УДК 343 **DOI: 10.34670/AR.2022.28.92.017**

Киберпреступность в России: сущность, общественная опасность и методы борьбы

Майстренко Григорий Александрович

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

Аннотация

Современное российское общество живет в информационную эпоху, когда значимые сведения хранятся, перерабатываются и распространяются посредством компьютерных технологий. Общественная опасность последних состоит в том, что они представляют собой реальную угрозу с точки зрения возникновения и развития новых форм преступной активности, реализуемых в онлайн среде. Возможность широкого доступа в социальные сети, всеохватность Интернета открывают возможности для преступников активно осваивать новый мир виртуальной реальности. Это актуализирует на сегодняшний день феномен киберпреступности, возникшей в результате формирования информационного общества. Статья посвящена исследованию сущности киберпреступлений, определению их уровня общественной опасности, а также выявлению методов борьбы с ними. Автор анализирует различные подходы к дефиниции киберпреступности, рассматривает степень ее угрозы обществу, а также определяет основные виды киберпреступлений. Подводя итоги исследования, автора отмечает, что рост киберпреступности в современной России и в мире требует активизации совместных усилий стран по борьбе с данным феноменом. При этом большое значение имеет принятие законов на национальном уровне, способствующих искоренению этого явления. В свою очередь, анализ сущности, причин и видов киберпреступлений является фундаментом, опираясь на который возможно организовать успешную работу по борьбе с ними как на законодательном, так и на правоприменительном уровне.

Для цитирования в научных исследованиях

Майстренко Г.А. Киберпреступность в России: сущность, общественная опасность и методы борьбы // Вопросы российского и международного права. 2022. Том 12. № 1А. С. 181-186. DOI: 10.34670/AR.2022.28.92.017

Ключевые слова

Киберпреступность, Россия, информационное общество, онлайн и оффлайн среда, общественная опасность, компьютерные сети, Интернет, киберэкстремизм, кибертерроризм.

Введение

Современное информационное общество характеризуется повышенной степенью угроз, возникающих в силу того, что жизнедеятельность подавляющей части индивидов протекает, по сути, в двух реальностях – оффлайн и онлайн среды [Рыжов, 2018, 8]. Традиционно внутри реальных экономических, социальных и политических отношений присутствуют процессы, порождающие преступную активность. В свою очередь, информационная среда, в которой отношения между индивидами переходят в онлайн-пространство, не является исключением. Возможность широкого доступа в социальные сети, всеохватность Интернета открывают возможности для преступников активно осваивать новый мир виртуальной реальности.

Это актуализирует на сегодняшний день феномен киберпреступности, возникшей в результате формирования информационного общества [Шинкарецкая, 2020, 56]. Последнее, в свою очередь, предполагает такой этап социально-экономического развития, на котором оно зависит преимущественно от производства, переработки, хранения и дальнейшего распространения информационного контента в социуме [Павловец, 2013, 104].

Современное российское общество невозможно отделить от информации, формирующей повестку дня, предпочтения и вкусы потребителей, обеспечивающей человеку возможность выживать в стремительно меняющемся мире и оперативно приспосабливаться к происходящим изменениям. Информационные технологии в последние годы прочно вошли в повседневный быт человека, реальность которого часто заменяют «умные» устройства и, в первую очередь, компьютер. Его значение как средства выхода в социальные сети, стремительного распространения материалов, а также информационных вбросов активно используется киберпреступниками.

Основная часть

Прежде чем перейти к вопросу о негативной роли, которую оказывает рост киберпреступлений на криминогенную обстановку в Российской Федерации, а также наметить некоторые, потенциально эффективные пути защиты от данного вида преступлений, целесообразно первоначально дефинировать понятие киберпреступности, рассмотреть различные подходы к его определению.

Необходимо отметить, что киберпреступность как явление стала возможной благодаря формированию информационного, или киберпространства. Прогрессивное развитие техники и технологий, с одной стороны, открыло новые возможности для саморазвития, образования, формирования новых профессиональных направлений, с другой – для активизации злоумышленников. Первоначально киберпреступность была следствием недостаточной изученности возможностей сети Интернет. В настоящее время условием для ее расширения является постоянное усложнение информационных технологий, открывающее новые возможности для преступников.

Наиболее емкое определение киберпреступности, позволяющее понять ее суть и свойства, приводит А.В. Федоров. Автор отмечает, что она предполагает совершение противоправных действий в информационном пространстве, созданном при помощи компьютерных технологий, где содержатся важные сведения о лицах, объектах, явлениях и процессах, которые находятся «… в математическом, символьном или в любом другом выражении», и движутся по компьютерной сети локального, либо глобального характера [Федоров, 2006, 111].

Представляет интерес, что А.В. Федоров относит к киберпреступлениям противоправные действия, совершаемые лицом, либо группой лиц, с использованием материалов, хранящихся не только на компьютере, но также и на любом ином носители, при помощи которого можно совершать операции по их виртуальной передаче, хранению и переработке.

С точки зрения В.А. Номоконова, киберпреступность существует не только там, где компьютер выступает в качестве предмета, а информационная безопасность – объекта противоправного деяния, но также и там, где компьютеры применяются в качестве орудий и средств преступлений против собственности, создают угрозу общественной безопасности, нарушения авторских прав [Номоконов, 2003, 105].В свою очередь, Т.М. Хусяинов полагает, что киберпреступность следует определять как Интернет-преступление, либо киберпреступление, в рамках которого необходимо рассматривать весь перечень противоправных деяний, совершаемых в сфере информационных технологий [Хусяинов, 2015, 120].

Все вышеперечисленные определения в широком, либо в узком смысле трактуют феномен киберпреступности. При этом важно не отождествлять понятие киберпреступности и, к примеру, кибербандитизма, компьютерной преступности. Здесь важно принимать во внимание, что с указанными явлениями киберпреступность соотносится как общее с частными проявлениями, так как, по сути, вмещает их в себя.

В наиболее общем виде киберпреступность представляет собой противоправное вмешательство в работу компьютеров, а также в функционирование ряда ее элементов, например, компьютерных сетей, программ, баз данных и проч., а также реализация противозаконных действий посредством компьютеров и элементов, определяющих их работу.

Стремительное распространение киберпреступности актуализирует исследование ее сущности, форм и способов, а также методов борьбы с ней не только в России, но и за рубежом. Это послужило основанием для разработки и утверждения Советом Европы перечня преступных деяний, совершенных с использованием компьютера, которые можно классифицировать как киберпреступления. Государства-члена Совета Европы, подписавшие 23 ноября 2001 г. в Будапеште Конвенцию о компьютерных преступлениях, предусматривали необходимость сплочения и совместной борьбы с ними посредством издания на международном и национальном уровнях законов, призванных сдерживать киберпреступность по целому ряду направлений. К числу таковых, согласно тексту Конвенции, относятся противозаконный доступ к данным, неправомерный перехват компьютерных данных с использованием технических средств, воздействие на данные и на процесс функционирования системы, противозаконное использование устройств, подлог и мошенничество с применением возможностей компьютера, детская порнография, нарушение авторских и смежных прав (ст.ст. 2-10 Конвенции).

Аналогичное регулирование противодействия проявлениям киберпреступности нашло свое правовое оформление и на национальном уровне (гл. 28 УК РФ).

Исходя из содержания определений киберпреступности, действующих как на международном уровне, так и выдвигаемых отечественными учеными, следует отметить расширяющуюся общественную опасность этого явления в силу отсутствия на первоначальном этапе возникновения компьютерных сетей должного контроля со стороны государства за деятельностью в данной сфере. Это привело к формированию преступной активности в сети, в первую очередь, к таким видам преступлений, как похищение конфиденциальной информации, мошенничество с целью получения денежных средств, шпионаж, а также распространение

объектов и услуг, входящих в перечень нелегальных (например, представление сведений относительно наркотической продукции, демонстрация деткой порнографии и т.д.). Как показывает практика, данные действия, ранее реализуемые преступниками в оффлайн пространстве, в настоящее время успешно осуществляются ими при помощи Интернет-технологий. Однако, виртуальный характер площадок, используемых для их совершения, дает реальные результаты. При этом особую опасность сегодня приобретают киберэкстремизм и крайняя форма его проявления – кибертерроризм, иными словами, использование компьютера и компьютерных данных с целью дезорганизации работы информационных систем, что может создать угрозу гибели людей, имущественных потерь, а также наступления иных опасных обстоятельств. Данные действия часто предпринимаются преступниками в целях расшатывания системы общественной безопасности, оказания воздействия на правительство и проч. Кроме того, сегодня распространенным является использование не только конфиденциальной информации, но и пространства социальных сетей в качестве площадок, позволяющих аккумулировать общественное недовольство властью, политическим строем, либо же вектором проводимых страной внутренних и внешних преобразований. Иллюстрацией данного феномена является Евромайдан 2013-2014 гг., а также протестные события 2009 г. в Кишиневе, получившие название «революция Твиттера». Указанные факты подтверждают не только опасность совершения посредством компьютерных технологий преступлений в отношении рядовых граждан, но и возможность их использования как механизма расшатывания системы государственного управления.

Принимая во внимание, что информационно-коммуникационные технологии являются неотъемлемой частью жизни современного общества, необходимо вырабатывать методы борьбы с киберпреступностью.

Несмотря на усложнение компьютерных технологий, одним их наиболее действенных методов является оповещение населения посредством СМИ о новых видах киберпреступлений. Предупреждение о формах и порядке действий преступников является одним из результативных методов, позволяющих оградить граждан от их действий.

Эффективным методом борьбы с киберпреступностью на бытовом уровне является безопасное использование компьютерных материалов, предполагающее ограничение контента, к примеру, для детской аудитории. Это позволит родителям создать условия доступа к глобальной сети в режиме, защищенном от возможного влияния преступности в сфере распространения детской порнографии и наркоторговли.

Наконец, на уровне РФ борьбе с киберпреступностью будет способствовать разработка специальных программ, позволяющих отслеживать подозрительную активность по ряду направлений преступлений с использованием компьютерных технологий, конкретизированных в международных документах и национальных актах.

Заключение

Подводя итоги, следует отметить, что рост киберпреступности в современной России и в мире требует активизации совместных усилий стран по борьбе с данным феноменом. При этом большое значение имеет принятие законов на национальном уровне, способствующих искоренению этого явления. В свою очередь, анализ сущности, причин и видов киберпреступлений является фундаментом, опираясь на который возможно организовать успешную работу по борьбе с ними как на законодательном, так и на правоприменительном уровне.

Библиография

1. Елагина А.С. Подходы к совершенствованию международного уголовного права // Вопросы российского и международного права. 2018. Том 8. № 10А. С. 96-101.
2. Елагина А.С. Интерпретация трендов уровня преступности: нормальные и шоковые изменения // Вопросы российского и международного права. 2018. Том 8. № 11А. С. 144-152.
3. Конвенция о компьютерных преступлениях. Будапешт, 23 ноября 2001 г.
4. Номоконов В.А. Актуальные проблемы борьбы с киберпреступностью // Информационные технологии и безопасность. Киев, 2003. Вып. 3. С. 104-108.
5. Павловец В.И. России нужны не биороботы, а креативный средний класс: о направлениях эффективного реформирования экономики и образования // Альманах современной науки и образования. 2013. № 1 (68). С. 102-105.
6. Рыжов В.Б. Информационная безопасность в государствах Европейского Союза: к постановке проблемы // Представительная власть: XXI век: законодательство, комментарии, проблемы. 2018. № 4 (163). С. 8-12.
7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (посл. ред.).
8. Федоров А.В. Информационная безопасность в мировом политическом процессе. М., 2006. 218 с.
9. Хусяинов Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования. Ижевск, 2015. С. 120-125.
10. Шинкарецкая Г.Г. Сотрудничесиво государств СНГ в борьбе с киберугрозами // Международное сотрудничество евразийских государств: политика, экономика, право. 2020. № 1. С. 55-62.

Cybercrime in Russia: essence, social danger and methods of struggle

Grigorii A. Maistrenko

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

Abstract

Modern Russian society lives in the information age, when significant information is stored, processed and distributed through computer technology. The social danger of the latter lies in the fact that they represent a real threat in terms of the emergence and development of new forms of criminal activity implemented in the online environment. The possibility of wide access to social networks, the ubiquity of the Internet opens up opportunities for criminals to actively explore the new world of virtual reality. This actualizes today the phenomenon of cybercrime that arose as a result of the formation of the information society. The article is devoted to the study of the essence of cybercrime, determining their level of public danger, as well as identifying methods to combat them. The author analyzes various approaches to the definition of cybercrime, considers the degree of its threat to society, and also determines the main types of cybercrime. Summing up the results of the study, the author notes that the growth of cybercrime in modern Russia and in the world requires intensified joint efforts of countries to combat this phenomenon. At the same time, the adoption of laws at the national level that contribute to the eradication of this phenomenon is of great importance. In turn, the analysis of the essence, causes and types of cybercrime is the foundation, based on which it is possible to organize successful work to combat them both at the legislative and law enforcement levels.

For citation

Maistrenko G.A. (2022) Kiberprestupnost' v Rossii: sushchnost', obshchestvennaya opasnost' i metody bor'by [Cybercrime in Russia: essence, social danger and methods of struggle]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 12 (1A), pp. 181-186. DOI: 10.34670/AR.2022.28.92.017

Keywords

Cybercrime, Russia, information society, online and offline environment, public danger, computer networks, Internet, cyber extremism, cyber terrorism.

References

1. Elagina A.S. (2018) Podkhody k sovershenstvovaniyu mezhdunarodnogo ugolovnogo prava [Approaches to the improvement of international criminal law]. Voprosy rossiiskogo i mezhdunarodnogo prava [Matters of Russian and International Law], 8 (10A), pp. 96-101.
2. Elagina A.S. (2018) Interpretatsiya trendov urovnya prestupnosti: normal'nye i shokovye izmeneniya [Interpretation of crime trends: normal and shock changes]. Voprosy rossiiskogo i mezhdunarodnogo prava [Matters of Russian and International Law], 8 (11A), pp. 144-152.
3. Fedorov A.V. (2006) *Informatsionnaya bezopasnost' v mirovom politicheskom protsesse* [Information security in the global political process]. Moscow.
4. Khusyainov T.M. (2015) Internet-prestupleniya (kiberprestupleniya) v rossiiskom ugolovnom zakonodatel'stve [Internet crimes (cybercrimes) in Russian criminal law]. In: *Ugolovnyi zakon Rossiiskoi Federatsii: problemy pravoprimeneniya i perspektivy sovershenstvovaniya* [Criminal law of the Russian Federation: problems of law enforcement and prospects for improvement]. Izhevsk.
5. *Konventsiya o komp'yuternykh prestupleniyakh. Budapesht, 23 noyabrya 2001 g.* [Computer Crime Convention. Budapest, November 23, 2001].
6. Nomokonov V.A. (2003) Aktual'nye problemy bor'by s kiberprestupnost'yu [Actual problems of combating cybercrime]. In: *Informatsionnye tekhnologii i bezopasnost'* [Information technologies and security]. Kiev. Is. 3.
7. Pavlovets V.I. (2013) Rossii nuzhny ne bioroboty, a kreativnyi srednii klass: o napravleniyakh effektivnogo reformirovaniya ekonomiki i obrazovaniya []. *Al'manakh sovremennoi nauki i obrazovaniya* [Almanac of modern science and education], 1 (68), pp. 102-105.
8. Ryzhov V.B. (2018) Informatsionnaya bezopasnost' v gosudarstvakh Evropeiskogo Soyuza: k postanovke problemy [Information security in the states of the European Union: to the formulation of the problem]. *Predstavitel'naya vlast': XXI vek: zakonodatel'stvo, kommentarii, problemy* [Representative power: XXI century: legislation, comments, problems]. 2018. № 4 (163). S. 8-12.
9. Shinkaretskaya G.G. (2020) Sotrudnichesivo gosudarstv SNG v bor'be s kiberugrozami [Cooperation of the CIS states in the fight against cyber threats]. *Mezhdunarodnoe sotrudnichestvo evraziiskikh gosudarstv: politika, ekonomika, pravo* [International cooperation of the Eurasian states: politics, economics, law], 1, pp. 55-62.
10. *Ugolovnyi kodeks Rossiiskoi Federatsii ot 13.06.1996 № 63-FZ (posl. red.)* [Criminal Code of the Russian Federation No. 63-FZ dated June 13, 1996 (last edition)].