УДК 004.056
https://doi.org/10.34680/BENEFICIUM.2019.3(32).93-100

КИБЕРБЕЗОПАСНОСТЬ КАК ПРЕДМЕТ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА ПОЛИЦИИ СОВРЕМЕННЫХ ГОСУДАРСТВ

СТЕПАНЯН А.И.
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, г. Санкт-Петербург, Россия

Активизация процесса развития информационно-коммуникационных технологий (ИКТ), отмечаемая в современном мире, открывает все возможности, обусловленные глобальным характером данного явления, а также легкостью и удобством использования его продуктов, для развития и упрощения организации бизнес-процессов и коммуникаций в современном обществе и в правовой сфере его жизни, в частности. Однако неотъемлемой частью процесса информатизации является и появление новых возможностей для преступников, которые могут воспользоваться теми же его преимуществами. Одной из актуальных проблем в современной полицейской деятельности является киберпреступность – быстро изменяющееся явление поистине глобального характера. В статье рассматриваются уникальные вызовы киберпреступности для полицейской деятельности в киберпространстве, которые требуют пересмотра традиционных подходов к понятию полицейской деятельности, применения новых инструментов (как законодательных, так и технических) для расследования такого рода преступлений, развития навыков работы с электронными доказательствами и, что не менее важно, умения сотрудничать с поставщиками Интернет-услуг. Проводится анализ роли международного сотрудничества полиции в обеспечении кибербезопасности России. Подчеркивается необходимость гармонизации законодательных подходов и обеспечения скоординированных действий по предупреждению и расследованию киберпреступности на различных уровнях: национальном, региональном и международном. Сделан вывод о необходимости формирования цифрового доверия, обеспечения безопасности и конфиденциальности посредством принятия согласованного набора нормативных правовых актов на региональном и международном уровнях в отношении использования ИКТ в преступных или других неправомерных целях; объединения адекватных технических возможностей для выявления и быстрого реагирования на кибератаки;

Образец цитирования:
Степанян А.И. (2019). Кибербезопасность как предмет международного сотрудничества полиции современных государств. *BENEFICIUM. 2019. 3(32):* 93-100. doi: https://doi.org/10.34680/BENEFICIUM.2019.3(32).93-100

For citation:
Stepanyan A.I. (2019). Cybersecurity as a Subject of International Cooperation between the Police of Modern States. *BENEFICIUM. 2019. 3(32):* 93-100. (In Russ.). doi: https://doi.org/10.34680/BENEFICIUM.2019.3(32).93-100

разработки минимальных критериев безопасности и схем аккредитации для программных приложений и систем.

Ключевые слова: глобализация девиантности; Интернет; информационно-коммуникационные технологии (ИКТ); кибербезопасность; киберпреступность; международное полицейское сотрудничество; полицейская деятельность; терроризм; транснациональная организованная преступность.

CYBERSECURITY AS A SUBJECT OF INTERNATIONAL COOPERATION BETWEEN THE POLICE OF MODERN STATES

STEPANYAN A.I.
Saint Petersburg University of the Ministry of Internal Affairs of the Russian Federation, Saint Petersburg, Russia

The intensification of the process of development of information and communication technologies (ICT), noted in the modern world, opens up all the opportunities due to the global nature of this phenomenon, as well as the ease and convenience of using its products, for the development and simplification of business processes and communications in modern society and in the legal sphere of its life, in particular. However, an integral part of the process of informatization is also the emergence of new opportunities for criminals who can take advantage of the same benefits. One of the most pressing problems in modern policing is cybercrime – a rapidly changing phenomenon of a truly global nature. The article discusses the unique challenges of cybercrime for police activity in cyberspace, which require a revision of traditional approaches to the concept of police activity, the use of new tools (both legislative and technical) for the investigation of such crimes, the development of skills to work with electronic evidence and, equally important, the ability to cooperate with Internet service providers. The article analyzes the role of international police cooperation in ensuring cybersecurity in Russia. It emphasizes the need to harmonize legislative approaches and ensure coordinated action to prevent and investigate cybercrime at various levels: national, regional and international. It is concluded that there is a need to build digital trust, security and confidentiality through the adoption of a coherent set of regulations at the regional and international levels regarding the use of ICT for criminal or other illegal purposes; the integration of adequate technical capabilities to identify and respond quickly to cyber attacks; the development of minimum security criteria and accreditation schemes for software applications and systems.

Keywords: globalization of deviance; Internet; information and communication technologies (ICT); cybersecurity; cybercrime; international police cooperation; police activity; terrorism; transnational organized crime.

Происходящие в современном мире процессы глобализации касаются практически всех сфер жизнедеятельности российского общества и детерминируют неизбежность преобразования существующих общественных отношений и, соответственно, трансформации деятельности государственных, в том числе правоохранительных, органов в соответствии с вызовами современности. Необходимость обеспечения способности правоохранительных структур осуществлять охрану и защиту прав и свобод личности в новых реалиях требует анализа опыта международного сотрудничества в сфере противодействия разным видам преступности, в том числе новым ее формам и проявлениям. При этом должна измениться концепция функционирования национальных правоохранительных систем и их структурных составляющих – полицейских систем. В условиях развития транснациональной преступности и выхода ее за рамки государственных границ, приоритетным направлением деятельности полицейских органов становится не карательная функция, а обеспечение правопорядка и общественной безопасности, профилактика и контроль над преступностью, предоставление широкого спектра социальных услуг населению [Nizhnik, 2017; Lavrinovich, 2017; Нижник, 2018; Нижник, 2019].

Глобализация (интернационализация) различных форм девиантности, включая организованную преступность в сфере проституции, наркотизма, терроризма, торговли людьми, – это вполне закономерный процесс, поскольку структура, масштабы и динамика девиантности и преступности напрямую обусловлены экономическими, политическими, социальными, демографическими факторами [Пинчук, 2018; Гилинский, 2008].

Одной из форм транснациональной организованной преступности выступает киберпреступность. Киберпространство остается главным источником различных незаконных действий, которые обуславливают миграцию традиционных преступлений, таких как детская порнография, мошенничество и нарушение авторских прав, в сети информационно-коммуникационных технологий (ИКТ).

Существующие подходы к борьбе с преступностью в реальном мире зачастую не работают в киберпространстве или не могут быть применимы к неправомерному использованию ИКТ в преступных целях. Разработка комплексного подхода к различным аспектам киберпреступности сопряжена с уникальными вызовами, которые являются новыми как для законодателей, так и для следственных органов и должны учитываться при разработке стратегий борьбы с преступностью в виртуальном мире:

– увеличение числа пользователей, подключенных к глобальной коммуникационной сети, являет собой сложную задачу для полиции в киберпространстве, поскольку одним из основных слабых мест, которые представляют возможность для преступников, является отсутствие понимания индивидуальной безопасности в интернете наряду с применением методов социальной инженерии;

– использование преступниками различных возможностей для сокрытия личных данных в глобальных сетях затрудняет правоохранительным органам отслеживание правонарушителей;

– наличие горизонтальной структуры и децентрализованной архитектуры сети затрудняют правоохранительным органам контроль за деятельностью в интернете и препятствуют расследованию преступлений, совершенных в киберпространстве;

– противоречие, связанное с тем, что уголовное право и уголовные расследования рассматриваются как вопрос национального суверенитета, в то время как протоколы, применяемые для передачи данных через Интернет, основаны на наиболее оптимальной маршрутизации, означающей, что процессы передачи данных проходят через две и более стран.

Глобальный контекст преступности, связанной с интернетом, и трансграничный характер сетей ИКТ также вызывают необходимость гармонизации законодательных подходов и скоординированных действий по предупреждению и расследованию киберпреступности на различных уровнях: национальном, региональном и международном. Так, представителями государств БРИКС на саммите в г. Уфе (Россия) 8-9 июля 2015 г. были рассмотрены проблемы противодействия использованию ИКТ «для целей транснациональной организованной преступности, разработки оружия и осуществления террористических актов»[1]. А в итоговом документе саммита Россия – АСЕАН, прошедшем в Сочи 19-20 мая 2016 г., в числе проявлений транснациональной организованной преступности, наряду с торговлей людьми, нелегальной миграцией, морским пиратством, контрабандой оружия, международной экономической преступностью и отмыванием денег, была названа и киберпреступность[2]. Концепция внешней политики Российской Федерации относит киберпреступность к вызовам и угрозам, имеющим «трансграничную природу» (п. 17) и обращает внимание на необходимость активизации совместной работы России и Европейского Союза (ЕС) по противодействию организованной преступности, включая такое ее проявление, как киберпреступность (п. 64)[3].

В ЕС правовая основа противодействия киберпреступности развивалась в условиях принятия законодательства об атаках на информационные системы[4] и использовании данных системы бронирования для предотвращения, выявления, расследования и уголовного преследования преступлений терро-

[1] Уфимская декларация VII саммита БРИКС (Принята в г. Уфе 09.07.2015) (2015). URL: http://brics2015.ru/ (дата обращения: 20.10.2019).

[2] Сочинская декларация юбилейного саммита Россия – АСЕАН в связи с 20-летием установления диалогового партнерства между Российской Федерацией и АСЕАН «На пути к взаимовыгодному стратегическому партнерству» (Принята в г. Сочи 20.05.2016) (2016). URL: http://russia-asean20.ru (дата обращения: 21.10.2019).

[3] Концепция внешней политики Российской Федерации (2016). URL: https://www.garant.ru/products/ipo/prime/doc/71452062/ (дата обращения: 15.10.2019).

[4] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (2013). *Official Journal of the European Union, №L218, August, 14, 2013:* 8. (In Eng.).

ристической направленности и тяжких преступлений[1]. В настоящее время государства – члены ЕС используют механизмы противодействия киберпреступности, разработанные на международном уровне. Конвенция о преступности в сфере компьютерной информации (Будапештская конвенция)[2] была подписана не только странами – членами ЕС, но и многими другими государствами – членами Совета Европы, Канадой, Японией, ЮАР, США; она вступила в силу 1 июля 2004 г. В Конвенции получили рассмотрение различные виды преступлений в сфере ИКТ: против конфиденциальности, целостности и доступности компьютерных данных и систем, подлог и мошенничество с использованием компьютеров, преступления, связанные с содержанием данных, в особенности преступления, связанные с детской порнографией, а также преступления, связанные с нарушением авторского и смежных прав (гл. I разд. 1, ч. 1-4).

В вышеназванных международных нормативных актах акцентируется внимание на продуктивности международного сотрудничества в сфере противодействия киберпреступности и необходимости его дальнейшего развития. Транснациональность киберпреступности проявляется, в частности, в том, что электронные письма с незаконным контентом или часто проходят через многие страны во время передачи от отправителя получателю, или незаконный контент может храниться за пределами страны, или незаконный доступ к нему осуществляется с ip-адреса, физически находящегося в другой стране. Есть и другие примеры преступлений в области компьютерных технологий, осложненных международным элементом, однако уголовное преследование на глобальном уровне обычно ограничивается теми преступлениями, которые криминализированы во всех странах, участвующих в расследовании [Understanding cybercrime, 2012]. Таким образом преступники могут использовать пробелы в материальном уголовном праве, действуя из стран, не имеющих эффективного законодательства о киберпреступности.

На данном этапе особую актуальность получил вопрос, связанный с неравномерной криминализацией ответственности за преступления, совершенные в киберпространстве во всем мире. Практика такова, что все большее количество преступлений в киберпространстве совершается со стороны юридических лиц. Неслучайно, что еще Будапештская конвенция на повестку дня ставила вопрос о коллективной ответственности юридических лиц[3].

Как показывает практика, целью кибератак чаще всего является хищение информации. В основном, преступники стремятся получить сведения о рос-

[1] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (2016). *Official Journal of the European Union, №L119, May, 4, 2016:* 132. (In Eng.).

[2] Convention on Cybercrime. Budapest, 23.XI.2001 (ETS – No. 185) (2001). (In Eng.). Retrieved October 4, 2019, from: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

[3] Convention on Cybercrime. Budapest, 23.XI.2001 (ETS – No. 185) (2001). (In Eng.). Retrieved October 4, 2019, from: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

сийских технологиях в оборонной промышленности, атомной промышленности, энергетике и ракетостроении, а также информацию из банковского сектора и систем государственного управления. Так, в 2018 г. выявленные хакерские атаки были направлены на кражу данных из российских учреждений кредитно-финансовой сферы (38%), органов государственной власти (35%), учреждений образования (7%), предприятий оборонной промышленности (7%), объектов ракетно-космической отрасли (4%), учреждений здравоохранения (3%) [Брифинг заместителя директора Национального координационного центра по компьютерным инцидентам, 2019].

В Российской Федерации преступлением признается не только использование и распространение вредоносного программного обеспечения, а также и его разработка. В последнее время динамика преступности в этой области остается стабильна. Так, в частности, по ст. 272 Уголовного кодекса Российской Федерации «Неправомерный доступ к компьютерной информации» в 2013 г. было выявлено 1799 преступлений, в 2015 г. – 1396, в 2017 г. – 1079, в 2018 г. – 1240; по ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ» в 2013 г. зарегистрировано 764 преступления, в 2015 г. – 974, в 2017 г. – 802, в 2018 г. – 592 [Брифинг заместителя директора Национального координационного центра по компьютерным инцидентам, 2019].

Всего в результате деятельности созданного в сентябре 2018 г. в России Национального координационного центра по компьютерным инцидентам (НКЦКИ) совместно с зарубежными партнерами уже предотвращено более 7 тыс. кибератак на различные объекты России и стран Организации Договора о коллективной безопасности (ОДКБ).

На базе НКЦКИ осуществляется активный обмен информацией о компьютерных инцидентах с партнерами из 122 стран мира. Центр объединяет все больше объектов критической информационной инфраструктуры: иностранные партнеры предоставляют ценную информацию, делятся опытом работы в сфере противодействия киберпреступности. Эффективность регионального сотрудничества очевидна.

Уникальные вызовы киберпреступности для полицейской деятельности в киберпространстве требуют пересмотра традиционных подходов к понятию полицейской деятельности, а также применения новых инструментов (как законодательных, так и технических) для расследования, развития навыков работы с электронными доказательствами, умения сотрудничать с отраслевыми игроками. Для этого необходима правовая основа, созданная на международном уровне. Кибербезопасность для устойчивого государственного управления требует постоянных обновлений, в том числе для уже существующих систем цифровой безопасности, а также повышения компетенций госслужащих в области кибербезопасности. Существует необходимость в создании цифрового доверия, безопасности и конфиденциальности, что может быть установлено с помощью реализации таких мер в области кибербезопасности, как:

– принятие согласованного набора нормативных правовых актов на региональном и международном уровнях в отношении использования ИКТ в преступных или других неправомерных целях;

– объединение адекватных технических возможностей для выявления и быстрого реагирования на кибератаки и обеспечение атмосферы доверия и безопасности;

– разработка минимальных критериев безопасности и схем аккредитации для программных приложений и систем.

Библиография

1. Брифинг заместителя директора Национального координационного центра по компьютерным инцидентам (2019). URL: https://tass.ru/obschestvo/6599550 (дата обращения: 13.10.2019).

2. Гилинский, Я.И. (2008). Глобализация и преступность. *Криминология: вчера, сегодня, завтра, 2008, №2(15),* С. 23-32.

3. Lavrinovich, K.I. (2017). The specifics of the implementation of the law enforcement function of the modern state based on the rule of law (on the example of the Russian Federation). *International Scientific Conference «Archibald Reiss Days» (Belgrade, 7-9 November, 2017): Thematic Conference Proceedings of International Significance. Vol. II.* – Beograd: Kriminalističko-policijska akademija, 2017. – pp. 261-267. (In Eng.).

4. Nizhnik, N.S. (2017). Police and civil society institutions: search for a vector of interaction in the field of combating crime. *International Scientific Conference «Archibald Reiss Days» (Belgrade, 7-9 November, 2017): Thematic Conference Proceedings of International Significance. Vol. II.* – Beograd: Kriminalističko-policijska akademija, 2017. – pp. 241-251. (In Eng.).

5. Нижник, Н.С. (2018). Полиция и гражданское общество: поиск вектора взаимодействия. *Полицейская деятельность, 2018, №5,* С. 52-66.

6. Нижник, Н.С. (2019). Правоохранительная система государства: содержание и организационное оформление. *Право и государство: проблемы, методологии, теории и истории: Материалы международной научной конференции. 16 мая 2019 г., Краснодарский университет МВД России / Под ред. Л.В. Карнаушенко.* – Краснодар, 2019.

7. Пинчук, А.Ю. (2018). *Международный терроризм как феномен современного миропорядка: монография.* – Казань: Бук, 2018.

8. Understanding cybercrime: phenomena, challenges and legal response (2012). September, 2012, p. 4. (In Eng.). Retrieved October 4, 2019, from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

References

1. Brifing zamestitelya direktora Natsional'nogo koordinatsionnogo tsentra po komp'yuternym intsidentam [Briefing by the Deputy Director of the National

Computer Incident Coordination Center] (2019). (In Russ.). Retrieved October 13, 2019, from: https://tass.ru/obschestvo/6599550.

2. Gilinskiy, Ya.I. (2008). Globalizatsiya i prestupnost' [Globalization and crime]. *Kriminologiya: vchera, segodnya, zavtra [Criminology: yesterday, today, tomorrow], 2008, №2(15)*: 23-32. (In Russ.).

3. Lavrinovich, K.I. (2017). The specifics of the implementation of the law enforcement function of the modern state based on the rule of law (on the example of the Russian Federation). *International Scientific Conference «Archibald Reiss Days» (Belgrade, 7-9 November, 2017): Thematic Conference Proceedings of International Significance. Vol. II.* – Beograd: Kriminalističko-policijska akademija, 2017. – pp. 261-267.

4. Nizhnik, N.S. (2017). Police and civil society institutions: search for a vector of interaction in the field of combating crime. *International Scientific Conference «Archibald Reiss Days» (Belgrade, 7-9 November, 2017): Thematic Conference Proceedings of International Significance. Vol. II.* – Beograd: Kriminalističko-policijska akademija, 2017. – pp. 241-251.

5. Nizhnik, N.S. (2018). Politsiya i grazhdanskoe obshchestvo: poisk vektora vzaimodeystviya [Police and civil society: finding a vector of interaction]. *Politseyskaya deyatel'nost' [Police activity], 2018, № 5*: 52-66. DOI: 10.7256/2454-0692.2018.5.23796. (In Russ.).

6. Nizhnik, N.S. (2019). Pravookhranitel'naya sistema gosudarstva: soderzhaniye i organizatsionnoye oformleniye [Law enforcement system of the state: content and organizational figuration]. *Pravo i gosudarstvo: problemy, metodologii, teorii i istorii: Materialy mezhdunarodnoy nauchnoy konferentsii. 16 maya 2019 g., Krasnodarskiy universitet MVD Rossii / Pod red. L.V. Karnaushenko [Law and State: Problems, Methodologies, Theories and History: Materials of an international scientific conference. May 16, 2019, Krasnodar University of the Ministry of Internal Affairs of Russia / Ed. L.V. Karnaushenko].* – Krasnodar, 2019. (In Russ.).

7. Pinchuk, A.Yu. (2018). *Mezhdunarodnyy terrorizm kak fenomen sovremennogo miroporyadka: monografiya [International terrorism as a phenomenon of the modern world order: monograph]*. – Kazan: Buk, 2018. (In Russ.).

8. Understanding cybercrime: phenomena, challenges and legal response (2012). September, 2012, p. 4. Retrieved October 4, 2019, from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.