УДК 343.34:004:349.6

DOI dx.doi.org/10.24866/1813-3274/2018-3/108-116

Ю. В. Надточий¹

Дальневосточный федеральный университет, г. Владивосток, Россия

E-mail: crimlaw@rambler.ru

КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Аннотация. В представленной работе констатируется, что мировое сообщество вступило в эпоху высоких информационных технологий, которые активно используются сегодня во всех сферах человеческой деятельности (связь, транспорт, энергетика, водоснабжение, финансы, торговля, наука, образование, оборона, охрана общественного порядка, окружающей среды и т.д.). На сегодняшний день наша жизнедеятельность без них немыслима и даже ежеминутно от них зависима. При этом подчёркивается, что стремительное развитие и повсеместное внедрение телекоммуникационных и глобальных компьютерных сетей сформировало новый опасный вид преступления – «киберпреступность», которая имеет свои характерные особенности и влечёт серьёзные угрозы, причиняя существенный вред самым различным охраняемым законом объектам, а именно жизни и здоровью людей, собственности, состоянию окружающей среды и др. В ходе исследования выявлено, что киберпреступность несёт в себе непосредственную угрозу экологической безопасности как составной части национальной безопасности. В связи с этим отмечается, что назрела острая необходимость защиты общества и государства от нарастающей виртуальной опасности во имя сохранения экологического равновесия и выживания человечества. При этом, несмотря на масштаб и сложность проблемы эффективного противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, полагаем, что модернизация уголовного закона должна осуществляться крайне осторожно, по принципу минимизации вносимых поправок. Для борьбы с обозначенным явлением и обеспечения экологической безопасности необходимы системный подход, тщательная разработка законодательной базы и интенсивное международное сотрудничество государств.

¹ Юлия Викторовна Надточий, кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии Юридической школы Дальневосточного федерального университета, г. Владивосток, Россия.

Для цитирования: Надточий Ю. В. Киберпреступность как угроза экологической безопасности // Азиатско-Тихоокеанский регион: экономика, политика, право. 2018. № 3. С. 108–116.

Ключевые слова: информационные технологии, киберпреступление, окружающая среда, уголовная ответственность, экологическая безопасность.

Julia V. Nadtochiy¹

Far Eastern Federal University, Vladivostok, Russia

E-mail: crimlaw@rambler.ru

CYBERCRIME AS A THREAT TO ENVIRONMENTAL SECURITY

Abstract. The research states that the world community has entered the era of high information technologies, which are actively used today in all spheres of human activity (communication, transport, energy, water supply, finance, trade, science, education, defense, protection of public order, environment, etc.). Nowadays our life without them is unthinkable and even dependent on them. It is emphasized that the rapid development and widespread introduction of telecommunications and global computer networks has formed a new dangerous form of crime – "cybercrime", which has its own characteristics and entails serious threats, causing a significant damage to various legally protected objects, namely life and health of people, property, environment etc. The study has revealed that cybercrime carries a direct threat to environmental safety as component of national security. In this regard, it is noted that there is an urgent need to protect society and the state from the growing virtual danger in the name of preserving the ecological balance and survival of mankind. At the same time, despite the scale and complexity of the problem of effective counteraction to crimes committed with the use of information and telecommunication technologies, we believe that the modernization of the criminal law should be carried out very carefully, on the principle of minimizing the amendments. In order to combat this phenomenon and ensure environmental safety, a systematic approach, careful development of the legislative framework and intensive international cooperation of States are necessary.

Key words: information technology, cybercrime, environment, criminal liability, environmental security.

Информационные системы сегодня вошли во все сферы жизни, в том числе и в право. Развитие цифровых технологий открывает огромный спектр возможностей.

¹ Julia V. Nadtochiy, PhD, associate Professor, associate Professor, Department of criminal law and criminology of Law school, Far Eastern Federal University, Vladivostok, Russia.

For citation: Nadtochiy, J. V. Cybercrime as a threat to environmental security // Asia-Pacific: Economics, politics, law // Asia-Pacific RIM: Economic, Politics, Law. 2018. № 3. P. 108–116.

Прогресс во всех отраслях науки и промышленности идёт с огромной скоростью, не прекращая удивлять и восхищать. Исследователи утверждают, что внедрение технологических новинок с каждым годом будет проходить всё более быстрыми темпами. Интересно отметить, что на повсеместное распространение электричества в XX столетии ушло 30 лет, а планшетные компьютеры вошли в обиход за 3-4 года.

Можно смело утверждать, что это, по своей сути, уникальное явление (цифровые технологии, являющиеся, как известно, видом информационных технологий) за последнее десятилетие полностью изменило жизнь каждого жителя не только нашей страны, но и планеты. Всё больше людей во всём мире сегодня применяют цифровые технологии, ведь они предназначены для более простой и быстрой передачи данных. Именно быстроедействие и универсальность этой схемы сделали ИТ-технологии столь востребованными.

Интернет становится не только способом обмена информацией, цифровые технологии позволяют создавать своеобразную копию физического мира. Каждый объект, подключённый к глобальной сети, находится под полным контролем владельца. Скажем, с помощью «умной» розетки можно контролировать работу электроприборов, включать и выключать их на расстоянии, стиральная машина сигнализирует о возможной поломке механизма, а smart-обогреватель может самостоятельно контролировать температуру в помещении. То же происходит и с целыми городами. Стремление мирового сообщества к повышению качества жизни людей и внедрению экологически чистых инновационных технологий повлекло создание «умных» городов (smart city), основным принципом проектирования которых является внедрение информационных технологий, которые позволяют в режиме реального времени вычислять и корректировать траектории развития города с позиций наиболее экологического и рационального решения. В качестве примера такого экограда можно привести Масдар в Объединённых Арабских Эмиратах, строительство которого ведётся с 2006 г. Предполагается, что город будет полностью обеспечиваться за счёт солнечной энергии и других альтернативных источников с минимальными выбросами углекислого газа. В нём не будет автомобилей, а будет создана система беспилотного электрического транспорта – Personal rapid transit (PRT) [5]. В городе Сочи планируется внедрить цифровое управление автомобильным потоком, электронные проездные для пассажиров, информационные сервисы «Мой Сочи/проездной» и т.п. [3, с. 183]. Подобных проектов разработано достаточно много, ведь в связи с интенсивным экономическим ростом повышается степень загрязнения окружающей среды, а, как показывают многочисленные исследования, основными источниками загрязнения и негативного воздействия являются объекты промышленности, энергетики, транспорта, строительства, что и обуславливает необходимость использования более экологичных и рациональных технологий городского хозяйства, чтобы стабилизировать экологическую обстановку.

Однако применение цифровых технологий имеет как свои преимущества, так и, естественно, недостатки. Увеличение числа пользователей современных электронных средств связи («виртуализация» жизнедеятельности) открыло новые возможности не только для политики, экономики и культуры, но и для преступной деятельности. Появляются новые формы общественно опасного поведения, происходит изменение облика преступника и преступности в целом. Всё чаще мировое сообщество говорит о таком явлении, как «киберпреступность», под которой в общем понимают любое незаконное действие в электронной сфере, которое совершено с использованием компьютерных технологий либо против них. Согласно рекомендациям экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети [1, с. 156]. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершённое в электронной среде. Эти преступления имеют свои характерные особенности, придающие им повышенную опасность и делающие их весьма сложными для выявления и пресечения. Прежде всего это максимальная скрытность деяний, что достигается благодаря совершенным методам обеспечения анонимности любых совершаемых в интернете действий. В цифровой экономике личность «уходит» в виртуальную реальность. Остаются лишь логины, пароли, ники и коды. В результате, скажем, коррупционер может пользоваться материальными благами анонимно, не раскрывая своей личности, что придаёт ему больше решимости. Далее, трансграничность, т.е. преступник и потерпевший (или потерпевшие) могут быть разделены гигантскими расстояниями. Киберпреступность охватила уже все страны мира и переросла в масштаб международных угроз. Следующей особенностью является возможность совершения преступлений в автоматизированном режиме. Известны случаи, когда «хакеры» разрабатывали программы, которые самостоятельно (то есть без их участия) снимали деньги с кредитных карт, либо совершали другие противозаконные действия. Ещё один момент – это нестандартность действий преступников. В отличие от «обычных» преступлений в данной сфере практически невозможно предугадать действия злоумышленников. Таким образом, «невидимость» компьютерного преступника и одновременно «удлинение его рук» путём доступа к любой информации, к любым охраняемым секретам – военным, финансовым, иным – делают компьютерную технику весьма привлекательной для представителей преступного мира.

Всё сказанное свидетельствует о высокой степени общественной опасности таких преступлений, мы можем говорить о возникновении новых нарастающих форматов угроз для национальной безопасности. А что же такое «национальная безопасность»? Обратимся к официальной трактовке обозначенного понятия. Согласно Стратегии национальной безопасности РФ, принятой Указом Президента РФ

31 декабря 2015 г., национальная безопасность понимается как состояние защищённости личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан РФ, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации [7]. Как вытекает из обозначенного документа, частью национальной безопасности является безопасность экологическая. В частности, в Стратегии сказано, что национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией РФ и законодательством РФ, и в том числе экологическую. Это подчёркивается и в Указе Президента РФ «О Стратегии экологической безопасности РФ на период до 2025 года» [8]. Что касается понятия самой экологической безопасности, то оно даётся в ФЗ «Об охране окружающей среды», принятом 10 января 2002 г., где под ней понимается «состояние защищённости природной среды и жизненно важных интересов человека от возможного негативного воздействия хозяйственной и иной деятельности, чрезвычайных ситуаций природного и технического характера, их последствий» [6].

Соответственно киберпреступность несёт в себе прямую и непосредственную угрозу, и экологической безопасности в том числе. Стоит отметить, что, с учётом всех обозначенных нами особенностей киберпреступности, так называемые «хакеры» чувствуют себя безнаказанными и уже не останавливаются на простых банковских грабежах, достигающих, между прочим, общего ущерба в миллиарды долларов, они стали политически, экологически опасны, так как без гранат, бомб и автоматов могут остановить работу опасных химических производств, сформировать коллапс в обеспечении энерго- или водоснабжения, прекратить очистку сточных вод, скрываясь за фальшивыми виртуальными адресами.

Известно, в частности, о разрушении хакерами центрифуг производства обогащённого урана в Иране в 2010 г., где преступники использовали вредоносный код, получивший название Stuxnet, который был запущен в систему. К счастью, тогда не произошло большой экологической катастрофы. В России объектом атаки стала Саяно-Шушенская ГЭС, по некоторым данным аварию спровоцировал тот же вирус, что и на иранском заводе [2]. Это говорит о том, что нужно готовиться к новым потенциальным угрозам и источникам производственных аварий по аналогии с возможными пожарами, землетрясениями. Таким образом, реализация цифровой технологии в мировой экономике без решения вопросов защиты от нарастающей виртуальной опасности во имя сохранения экологического равновесия в биосфере от нового оружия массового вредительства становится не менее опасной, но более реальной угрозой, чем применение ядерного оружия. Обеспечение экологической безопасности при таком переводе общения на цифровую технологию требует многоплановых подготовительных соглашений международ-

ного уровня. Международные соглашения достигнуты Россией с Китаем, Индией, Египтом, Ираном, Вьетнамом.

Стоит отметить, что особую озабоченность у специалистов в рамках экологической безопасности вызывает ускоренное внедрение на дорогах мира транспортных систем с искусственным интеллектом, о чём говорилось выше. Последние разработки и практика их освоения показывают, что обеспечение экологической безопасности с учётом климатических, магнитных и других внешних факторов с помощью искусственного интеллекта можно довести до 90-95%, однако 100%-ная безопасность может быть обеспечена только разделением путей перемещения роботомашин и человека и формированием новой культуры общения человека с оцифрованными транспортными средствами. Примерами могут служить специальные переходы на традиционных тропах животных, которые защищают их от транспорта [2].

Государство должно реагировать на отклоняющееся поведение, и так как мы говорим о преступности, то здесь нас интересует не любое отклоняющееся поведение, а наиболее опасные его формы. Соответственно необходимо выявить эти наиболее общественно опасные формы, с которыми надо бороться уголовно-правовыми средствами. Здесь стоит констатировать, что несмотря на то, что накопившиеся проблемы сделали перемены не только насущно необходимыми, но и уже серьёзно запоздалыми, до настоящего времени, пожалуй, нет чёткого понимания относительно того, насколько современное уголовное право должно измениться, адаптируясь к условиям информационного общества. На уровне профессиональных субъектов уголовной политики нет не только стратегически выверенного последовательного плана модернизации уголовного законодательства, но и относительно внятного представления о специфике и масштабах проблемы.

Здесь нужно ответить на вопрос: как эффективно защитить человечество от нарастающих угроз в цифровой сфере, иными словами, от киберпреступников? Прежде всего необходимо решить ряд новых задач. Это, во-первых, построение эффективной системы защиты информации и информационно-коммуникационной инфраструктуры; во-вторых, приведение в соответствие сложившихся положений уголовного права с последствиями глобальной информатизации преступности, в частности решение вопросов: о пригодности классических положений института соучастия к случаям виртуального преступного взаимодействия, являющегося дистанционным и, как правило, анонимным; о том, каким должно быть оптимальное количество составов преступлений, посвящённых защите от киберпреступников и где они должны располагаться; есть ли необходимость и насколько обширно следует изменить диспозиции традиционных составов преступлений путём детализации их совершения специфическим способом – с использованием информационно-коммуникационных технологий; будет ли модернизация традиционных составов преступлений достаточной для противодействия современным криминальным угрозам.

Взглянув на действующий УК РФ, мы можем наблюдать, что сегодня помимо отдельной главы 28 «Преступления в сфере компьютерной информации», состоящей уже из четырёх статей и дополнительных составов мошенничества в сфере высоких технологий (ст. ст. 159³, 159⁶ УК РФ), в нём в последние годы наблюдается тенденция признания использования информационно-телекоммуникационных технологий в качестве квалифицирующих признаков преступлений, которое произошло точно в рамках практически всех разделов и глав уголовного закона. В частности, это коснулось и преступлений, посягающих на экологическую безопасность, в рамках ст. 258¹ (Незаконные добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесённым в Красную книгу РФ и (или) охраняемым международными договорами РФ). В 2017 г. ч. 2 обозначенной статьи была дополнена новым квалифицирующим признаком, сформулированным в п. «б», устанавливающим уголовную ответственность за совершение рассматриваемого деяния с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет») (ФЗ от 20.12.2017 г. № 412-ФЗ), а чуть позже, в 2018 г., рассматриваемая статья дополнена ч. 1.1 в которой криминализованы приобретение или продажа животных, являющихся предметом данного состава преступления, с использованием вышеуказанных электронных сетей (ФЗ от 27.06.2018 г. № 157-ФЗ). Других составов, посягающих на экологическую безопасность, подобные изменения не коснулись.

Можно заключить, что законодатель, безусловно, реагирует на новые цифровые угрозы, другое дело, как он это делает, насколько эффективно и оправданно. В целом представляется, что подобные изменения должны быть социально и криминологически обоснованными. Здесь не стоит бросаться в крайности, дабы не перенасытить уголовный закон ненужными составами, что лишь затруднит работу правоприменителя и приведёт к избыточности закона, а как следствие, низкой его эффективности. Стоит учитывать, что далеко не всякое применение информационных технологий (например, Интернета) влияет на степень общественной опасности деяния. Так, скажем, не имеет принципиального значения, состоялось ли разглашение сведений, составляющих коммерческую, налоговую или иную тайну, путём передачи документов либо посредством отправки письма по электронной почте. Мошенник, обманывающий потерпевших через Skype, вымогатель, отправляющий свои угрозы посредством сервиса WhatsApp, вряд ли совершает более тяжкое преступление по сравнению с классическими его формами. Таким образом, использование информационно-коммуникационных технологий имеет неравнозначный характер с точки зрения влияния на характер и степень общественной опасности преступления.

Включение квалифицирующего признака в состав преступления необходимо лишь в случаях, когда он объективно повышает вероятность наступления вредных последствий, что является важнейшим показателем опасности действия. Как справедливо

писал по этому поводу В.Н. Кудрявцев, «опасность действия заключается в том, что оно может вызвать определённые вредные последствия. Однако эти последствия наступают не во всех случаях. Естественно, что действия будут сравнительно тем опаснее, чем выше степень вероятности наступления вредных последствий» [4, с. 102].

В заключение отметим, что, несмотря на масштаб и сложность проблемы эффективного противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, полагаем, что модернизация уголовного закона должна осуществляться крайне осторожно, по принципу минимизации вносимых поправок. Нет никакой необходимости сплошного «насыщения» диспозиций уголовно-правовых норм, в том числе в сфере обеспечения экологической безопасности, указанием на возможность их совершения посредством информационно-коммуникационных технологий. Такие оговорки должны иметь место только в случаях пробельности уголовного закона, его очевидного несоответствия современным угрозам. Для борьбы с обозначенным явлением и обеспечения экологической безопасности необходим системный подход, тщательная разработка законодательной базы, интенсивное международное сотрудничество.

СПИСОК ЛИТЕРАТУРЫ

1. Глухова, А. А. Новейшие способы совершения киберпреступлений как угроза экономической безопасности России // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2009. – № 1. – С. 156–161.
2. Кальнер, В. Д. Цифровая экономика и экологическая безопасность жизнедеятельности // Экология и промышленность России. – 2018. – Т. 22, № 1. – С. 62–67.
3. Королева, А. Н. Правовое регулирование реализации экологических прав граждан на основе применения технологии «умный город» // Реализация и защита экологических прав граждан : сборник материалов всероссийской конференции по вопросам реализации и защиты экологических прав граждан (19 октября 2017 г., Самара) / под ред. А. Г. Безверхова, А. В. Юдина. – Самара : Вектор, 2018. – С. 175–188.
4. Кудрявцев, В. Н. Объективная сторона преступления / В. Н. Кудрявцев. – М. : Юрид. лит., 1960. – 218 с.
5. Попова, Т. Опыт развития умных городов внедряют в России [Электронный ресурс] // Независимая газета (интернет-версия). – 2018. – 26 января. – Режим доступа: http://www.ng.ru/science/2018-01-26/100_smartcity260118.html.
6. Об охране окружающей среды [Электронный ресурс] : федеральный закон от 10 января 2002 г. № 7-ФЗ. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34823/.
7. О Стратегии национальной безопасности Российской Федерации [Электронный ресурс] : указ Президента Российской Федерации от 31 декабря 2015 г. № 683. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/.

8. О Стратегии экологической безопасности Российской Федерации на период до 2025 года [Электронный ресурс] : указ Президента Российской Федерации от 19 апреля 2017 г. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_215668/.

REFERENCES

1. Glukhova A.A. Noveishie sposoby soversheniya kiberprestuplenii kak ugroza ekonomicheskoi bezopasnosti Rossii [The Latest ways of committing cyber crimes as a threat to economic security of Russia]. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii*, 2009, no. 1, pp. 156–161.

2. Kal'ner V.D. Tsifrovaya ekonomika i ekologicheskaya bezopasnost' zhiznedeyatel'nosti [Digital economy and environmental safety]. *Ekologiya i promyshlennost' Rossii*, 2018, vol. 22, no. 1, pp. 62–67.

3. Koroleva A.N. Pravovoe regulirovanie realizatsii ekologicheskikh prav grazhdan na osnove primeneniya tekhnologii «umnyi gorod» [Legal regulation of implementation of environmental rights of citizens through the application of technology «smart city»]. *Realizatsiya i zashchita ekologicheskikh prav grazhdan : sbornik materialov vserossiiskoi konferentsii po voprosam realizatsii i zashchity ekologicheskikh prav grazhdan (19 oktyabrya 2017 g., Samara)* [Realization and protection of citizens' environmental rights: proceedings of the national conference on issues of implementation and protection of citizens' environmental rights (19 October, 2017, Samara). Samara: Vector Publ., 2018, pp. 175–188.

4. Kudryavtsev V.N. *Ob"ektivnaya storona prestupleniya* [The objective side of the crime]. Moscow: Yuridicheskaya literatura Publ., 1960. 218 p.

5. Popova T. Opyt razvitiya umnykh gorodov vnedryat v Rossii [Experience of smart cities development will be introduced in Russia]. *Nezavisimaya Gazeta* (Internet version), 2018, January 26. Available at: http://www.ng.ru/science/2018-01-26/100_smartcity260118.html (accessed 16 November 2018).

6. *On Environmental Protection: Federal Law of January 10, 2002 No. 7-FZ*. Available at: http://www.consultant.ru/document/cons_doc_LAW_34823/ (accessed 16 November 2018). (In Russian).

7. *On the National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation of December 31, 2015 No. 683*. Available at: http://www.consultant.ru/document/cons_doc_LAW_191669/ (accessed 16 November 2018). (In Russian).

8. *On the Strategy of Ecological Safety of the Russian Federation for the period until 2025: Decree of the President of the Russian Federation of April 19, 2017*. Available at: http://www.consultant.ru/document/cons_doc_LAW_215668/ (accessed 16 November 2018). (In Russian).