_NcN2nOO.pdf (accessed 27 November 2019).

[5] Турышев, А.А. Информация как признак преступлений в сфере экономической деятельности: Автореф. дис. … к.ю.н. - Омск, 2006. 23 с.

[6] Есаков, Г.А. Экономическое уголовное право: понятие, содержание и перспективы/ Г.А. Есаков // Lex Russica. - 2013. - № 9. - С. 961-969; Клепицкий, И.А. Экономика и уголовное право/ И.А. Клепицкий // Закон. - 2013. - № 8. - С. 48-58.

THE DIGITAL ECONOMY, CYBER SECURITY AND RUSSIAN CRIMINAL LAW

© 2019 Denisova Anna Vasilevna
PhD, Associate Professor, the Chief Researcher of the Department
of Prosecutorial Supervision and Strengthening the Law in the Field of Criminal Law
Regulation, Execution of Criminal Sentences and Other Criminal Law Measures
University of prosecutor's office of the Russian Federation
E-mail: anden2012@yandex.ru

All branches of law are constantly under the influence of the social environment, especially national politics and economy, and therefore the author has set the goal of studying the impact of the development processes of the digital economy of the Russian Federation on the Russian criminal law as an important component of cyber security. The author describes the problems hindering the development of the Russian digital economy, which can be resolved using criminal law instruments. The study revealed the gaps in the Russian criminal law regarding the socially dangerous acts committed with the use of modern information technologies.

Keywords: the digital economy; cyber security; Russian criminal law; cybercrimes; informational economic crimes.

УДК 342

ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ В СТРАНАХ СНГ

© 2019 Ефремова Елена Александровна
Доцент
Самарский государственный экономический университет
E-mail: lenoksamara97@gmail.com

Мы живем в такое время, в котором процветают цифровые технологии. Наш век справедливо можно назвать «веком цифровых технологий». Не секрет, что технологии заметно упрощают нашу жизнь. С их появлением и развитием люди стали меньше времени тратить на бытовые и хозяйственные дела и больше времени уделять саморазвитию и личностному росту.