УДК 34 **DOI: 10.34670/AR.2022.99.72.015**

Государственная политика в сфере борьбы с киберпреступностью: российский и зарубежный опыт

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

Актуальность данной статьи обусловлена тем, что становление информационного общества имеет как несомненные положительные, так и определенные негативные последствия. С одной стороны, ускорилась передача информации большого объема, ускорились ее обработка и внедрение новых технологий. С другой, серьезное беспокойство вызывает распространение фактов противозаконного сбора и использования информации, несанкционированного доступа к информационным ресурсам и прочих проявлений киберпреступности. В статье проанализированы аспекты правового регулирования борьбы с киберпреступностью как в Российской Федерации, так и в зарубежных странах. Исследованы особенности преступлений в сфере информационно-телекоммуникационных технологий, обращено внимание на основные проблемы по их выявлению, раскрытию и расследованию. Раскрыты направления международного взаимодействия в сфере противодействия киберпреступности, базирующиеся на международных нормативно-правовых актах. Освещен определенный зарубежный опыт организации деятельности подразделений полиции и нормативного регулирования в указанной сфере. Отмечена необходимость изучения опыта зарубежных стран по организации деятельности подразделений борьбы с киберпреступностью. Выделены направления 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.

Для цитирования в научных исследованиях

Майстренко Г.А. Государственная политика в сфере борьбы с киберпреступностью: российский и зарубежный опыт // Теории и проблемы политических исследований. 2022. Том 11. № 5А. С. 131-138. DOI: 10.34670/AR.2022.99.72.015

Ключевые слова

Борьба с киберпреступностью, информатизация общества, информационно-телекоммуникационные технологии, хакерство, государственная политика.

Введение

Актуальность данной статьи обусловлена тем, что становление информационного общества имеет как несомненные положительные, так и определенные негативные последствия. С одной стороны, ускорилась передача информации большого объема, ускорились ее обработка и внедрение новых технологий. С другой, серьезное беспокойство вызывает распространение фактов противозаконного сбора и использования информации, несанкционированного доступа к информационным ресурсам, незаконного копирования информации в электронных системах, хищение информации из библиотек, архивов, банков и баз данных, нарушение технологий обработки информации, запуск программ-вирусов, уничтожение и модификация данных в информационных системах, перехват информации в технических каналах ее утечки, манипулирование общественным и индивидуальным сознанием и т.п. Как отмечают представители экспертного сообщества, XX1 век – век информации и информационных технологий, и жители Планеты все чаще испытывают на себе негативное воздействие эпистемологических войн [Рыжов, 2018, 8]. К примеру, все примеры манипулирования общественным сознанием мы можем наблюдать на Украине, когда украинский народ верит в любую, даже самую нелепую информацию, которую им предоставляют украинские СМИ, которые полностью подконтрольны государству и западным спецслужбам.

Основная часть

Преобразование индустриального общества в информационное изменило статус информации. На сегодня она может быть как средством обеспечения безопасности, так и угрозой, и опасностью [Овчинский, 2017, 311].

Более того, процесс установки системы эффективного правового регулирования борьбы с киберпреступностью невозможна без учета достижений и ошибок, допущенных иностранными государствами при формировании этого института.

В настоящее время развитие правового регулирования противодействия киберпреступности в Российской Федерации находится на активном этапе. Во многих зарубежных странах эта система работает давно и дала положительные результаты, хотя киберпреступность все еще опережает уровень развития инструментов противодействия ей. Поэтому, анализируя современные российские реалии, мы можем отметить незавершенность этого процесса на сегодняшний день и необходимость дальнейших трансформаций. При таких условиях актуальными становятся вопросы положительного и отрицательного опыта других государств, что является очень соответствующим вектором развития научно-исследовательского института.

Бесспорно, на современном этапе развития человеческого общества важным стратегическим ресурсом, который нуждается в охране, является информация, она содержит чрезвычайно широкий спектр сведений: от простых данных о гражданах страны до информации о стратегических государственных программах. Поэтому эти данные все чаще становятся предметом преступных посягательств. Комплексное и широкомасштабное использование

информационных технологий на основе персональных компьютеров, информационно-вычислительных сетей и компьютеризированных коммуникационных систем обеспечило человечеству выход на новый этап своего развития – этап информационного общества. Как следствие – появление нового вида преступности – компьютерной, или киберпреступности. Для современного общества (в период его перехода от индустриального этапа развития к новому – постиндустриальному, информационному) актуальность этой проблемы не вызывает сомнений.

По разным экспертным оценкам во всем мире ущерб от деятельности киберпреступников составляют ежегодно от 400 до 1000 млрд. долларов [Смирнова, 2016, 243]. На международном уровне в ряде нормативно-правовых актов признано, что киберпреступность угрожает не только национальной безопасности отдельных стран, но и безопасности человечества и международного правопорядка. Стратегия государственных подходов и механизмов по улучшению информационных систем должна способствовать сокращению масштабов киберпреступности и создать основные принципы национальной политики противодействия киберпреступности в международном киберпространстве. Противодействие киберпреступности в широком понимании включает в себя общегосударственные меры экономического, политического, воспитательного и иного характера, а также комплекс специальных мероприятий, направленных на непосредственное преодоление преступности. Учитывая международный характер киберпреступности, в борьбе с ней жизненно важное значение имеет гармонизация национальных законодательств. Тем не менее, гармонизация должна учитывать региональные требования и возможности. Большое значение региональных аспектов в осуществлении стратегий борьбы с киберпреступностью подчеркивает тот факт, что многие правовые и технические стандарты были согласованы между различными странами. Глобальная программа кибербезопасности основана на пяти основных принципах: 1) юридические меры; 2) технические и процедурные меры; 3) организационные структуры; 4) создание потенциала; 5) международное сотрудничество. Отечественная система государственных механизмов борьбы с киберпреступностью также использует эти принципы [Пузырева, Мысина, 2020, 45].

Среди пяти принципов при рассмотрении стратегии борьбы с киберпреступностью, вероятно, правовые меры являются наиболее важными. Во-первых, эти меры требуют принятия основных положений уголовного законодательства, предусматривающих уголовную ответственность за такие действия, как компьютерное мошенничество, незаконный доступ, искажение данных, нарушение авторских прав, распространение детской порнографии и тому подобное. Механизмы и инструменты, необходимые для расследования киберпреступлений, могут существенно отличаться от тех, что используются для расследования общих преступлений.

Эффективная борьба с киберпреступностью требует развитой организационной структуры. Не имея правильно созданной системы соответствующих органов, которая позволяет избежать дублирования и четко распределяет полномочия, вряд ли можно ожидать комплексное решение юридических, технических и социальных аспектов данной проблемы. Киберпреступность является глобальным явлением. Для того чтобы иметь возможность эффективно расследовать киберпреступления, необходимо не только гармонизировать законодательство, но и разработать соответствующие механизмы международного сотрудничества. Уровень доверия должен возрасти не только между государствами, но и между частным и государственным секторами.

Правовая система Российского государства в части борьбы с киберпреступностью в основном основана на следующих нормативно-правовых актах: Конституция Российской

Федерации; Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (от 02.07.2021 N 331-ФЗ) [4]; Федеральный закон «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» от 01.10.2008 № 164-ФЗ. Данные нормативно-правовые акты требуют ежегодного совершенствования и внесения в них изменений с учетом отечественной практики их применения и зарубежного опыта. Тогда система борьбы с киберпреступлениями будет эффективной, а методы противодействия современными.

Рассматривая вопросы противодействия киберпреступности, целесообразно присоединиться к тем ученым-криминологам, которые выделяют общесоциальные, специально-криминологические и индивидуальные направления противодействия. Противодействие киберпреступности на общесоциальном уровне (направлении) предусматривает комплекс перспективных социально-экономических механизмов и мер [Дремлюга, 2022, 128].

Одним из наиболее важных элементов в предупреждении киберпреступлений является обучение пользователя. Некоторые киберпреступления, особенно те, которые связаны с мошенничеством типа «спуфинг» (в контексте сетевой безопасности spoofing attack (англ. spoofing – подмена) – ситуация, в которой один человек или программа успешно маскируется под другую путем фальсификации данных и позволяет получить незаконные преимущества), как правило, обусловлены не отсутствием средств технической защиты, а неосведомленностью или простой безответственностью. Существуют различные программные продукты, позволяющие автоматически определять некоторые мошеннические веб-сайты, хотя, к сожалению, не все. Несмотря на то, что средства технической защиты будут продолжать развиваться и доступные программные продукты регулярно обновляться, такие продукты пока еще не могут заменить другие подходы. Стратегия защиты пользователя, основанная только на программных продуктах, еще не дает гарантии полной защиты пользователей [Пузырева, Мысина, 2020, 34].

Важную роль играет также беспрекословное соблюдение установленных правил и процедур информационной безопасности. Например, если пользователи знают, что их финансовые учреждения никогда не будут связываться с ними по электронной почте с просьбой сообщить пароль или детали банковского счета, они не станут жертвами фишинга или атак с целью кражи идентификации. Обучение пользователей Интернета сокращает количество потенциальных жертв киберинцидентов. Государство должно разработать соответствующую информационную программу разумного поведения по предупреждению киберпреступности. К ее распространению следует приобщить общественные кампании, школы, информационные центры и ВУЗы, реализуя частно-государственное партнерство.

Киберпреступность – по своей природе трансграничное явление, позволяющее большинству ученых указывать на то, что для киберпреступлений характерен максимальный уровень латентности. Факторами латентности преступлений выступают следующие: 1) сложность механизма совершения киберпреступлений, совмещенная с очень разнообразными сферой и последствиями их совершения, а также «компьютерная безграмотность» большинства потенциальных жертв киберпреступлений, их пренебрежение своей безопасностью; 2) негативное поведение жертв (очевидцев) преступления – не обращение жертвы и лиц, которым известно о преступлении, в правоохранительные органы и несообщение о факте совершения киберпреступления; 3) недостатки в работе правоохранительных органов в отношении реагирования на обращения и сообщения о киберпреступлениях [Смирнова, 2016, 117].

Масштабность Интернета указывает на то, что определенные элементы киберпреступности не могут быть ограничены только территорией определенной страны, поэтому в любом случае

национальное законодательство должно соответствовать общепризнанным стандартам в этой области, чтобы иметь возможность продолжать международное сотрудничество.

Так, в сфере активной борьбы с киберпреступностью 14 февраля 2008 г. была принята французская стратегия борьбы с киберпреступностью. киберпреступность. Интересным моментом стратегии является курс на установление сотрудничества между провайдерами и полицией и жандармерией, и создание Национальной комиссии по вопросам профессиональной этики в связях с общественностью [Простосердов, 2017, 93]. Особенно целесообразным является последнее направление. Любое ограничение прав и свобод граждан требует должного разъяснения и двустороннего конструктивного диалога с гражданами. Здесь важно обратить внимание на запуск веб-сайта Charte de'Internet, который определяет принципы добровольных обязательств пользователей и Интернет-провайдеров. Еще одна подобная тенденция – создание интернет-ресурса Mineurs.org, который предоставляет информацию о проектах в сфере безопасного использования киберсетей. То есть заключение международных соглашений во Франции предусматривает возможность разрешения на удаленный поиск информационных ресурсов без получения предварительного разрешения страны, где размещается сервер. В этой работе перспективы развития правового регулирования борьбы с киберпреступностью объясняются потенциальной потребностью отмены государственных границ в вопросах киберпреступности. Для воплощения этого направления в России целесообразно изучить опыт Франции, поскольку возможность такого «свободного» сотрудничества не предусмотрена действующим законодательством.

Таким образом, особенностями правового регулирования борьбы с киберпреступностью во Франции являются: 1) существенная роль государства в регулировании общественных отношений в Интернете; 2) контроль над пользователями путем установления требования об авторизации авторов веб-сайтов; 3) налаживание сотрудничества между правоохранительными органами и Интернет-провайдерами с целью оперативного реагирования на появление угроз; 4) наличие двустороннего диалога с гражданами и надлежащее разъяснение их прав и обязанностей как пользователей Интернета, предоставление инструкций; 5) установление курса на свободное сотрудничество с другими странами путем предоставления доступа к собственным киберсетям в случае совершения киберпреступности во Франции.

Рассмотрим опыт Республики Беларусь, как одной из первых стран бывшего СССР, в которой был создан специальный орган для борьбы с киберпреступностью – управления по раскрытию преступлений в сфере высоких технологий Министерства внутренних дел Республики Беларусь. 27 февраля 2001 года в структуре криминальной милиции МВД появилось управление оперативно-организационной работы, в составе которого до ноября 2002 года активно действовало специализированное отделение по раскрытию преступлений в сфере высоких технологий, а уже 28 ноября 2002 года на основании приказа Министра внутренних дел, с целью совершенствования организации работы указанных подразделений, в МВД было создано самостоятельное управление, которое осуществляет практическую деятельность по раскрытию преступлений в сфере высоких технологий. Данный орган имеет статус самостоятельного оперативно-розыскного подразделения Министерства, осуществляющего координацию подразделений главного управления криминальной милиции МВД и органов внутренних дел при выявлении ими преступлений против информационной безопасности. Для осуществления взаимодействия с другими правоохранительными органами и организациями применяется условное наименование Управления «К» МВД Республики Беларусь [Овчинский, 2017, 438].

Анализируя законодательную базу борьбы с киберпреступности в Беларуси, которая представлена незначительным количеством норм и законов: одна глава в Уголовном кодексе Республики Беларусь, Закон о электросвязь, Закон об информации, информатизации и защите информации, Конвенция о киберпреступлениях, Дополнительный протокол к Конвенции о киберпреступлениях, Указ «О мерах по совершенствованию использования национального сегмента сети Интернет», Указ «О некоторых вопросах развития информационного общества в Республике Беларусь», Указ «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, проводящими оперативно-розыскную деятельность». В целом отмечаем тождество законодательной базы Республики Беларусь и Российской Федерации, однако есть один отличительный нормативно-правовой акт «Концепция информационной безопасности Республики Беларусь».

Заключение

Итак, анализируя модели правового регулирования борьбы с киберпреступностью, нами установлена тенденция к попыткам установления контроля за всемирной сетью, однако имеющиеся запреты все же не содержат признаков существенного нарушения прав и свобод человека и гражданина. В изучаемых государствах существует двусторонний диалог власти и граждан, благодаря которому в обществе формируется верное понимание необходимости установления ограничений, запретов или регламентов. В то же время мы обратили внимание на незначительное количество нормативно-правовых актов, которые при этом должным образом урегулируют данный институт, то есть в них преобладает саморегулирование сферы кибербезопасности. Также целесообразно отметить роль международного законодательства и межгосударственных соглашений, которые значительным образом имеют влияние на общественные отношения внутри государств. Очевидно, что их роль в отечественном праве необходима и выводить борьбу с киберпреступностью на новый уровень.

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. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.).
3. Конвенция против транснациональной организованной преступности (принята в г. Нью-Йорке 15.11.2000 Резолюцией 55/25 на 62-ом пленарном заседании 55-ой сессии Генеральной Ассамблеи ООН) (с изм. от 15.11.2000).
4. Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 (в ред. от 01.07.2020).
5. Овчинский В.С. (сост.) Основы борьбы с киберпреступностью и кибертерроризмом. М.: Норма, 2017. 527 с.
6. Постановление Совета безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь».
7. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве. М.: Юрлитинформ, 2017. 167 с.
8. Пузырева Ю.В., Мысина А.И. Международное полицейское сотрудничество по вопросам раскрытия и расследования преступлений в сфере информационных технологий. М.: ИНФРА-М, 2020. 92 с.
9. Рыжов В.Б. Информационная безопасность в государствах Европейского союза: к постановке проблемы // Представительная власть – XX1 век. 2018. № 4. С. 8-12.
10. Смирнова И.Г. (ред.) Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ. М.: Юрлитинформ, 2016. 306 с.
11. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (от 02.07.2021 № 331-ФЗ).
12. Федеральный закон «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» от 01.10.2008 № 164-ФЗ.

State policy in the field of combating cybercrime: Russian and foreign experience

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

The relevance of this article is due to the fact that the formation of the information society has both undoubted positive and certain negative consequences. On the one hand, the transfer of large-volume information has accelerated, its processing and the introduction of new technologies have accelerated. On the other hand, the spread of facts of illegal collection and use of information, unauthorized access to information resources and other manifestations of cybercrime causes serious concern. The article analyzes aspects of the legal regulation of the fight against cybercrime both in the Russian Federation and in foreign countries. The features of crimes in the field of information and telecommunication technologies are studied, attention is drawn to the main problems in their identification, disclosure and investigation. The directions of international cooperation in the field of combating cybercrime, based on international legal acts, are revealed. A certain foreign experience in organizing the activities of police units and normative regulation in this area is highlighted. The need to study the experience of foreign countries in organizing the activities of units to combat cybercrime is noted. The areas of interaction between the operational units of the internal affairs for the purpose of promptly documenting crimes in the field of information and telecommunication technologies and the types of cooperation between the internal affairs bodies and law enforcement agencies of other states are highlighted.

For citation

Maistrenko G.A. (2022) Gosudarstvennaya politika v sfere bor'by s kiberprestupnost'yu: rossiiskii i zarubezhnyi opyt [State policy in the field of combating cybercrime: Russian and foreign experience]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 11 (5A), pp. 131-138. DOI: 10.34670/AR.2022.99.72.015

Keywords

Fight against cybercrime, informatization of society, information and telecommunication technologies, hacking, public policy.

References

1. Dremlyuga R.I. (2022) Ugolovno-pravovaya okhrana tsifrovoi ekonomiki i informatsionnogo obshchestva ot kiberprestupnykh posyagatel'stv: doktrina, zakon, pravoprimenenie [Criminal legal protection of the digital economy and the information society from cybercriminal attacks: doctrine, law, and law enforcement]. Moscow: Yurlitinform Publ.
2. Federal'nyi zakon «O personal'nykh dannykh» ot 27.07.2006 № 152-FZ (ot 02.07.2021 № 331-FZ) [Federal Law “On Personal Data” No. 152-FZ dated July 27, 2006 (No. 331-FZ dated July 2, 2021)].

3. Federal'nyi zakon «O ratifikatsii Soglasheniya o sotrudnichestve gosudarstv – uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v bor'be s prestupleniyami v sfere komp'yuternoi informatsii» ot 01.10.2008 № 164-FZ [Federal Law No. 164-FZ dated 01.10.2008 "On Ratification of the Agreement on Cooperation between the Member States of the Commonwealth of Independent States in Combating Crimes in the Sphere of Computer Information"].
4. Konventsiya o prestupnosti v sfere komp'yuternoi informatsii ETS N 185 (Budapesht, 23 noyabrya 2001 g.) [Computer Crime Convention ETS N 185 (Budapest, November 23, 2001)].
5. Konventsiya protiv transnatsional'noi organizovannoi prestupnosti (prinyata v g. N'yu-Iorke 15.11.2000 Rezolyutsiei 55/25 na 62-om plenarnom zasedanii 55-oi sessii General'noi Assamblei OON) (s izm. ot 15.11.2000) [Convention against Transnational Organized Crime (adopted in New York on November 15, 2000 by Resolution 55/25 at the 62nd plenary meeting of the 55th session of the UN General Assembly) (as amended on November 15, 2000)].
6. Konstitutsiya Rossiiskoi Federatsii. Prinyata vsenarodnym golosovaniem 12.12.1993 (v red. ot 01.07.2020) [The Constitution of the Russian Federation. Adopted by popular vote on December 12, 1993 (as amended on July 1, 2020)].
7. Ovchinskii V.S. (comp.) Osnovy bor'by s kiberprestupnost'yu i kiberterrorizmom [Fundamentals of combating cybercrime and cyberterrorism]. Moscow: Norma Publ.
8. Postanovlenie Soveta bezopasnosti Respubliki Belarus' ot 18 marta 2019 g. № 1 «O Kontseptsii informatsionnoi bezopasnosti Respubliki Belarus'» [Resolution of the Security Council of the Republic of Belarus dated March 18, 2019 No. 1 "On the Concept of Information Security of the Republic of Belarus"].
9. Prostoserdov M.A. (2017) Ekonomicheskie prestupleniya, sovershaemye v kiberprostranstve [Economic crimes committed in cyberspace]. Moscow: Yurlitinform Publ.
10. Puzyreva Yu.V., Mysina A.I. (2020) Mezhdunarodnoe politseiskoe sotrudnichestvo po voprosam raskrytiya i rassledovaniya prestuplenii v sfere informatsionnykh tekhnologii [International police cooperation on the disclosure and investigation of crimes in the field of information technology]. Moscow: INFRA-M Publ.
11. 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 [Representative power in the XXI century], 4, pp. 8-12.
12. Smirnova I.G. (ed.) (2016) Kiberprestupnost': kriminologicheskii, ugolovno-pravovoi, ugolovno-protsessual'nyi i kriminalisticheskii analiz [Cybercrime: criminological, criminal law, criminal procedure and forensic analysis]. Moscow: Yurlitinform Publ.