УДК 34 **DOI: 10.34670/AR.2022.62.45.015**

Генезис противодействия киберпреступности на международном и национальном уровнях

Майстренко Григорий Александрович

Кандидат юридических наук, старший научный сотрудник,
Научно-исследовательский институт Федеральной службы исполнения наказаний России,
125130, Российская Федерация, Москва, ул. Нарвская, 15-а;
e-mail: G.Maystrenko@yandex.ru

Аннотация

В статье исследуются особенности преступлений в сфере информационно-телекоммуникационных технологий. Особое внимание обращается на основные проблемы их выявления, раскрытия и расследования. Выявляются направления международного взаимодействия в сфере противодействия киберпреступности, базирующиеся на международных нормативно-правовых актах. Отмечается необходимость изучения опыта зарубежных стран по организации деятельности подразделений по борьбе с киберпреступностью. Освещается определенный зарубежный опыт организации деятельности подразделений полиции по противодействию киберпреступности. Выделяются уровни взаимодействия оперативных подразделений внутренних дел с целью оперативного документирования преступлений в сфере информационно-телекоммуникационных технологий и виды сотрудничества органов внутренних дел с правоохранительными органами других государств. Отмечается, что совершенствование административно-правового обеспечения противодействия киберпреступности в Российской Федерации должно происходить с учетом национальных особенностей на основании детального научного анализа международного законодательства.

Для цитирования в научных исследованиях

Майстренко Г.А. Генезис противодействия киберпреступности на международном и национальном уровнях // Теории и проблемы политических исследований. 2022. Том 11. № 3А. С. 66-72. DOI: 10.34670/AR.2022.62.45.015

Ключевые слова

Информатизация общества, преступления, информационно-телекоммуникационные технологии, противодействие киберпреступности, уровни взаимодействия.

Введение

Актуальность данной темы исследования определяется тем, что среди современных тенденций развития общества весьма значимой является глобальная информатизация практически всех сфер жизнедеятельности человека, включая экономику, государственное управление, науку, образование и т. д. Широкая информатизация является основным признаком перехода цивилизованного мира к состоянию технологически нового, информационного общества [Прончев и др., 2014, 6].

Во многих развивающихся странах неуклонно растут темпы развития цифровой экономики, которые в несколько раз превышают показатели всех остальных отраслей производства. В условиях глобальной информатизации меняются характер формирования современных правоотношений в сфере распространения информации, сущность, содержание, роль и место организационно-правовых основ защиты информации, в том числе с ограниченным доступом к определенным видам информации, а вслед за этим и основы правоохранительной деятельности по обеспечению общественного порядка [Дремлюга, 2022].

Киберпреступность не является традиционным преступлением: это относительно молодое явление, которое сопряжено с появлением и распространением глобальной сети Интернет. С самого момента популяризации Интернета данный вид преступности проявил себя, информация стала уязвимым ресурсом для злоумышленников. Особая природа Всемирной сети обеспечила глобальность и анонимность для ее пользователей, что послужило в качестве предпосылки для появления данного вида преступности.

С распространением киберпреступлений связано возникновение потребности правового регулирования этого вопроса как в мире, так и в Российской Федерации. Противодействие любому негативному влиянию требует формирования понимания сущности проблемы и знания ее генезиса. Поскольку скорость развития общества неразрывно связана с достижениями научно-технического прогресса и преступными проявлениями, важными являются также обращение к вопросу исторического развития, внедрение правовых механизмов для борьбы с киберпреступностью как в мире, так и в нашем государстве.

Основная часть

В 1980-е гг., на заре развития современных информационных технологий, уровень киберпреступности в нашей стране был невысоким, поскольку уровень популяризации информационных технологий был ниже, чем в некоторых зарубежных странах. Однако сегодня нашу страну в мире воспринимают чуть ли не оплотом мирового хакерского движения, что в первую очередь связано с наличием образованного молодого поколения. Использование современных информационных технологий почти во всех сферах общественной жизни Российской Федерации, включая государственные и негосударственные структуры, ставит проблему борьбы с киберпреступностью. Кроме прямого вреда от несанкционированного доступа к информации, ее распространения, изменения, уничтожения и т. д., киберпреступность является источником угрозы национальной безопасности, экономике, правам человека и его интересам. Степень угрозы компьютерных преступлений не полностью понятна в обществе из-за отсутствия научной разработки фундаментальных понятий, связанных с ними. Поэтому отечественный законодатель и исследователи должны учитывать опыт других государств в данной сфере [Пузырева, Мысина, 2020, 42].

Сейчас происходит последний этап развития – появление новых форм компьютерных

преступлений. Как отмечает Дж. Люстхаус, среди них стоит отметить интернет-войну (впервые группы компьютерных активистов, осуждая военные действия в Югославии и НАТО, осуществляли взлом правительственных компьютеров и распространяли антивоенную интернет-пропаганду) и интернет-забастовку (групповая деятельность, которая приводит к перегрузке интернет-сайта и невозможности его посещения другими пользователями) [Lusthaus, 2018].

Очевидно, такой перечень новых форм не является исчерпывающим, но его основная цель – продемонстрировать, что вопросы правового регулирования киберпреступности в мире нуждаются в постоянной эволюции и совершенствовании, поскольку компьютерные преступники постоянно меняют направления и методы своей деятельности. Поэтому основными чертами современного этапа являются: 1) эволюция киберпреступности, появление ее новых форм; 2) попытки законодателей адекватно реагировать на эти изменения [Овчинский, 2017, 234].

Благодаря анализу юридической доктрины мы выделили следующие этапы процесса развития явления киберпреступности.

1. Подготовительная фаза (начало 1960-х – начало 1970-х гг.) – от первых преступлений с применением компьютеров до появления организованных преступных групп компьютерных злоумышленников, которые использовали собственные знания для незаконного обогащения и нарушали установленный порядок.

2. Этап распространения киберпреступности (начало 1970-х гг. – 1989 г.) – от появления хакеров и их организованных групп до принятия первого регуляторного акта о киберпреступности и первого в истории ареста хакеров.

3. Этап транснациональной киберпреступности и кибертерроризма (1994 г. – начало XXI в.) – от «дела Владимира Левина», которое можно считать первой крупной международной транснациональной киберпреступностью, до начала нового века, в котором не было значительных исторических событий развития кибертерроризма, но происходила систематическая эволюция киберпреступности (конечная дата была выбрана условно).

4. Современная стадия киберпреступности (XXI в.) – возникновение новых форм компьютерных преступлений. Эволюционным является принятие в Российской Федерации Федерального закона от 27 июля 2006 г. № 152-ФЗ. С этого момента россияне оказались под государственной защитой от преступников в сфере информационных технологий.

Итак, мы установили, что генезис развития и генезис правового регулирования борьбы с киберпреступностью невозможно идентифицировать. Киберпреступность развивается в соответствии с эволюцией новейших технологий, поэтому сегодня это область, которая постоянно находится на шаг впереди своей регуляторной базы.

Принимая во внимание стадию развития, отметим, что на первых двух этапах законодательное регулирование этого института практически не было осуществлено. Так, нами приведен пример киберпреступления, в результате которого произошло первое задержание хакеров, однако их условное наказание свидетельствует об отсутствии на тот момент адекватных инструментов борьбы с компьютерными преступниками. На втором и третьем этапах правовое регулирование борьбы с киберпреступностью в мире уже проходило полноценно.

Первый этап генезиса правового регулирования борьбы с киберпреступностью будет ограничен периодом с 1986 г., т. е. принятием первого компьютерного закона в истории, до 1989 г., когда была принята Рекомендация Комитета министров Совета Европы № R (89) 9, что

существенно повлияло на дальнейшее развитие законодательства о киберпреступности и послужило толчком к изменениям в уголовном законодательстве в европейских странах. Так, после 1989 г. началась быстрая эволюция уголовного права европейских государств в части усиления борьбы с компьютерными преступлениями, которая активно продолжается и по сей день [Рыжов, 2018, 11].

Первый этап генезиса правового регулирования киберпреступности в мире характеризуется следующими особенностями: принятием первого в истории «компьютерного» закона; внесением изменений в национальное уголовное законодательство в некоторых странах; принятием рекомендаций европейским странам по борьбе с киберпреступностью, что впоследствии значительно повлияло на быстрое развитие европейского законодательства. Важность начальной фазы заключается в том, что к моменту своего возникновения киберпреступность уже росла с тревожной скоростью и быстро развивалась. Принятие первых регламентов не повлияло на уменьшение киберпреступности, однако оно продемонстрировало желание ведущих стран бороться с этим негативным явлением. Поэтому, по нашему мнению, 1989 г. является исходной датой для следующего этапа генезиса правового регулирования киберпреступности в мире – внесения изменений в уголовное законодательство европейских стран, что продолжалось условно до 2000 г. Использование слова «условно» является обусловлено тем, что этот процесс в целом продолжается и по сей день. 2000 г. означает начало принятия важных международно-правовых актов, которые сегодня составляют основу европейского и мирового законодательства о киберпреступности. Такими международно-правовыми инструментами по регулированию международных отношений в этой области, к примеру, являются Конвенция ООН против транснациональной организованной преступности, Резолюция № 55/59 Генеральной Ассамблеи ООН «Венская декларация о преступности и правосудии: ответы на вызовы XXI века», Конвенция о преступности в сфере компьютерной информации ETS № 185, Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем ETS № 189, а также Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий.

По справедливому мнению Д.В. Пучкова, фактически за последние три десятилетия в международном праве появился ряд актов, которые имели значительное влияние на борьбу с киберпреступностью [Пучков, 2020, 84]. Вот почему мы назвали третью стадию генезиса правового регулирования борьбы с киберпреступностью в мире «консолидацией» и хронологически ограничили ее. Сегодня этот этап следует рассматривать как самый важный, поскольку киберпреступники всегда опережали развитие законодательных норм. Однако с начала XXI в. развитые страны изъявили готовность принимать жесткие меры по борьбе с киберпреступностью. Таким образом, третий этап генезиса правового регулирования борьбы с киберпреступностью в мире характеризуют следующие признаки: 1) динамическая эволюция национальных законов ведущих государств с точки зрения усиления уголовной ответственности за совершение компьютерных преступлений; 2) принятие основных международных правовых актов относительно сотрудничества и взаимопомощи ведущих стран мира в вопросах кибербезопасности, которые сегодня составляют правовую основу сферы противодействия киберпреступности; 3) выход законодателей на новый уровень в борьбе с киберпреступниками вследствие усиления межгосударственных отношений и расширения содержания понятия киберпреступности.

Что касается следующего периода, который является последним, мы считаем, что это современный этап правового регулирования борьбы с киберпреступностью, который продолжается и сегодня. Этот период можно охарактеризовать с учетом конкретных основных событий, которые произошли или происходят. Его главная характеристика – совершенствование законодательства о киберпреступности государствами, которые на несколько шагов отстают от развитых стран. Выделяя специфические особенности современного этапа, отметим следующее: 1) международное право существенно не изменилось, но постепенно развивается; 2) увеличилось количество стран мира, принимающих участие в борьбе с киберпреступностью.

Заключение

Изучение генезиса правового регулирования борьбы с киберпреступностью в мире требует выделения собственной исторической классификации. В процессе анализа научной доктрины мы установили, что исследовательский вопрос следует классифицировать следующим образом: 1-й этап – создание правовых основ регулирования борьбы с киберпреступностью (1986-1989 гг.) – от принятия первого в истории компьютерного закона до принятия Рекомендации Комитета министров Совета Европы № R (89) 9, которая имела решающее значение для дальнейшего развития законодательства, направленного на борьбу с киберпреступностью, и действовала как толчок для развития уголовного права; 2-й этап – изменение уголовного закона развитых стран (1989-2000 гг.) – быстрая эволюция уголовного права европейских государств с точки зрения активизации борьбы с киберпреступностью, которая в определенной мере продолжается и по сей день (конечный срок этого периода мы условно связываем с 2000 г., после которого дальнейшие изменения в национальные законы уже не носят массового характера); 3-й этап – консолидация международного сообщества в борьбе с киберпреступностью (2000-2001 гг.) – появление в международном праве ряда актов, которые имели значительное влияние на борьбу с киберпреступностью; 4-й этап – современная стадия правового регулирования борьбы с киберпреступностью (с 2001 г.) – совершенствование законодательства о киберпреступности. С этого момента в России на всех уровнях государственной власти произошли существенные изменения по передаче персональных данных, базы данных граждан РФ получили защиту от произвольного распространения и передачи третьим лицам.

Борьба с преступностью является комплексной активной системой мер, применяемых в качестве реакции государства на противоправную деятельность лиц или их групп, и входит в компетенцию правоохранительных органов и органа законодательной власти по преодолению данной проблемы.

Библиография

1. Дремлюга Р.И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение. М.: Юрлитинформ, 2022. 325 с.
2. О персональных данных: федер. закон Рос. Федерации от 27.07.2006 № 152-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 08.07.2006: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14.07.2006. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/
3. Овчинский В.С. (сост.) Основы борьбы с киберпреступностью и кибертерроризмом. М.: Норма, 2017. 527 с.
4. Прончев Г.Б. и др. Проблемы безопасности информационного общества современной России. М.: Экон-Информ, 2014. 215 с.
5. Пузырева Ю.В., Мысина А.И. Международное полицейское сотрудничество по вопросам раскрытия и

расследования преступлений в сфере информационных технологий. М.: ИНФРА-М, 2020. 91 с.
6. Пучков Д.В. Кибернетические технологии в социально-биологической сфере: уголовно-правовые аспекты. М.: Юрлитинформ, 2020. 196 с.
7. Рыжов В.Б. Информационная безопасность в государствах Европейского союза: к постановке проблемы // Представительная власть – XXI век: законодательство, комментарии, проблемы. 2018. № 4. С. 8-12.
8. Смирнова И.Г. и др. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ. М.: Юрлитинформ, 2016. 306 с.
9. Lusthaus J. Industry of anonymity: inside the business of cybercrime. Cambridge: Harvard University Press, 2018. 289 p.
10. Recommendation No. R (89) 9 of the Committee of Ministers to member states on computer-related crime. URL: https://rm.coe.int/09000016804f1094

The genesis of countering cybercrime at the international and national levels

Grigorii A. Maistrenko

PhD in Law, Senior Researcher,
Scientific-Research Institute of the Federal Penitentiary Service of the Russian Federation,
125130, 15-a, Narvskaya str., Moscow, Russian Federation;
e-mail: G.Maystrenko@yandex.ru

Abstract

The article aims to identify the features of crimes in the field of information and telecommunication technologies. Special attention is paid to the main problems of detecting, solving and investigating them in the Russian Federation. The author of the article makes an attempt to identify the directions in international cooperation in the field of countering cybercrime, based on international legal acts. The article points out that it is necessary to study the experience of foreign countries in the organization of the activities of cybercrime units, highlights foreign experience in the organization of the activities of cybercrime units of the police, and identifies the levels of interaction among operational units of internal affairs for the purpose of operational documentation of crimes in the field of information and telecommunication technologies and the types of cooperation of the internal affairs bodies of the Russian Federation with law enforcement agencies of other states. Having considered the genesis of countering cybercrime at the international and national levels, the author comes to the conclusion that administrative legal support for countering cybercrime in the Russian Federation should be improved with due regard to national peculiarities and on the basis of the results of a detailed scientific analysis of international legislation.

For citation

Maistrenko G.A. (2022) Genezis protivodeistviya kiberprestupnosti na mezhdunarodnom i natsional'nom urovnyakh [The genesis of countering cybercrime at the international and national levels]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 11 (3A), pp. 66-72. DOI: 10.34670/AR.2022.62.45.015

Keywords

Informatization of society, crimes, information and telecommunication technologies, countering cybercrime, levels of interaction.

References

1. Dremlyuga R.I. (2022) Ugolovno-pravovaya okhrana tsifrovoi ekonomiki i informatsionnogo obshchestva ot kiberprestupnykh posyagatel'stv: doktrina, zakon, pravoprimenenie [Criminal law protection of the digital economy and information society from cyberattacks: doctrine, law, law enforcement]. Moscow: Yurlitinform Publ.
2. Lusthaus J. (2018) Industry of anonymity: inside the business of cybercrime. Cambridge: Harvard University Press.
3. O personal'nykh dannykh: feder. zakon Ros. Federatsii ot 27.07.2006 № 152-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 08.07.2006: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 14.07.2006 [On personal data: Federal Law of the Russian Federation No. 152-FZ of July 27, 2006]. Available at: http://www.consultant.ru/document/cons_doc_LAW_61801/ [Accessed 12/08/22].
4. Ovchinskii V.S. (comp.) (2017) Osnovy bor'by s kiberprestupnost'yu i kiberterrorizmom [The fundamentals of combating cybercrime and cyberterrorism]. Moscow: Norma Publ.
5. Pronchev G.B. et al. (2014) Problemy bezopasnosti informatsionnogo obshchestva sovremennoi Rossii [Security problems of the information society of modern Russia]. Moscow: Ekon-Inform Publ.
6. Puchkov D.V. (2020) Kiberneticheskie tekhnologii v sotsial'no-biologicheskoi sfere: ugolovno-pravovye aspekty [Cybernetic technologies in the sociobiological sphere: criminal legal aspects]. Moscow: Yurlitinform Publ.
7. Puzyreva Yu.V., Mysina A.I. (2020) Mezhdunarodnoe politseiskoe sotrudnichestvo po voprosam raskrytiya i rassledovaniya prestuplenii v sfere informatsionnykh tekhnologii [International police cooperation on solving and investigating crimes in the field of information technology]. Moscow: INFRA-M Publ.
8. Recommendation No. R (89) 9 of the Committee of Ministers to member states on computer-related crime. Available at: https://rm.coe.int/09000016804f1094 [Accessed 12/08/22].
9. Ryzhov V.B. (2018) Informatsionnaya bezopasnost' v gosudarstvakh Evropeiskogo soyuza: k postanovke problemy [Information security in the European Union: the problem statement]. Predstavitel'naya vlast' – XXI vek [Representative power – the 21st century], 4, pp. 8-12.
10. Smirnova I.G. et al. (2016) Kiberprestupnost': kriminologicheskii, ugolovno-pravovoi, ugolovno-protsessual'nyi i kriminalisticheskii analiz [Cybercrime: criminological, criminal legal, criminal procedural and forensic analysis]. Moscow: Yurlitinform Publ.