УДК 34.400
ББК 64.700

DOI 10.47475/2618-8236-2021-16305

Понятие и место информационной безопасности в национальной безопасности России

Ш. Г. Утарбеков

Челябинский государственный университет, Челябинск, Россия

Обеспечение на современном этапе национальной безопасности обусловливает определение стратегических направлений, содействующих охране законных прав и интересов человека, общества и государства от внешнего и внутреннего неблагоприятного воздействия. В условиях высоких темпов развития технико-информационных ресурсов актуализируется проблема оптимизации средств в сфере информационной безопасности.

Ключевые слова: *информационная безопасность, компьютерная информация, право на информацию.*

Согласно системе данных официальной статистики МВД РФ, регистрация преступлений с использованием компьютерных и телекоммуникационных технологий стала осуществляться с 2017 г.[1] В 2017 г. было зарегистрировано 90 587 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. Относительный показатель преступлений рассматриваемого вида в общем перечне преступности составил 4,4%. Тенденция существенного роста показателей данного вида преступности наметилась в 2018 г., когда было зарегистрировано 174 674 преступления, совершенных с использованием компьютерных и телекоммуникационных технологий. В результате доля указанных преступлений в общем перечне преступности увеличилась до 8,77%. Тенденция роста абсолютных и относительных показателей преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, сохраняется в 2019–2020 гг. Исходя из данных официальной статистики, количество преступлений с использованием компьютерных и телекоммуникационных технологий в 2019 г. составило 294 409. Удельный вес данного вида преступлений в общей структуре преступности в 2019 г. достиг 14,54%. В 2020 г. было зарегистрировано 510 396 преступлений данного вида, доля которых в общей преступности возросла до 24,96%. Таким образом, показатели преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, характеризуются устойчивым ростом.

Обращаясь к вопросу о противодействии угрозам кибербезопасности, необходимо подчеркнуть, что данный аспект подлежал активному обсуждению на международном уровне с начала 1980-х гг. Следует сказать, что Российская Федерация не ратифицировала Европейскую конвенцию в силу того, что условием России являлся пересмотр п. *b* ст. 32. В данной конвенциональной норме устанавливалась возможность доступа и получения следственными органами через компьютерную систему к хранящимся на территории другой стороны компьютерным данным.

Учитывая нарастающие угрозы кибербезопасности, Россия в 2016 г. разрабатывает проект Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности. Универсальный характер данного проекта позволяет объединить мировое сообщество в борьбе с киберпреступностью. Проект изначально был представлен иностранным партнерам на совещании руководителей специальных служб, организованном секретарем Совета Безопасности РФ. Исходя из цели представленного проекта, направленной на консолидацию международным сообществом ресурсов по предупреждению преступлений и противоправных деяний в области информационно-коммуникационных технологий, разработан перечень противоправных посягательств, включающий: 1) преступления, сопряженные с охраняемой национальным правом информацией; 2) неправомерный доступ к информации; 3) разработку и использование вредоносных программ и спама; 4) преступления, связанные с детской порнографией; 5) нарушение авторских прав [1. С. 11].

[1] Министерство внутренних дел Российской Федерации (http://www.mvd.ru/presscenter/statistics/reports/how; дата обращения 22.07.2021).

Представленный Россией проект «О сотрудничестве в сфере противодействия информационной преступности» содержит меры, содействующие техническому правовому взаимодействию. Особое внимание акцентируется на проведении совместных расследований, сборе параметров трафика и передаче осужденных. Практическое значение имеет образование работающего в круглосуточном режиме контактного центра. Стоит сказать, что отличие данного проекта от Европейской конвенции состоит: 1) в универсализации норм международного права под эгидой ООН; 2) исключении вероятности внедрения специальных служб в компьютерные системы иностранных государств; 3) создании механизма по соблюдению суверенитета государств.

Российская Федерация в рамках Генеральной Ассамблеи ООН 2017 г. активно промульгировала идею объединения усилий государств по противодействию киберпреступности. Для этого на обсуждение был вынесен вопрос о принятии на основании предлагаемого Россией проекта Конвенции о борьбе с киберпреступностью универсального характера. В качестве ключевого направления обеспечения кибербезопасности в современном информационном пространстве определена разработка правил ответственного поведения в цифровой области. Пристальное внимание сосредоточено на разработке и реализации странами-участниками мер, противодействующих хакерству как одному из распространенных видов киберпреступности [2. С. 14].

Разрешение проблемы по преодолению угрозы кибербезопасности в условиях современных глобализационных процессов предопределило повышенный интерес к созданию механизма, предусматривающего недопустимость использования информационно-коммуникационных технологий как средства воздействия, причинения экономического вреда, пропаганды террористической и экстремистской идеологии. Примечательно, что Россией были высказаны предложения о формировании российско-американской группы кибербезопасности [2. С. 21].

В ходе заседания Генеральной Ассамблеи ООН 9 ноября 2018 г. Россией предложен проект резолюции, раскрывающий целесообразность создания Кодекса ответственного поведения государств в Интернете. Согласно данному проекту, открывающиеся новые возможности в сфере информационно-коммуникационных технологий неизбежно отражаются на росте соответствующих видов преступности. Вследствие этого на международном уровне актуализируется необходимость:

1) образования в рамках Генеральной Ассамблеи ООН рабочей группы открытого состава по международной информационной безопасности;
2) регламентации перечня правил ответственного поведения стран в пределах информационного пространства.

В проекте особое внимание акцентировалось на нарастающей тенденции увеличения количества преступлений в цифровом мире и негативном их влиянии, детерминирующем критическое состояние инфраструктуры стран. В этой связи были высказаны предложения о необходимости детализации международным сообществом правил поведения государств, направленных на решение вопросов по обмену информацией. В качестве новых угроз кибербезопасности отмечены такие уголовно-правовые посягательства, как: неправомерный доступ в электронной форме к информации; воздействие на информацию и ее перехват; создание, распространение и использование вредоносных программ; незаконный оборот устройств, хищение путем использования цифровых технологий; распространение спама и др.

Вопрос международного сотрудничества с целью эффективного противостояния киберугрозам и кибератакам вновь подлежал обсуждению 20 мая 2019 г. на 28-й сессии Комиссии ООН по предупреждению преступности и уголовному правосудию. Подчеркивая актуальность данной проблемы, международное сообщество отметило насущную потребность в совершенствовании нормативно-правовой основы в сфере борьбы с киберпреступностью. С учетом целесообразности комплексного подхода к анализу мировой ситуации в области киберпреступности подчеркивалась особая значимость проведения дискуссии с участием представителей от бизнес-сообщества и академических кругов и поиска путей разрешения проблем в сфере борьбы с преступным использованием информационно-коммуникационных технологий [5. С. 11].

Примечательно, что в рамках Второго Международного конгресса по кибербезопасности, проходившего 20—21 июня 2019 г. в Москве, экспертному обсуждению подлежали основные мировые киберугрозы, а также методы, способы и средства противодействия [4. С. 15]. Определяющим

направлением в ходе работы форума являлась выработка международной стратегии взаимодействия государств и правоохранительных органов в сфере противодействия киберпреступности. Оценке подлежали ключевые технологические достижения в области защиты современных киберсистем. Было достигнуто понимание актуальности проблемы безопасности в условиях цифрового мироустройства, что предопределило осознание актуальности разработки и реализации комплексных мер противодействия киберпреступности. Признанию подлежал прагматичный подход, требующий научного обоснования вероятных мировых угроз на обозримое будущее. Вследствие этого в целях обеспечения кибербезопасности обозначены задачи по разработке и внедрению эффективных средств прогнозирования, профилактики, предупреждения и противодействия [8. С. 22].

Подводя итог сказанному, следует заключить, что по-прежнему актуальным является принятие универсального международного нормативно-правового акта, позволяющего ориентировать правовую политику государств на правовое регулирование ключевых направлений обеспечения информационной безопасности с учетом присущих каждому государству национальных особенностей [6. С. 17]. Среди стратегических направлений правового регулирования стоит отметить необходимость совершенствования нормативно-правовой базы с учетом обновляющихся киберугроз в условиях развития новых цифровых технологий [7. С. 90]. Требуется формирование правового механизма, содействующего повышению качества и устойчивости элементов государственного управления в отношении финансовой системы. Принятие надлежащих правовых мер становится актуальным для укрепления государственно-частного партнерства, создания и успешной реализации практико-ориентированных программ, обеспечивающих высокий уровень защищенности кредитных организаций. В современных условиях целесообразным представляется формирование кибернетической культуры и повышение грамотности населения путем проведения соответствующих информационно-просветительских мероприятий. Активизации заслуживает деятельность органов правоохранительной системы по выявлению, раскрытию и расследованию компьютерных преступлений, приобретающих в современных реалиях трансграничный характер. Стабильный рост преступлений, предусмотренных гл. 28 УК РФ, предполагает разрешение проблем, сопряженных с имеющимися сложностями при обнаружении, раскрытии, доказывании, установлении виновного, в том числе с точной правовой оценкой реализованного деяния.

Сформулированные положения в сфере повышения качества правового обеспечения информационной безопасности на национальном уровне необходимо подкреплять принятием правовых мер по формированию системы информационной безопасности на межгосударственном и международном уровнях посредством развития взаимовыгодного сотрудничества государств. Следует учитывать, что повышение эффективности мер по обеспечению международной кибербезопасности детерминирует установление единообразного подхода к квалификации совершаемых в области высоких технологий противоправных деяний[1].

В 2015 г. Европейским агентством по сетевой и информационной безопасности (ENISA) определены основные направления обеспечения информационной безопасности «умного города», такие как: безопасность всех типов интеллектуальных сетей, обязательность разработки лучших практик путем организации государственного и частного партнерства для улучшения существующих моделей управления безопасностью умных сетей, в том числе в области облачных вычислений[2].

Одновременно с расширением областей применения информационных технологий возникают и новые информационные угрозы, связанные с достижением террористических, экстремистских, криминальных и иных противоправных целей.

В Доктрине информационной безопасности Российской Федерации, которая представляет собой систему официальных взглядов на обеспечение национальной безопасности в информационной сфере, отмечено, что «информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства». При этом государство призвано обеспечить реализацию таких

[1] Базовые и дополнительные требования к умным городам (стандарт «Умный город»): утв. Минстроем России 04.03.2019 // КонсультантПлюс. [Документ не опубликован].

[2] Annual activity report, 2015 (https://www.enisa.europa.eu/publications/corporate/enisa-annual-activity-report-2015; дата обращения 22.07.2021).

важнейших национальных интересов в информационной сфере, как защита конституционных прав и свобод человека и гражданина при получении и использовании информации, информационная поддержка демократических институтов, механизмов взаимодействия государства и гражданского общества, сохранение культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации, функционирование информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации, развитие информационных технологий и электронной промышленности, доведение до общественности достоверной информации о государственной политике Российской Федерации, содействие формированию системы международной информационной безопасности.

Помимо этого, государство должно обеспечить защиту детей от дестабилизирующего воздействия информационной продукции путем сохранения их психического, психологического здоровья и благополучия, а также формирования позитивного мировосприятия[1].

В связи с этим в качестве важнейшего элемента реализации государственной политики Российской Федерации в области информационной безопасности следует признать уголовно-правовой механизм, включающий в себя нормы о преступлениях в информационно-коммуникационном пространстве.

Учитывая то, что информационные отношения являются дополнительным, а не основным непосредственным объектом преступлений в информационно-коммуникационном пространстве (за исключением преступлений в сфере компьютерной информации), их классификацию целесообразно проводить, традиционно руководствуясь содержанием основного непосредственного объекта.

[1] Концепция информационной безопасности детей: распоряжение Правительства РФ от 02.12.2015 № 2471-р // Собр. законодательства Рос. Федерации. 2015. № 49. Ст. 7055.

Список литературы

1. Авдеев, В. А. Научные и практико-ориентированные основы квалификации преступлений и их модификация в условиях эволюционного детерминизма / В. А. Авдеев // Российский судья. — 2019. — № 16.

2. Волеводз, А. Г. Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран / А. Г. Волеводз // Правовые вопросы связи. — 2004. — № 1.

3. Гриб, В. Г. Факторы, влияющие на борьбу с хищениями и коррупцией, и меры по их устранению / В. Г. Гриб // Российский следователь. — 2015. — № 4.

4. Зинина, У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореф. дис. … канд. юрид. наук / У. В. Зинина. — М., 2007.

5. Кибальник, А. Г. Современное понимание свободы воли в российской уголовно-правовой доктрине / А. Г. Кибальник // Общество и право. — 2017. — № 1 (59).

6. Маякова, А. С. Компьютерные преступления: отдельные вопросы квалификации / А. С. Маякова // Проблемы экономики и юридической практики. — 2017. — № 6.

7. Международные акты о правах человека: сб. док. / сост. В. А. Карташкин, Е. А. Лукашева. — 2-е изд., доп. — М.: Норма, 2002.

8. Сухов А. Н. Организованная преступность и коррупция / А. Н. Сухов // Российский следователь. — 2015. — № 14.

Дата поступления: 20.10.2021
Дата принятия к опубликованию: 25.10.2021

Сведения об авторе

Утарбеков Шамиль Галимович — кандидат юридических наук, доцент кафедры конституционного и муниципального права Института права Челябинского государственного университета, Челябинск, Россия. law@csu.ru

Библиографическое описание: Утарбеков, Ш. Г. Понятие и место информационной безопасности в национальной безопасности России / Ш. Г. Утарбеков // Вестник Челябинского государственного университета. Серия: Право. — 2021. — Т. 6, вып. 3. — С. 34—38. — DOI: 10.47475/2618-8236-2021-16305.

Bulletin of Chelyabinsk State University. Series: Law. 2021. Vol. 6, iss. 3. Pp. 34—38.

The Concept and Place of Information Security in the National Security of Russia

Sh. G. Utarbekov

Chelyabinsk State University, Chelyabinsk, Russia. law@csu.ru

Ensuring national security at the present stage determines the definition of strategic directions that contribute to the protection of the legitimate rights and interests of a person, society and the state from external and internal adverse effects. In conditions of high rates of development of technical and information resources, the problem of optimization of means in the field of information security is being actualized.

Keywords: *information security, computer information, right to information.*

References

1. Avdeev V. A. Nauchnye i praktiko-orientirovannye osnovy kvalifikatcii prestupleniy i ikh modifikatciia v usloviiakh e'voliutcionnogo determinizma [Scientific and practice-oriented bases of qualification of crimes and their modification in the conditions of evolutionary determinism]. *Rossiyskiy sud'ia* [Russian judge], 2019, no. 16. (In Russ.).

2. Volevodz A. G. Ugolovnoe zakonodatel'stvo ob otvetstvennosti za komp'iuternye prestupleniia: opyt raznykh stran [Criminal legislation on responsibility for computer-related crime: the experience of different countries]. *Pravovye voprosy sviazi* [Legal issues of communication], 2004, no. 1. (In Russ.).

3. Grib V. G. Faktory, vliiaiushchie na bor'bu s hishcheniiami i korruptciey, i mery po ikh ustraneniiu [Factors affecting the fight against fraud and corruption, and measures to eliminate them]. R*ossiyskiy sledovatel'* [Russian investigator], 2015, no. 4. (In Russ.).

4. Zinina U. V. *Prestupleniia v sfere komp'iuternoy informatcii v rossiyskom i zarubezhnom ugolovnom prave* [Crimes in the field of computer information in Russian and foreign criminal law. Abstract of thesis]. Moscow, 2007. (In Russ.).

5. Kibalnik A. G. Sovremennoe ponimanie svobody voli v rossiyskoy ugolovno-pravovoy doktrine [Modern understanding of freedom of will in the Russian criminal law doctrine]. *Obshchestvo i pravo* [Society and law], 2017, no. 1 (59). (In Russ.).

6. Mayakova A. S. Komp'iuternye prestupleniia: otdel'nye voprosy kvalifikatcii [Computer crimes: separate issues of qualification]. *Problemy ekonomiki i iuridicheskoy praktiki* [Problems of economics and legal practice], 2017, no. 6. (In Russ.).

7. Kartashkin V. A., Lukasheva E. A. (compil.). *Mezhdunarodnye akty o pravakh cheloveka* [International acts on human rights: a collection of documents]. Moscow, 2002. (In Russ.).

8. Sukhov A. N. Organizovannaia prestupnost' i korruptcii [Organized crime and corruption]. R*ossiyskiy sledovatel'* [Russian investigator], 2015, no. 14. (In Russ.).