УДК 343.1
DOI: 10.18384/2310-7227-2021-1-95-101

КИБЕРПРЕСТУПНОСТЬ КАК СОЦИАЛЬНАЯ УГРОЗА И ОБЪЕКТ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Тимофеев А. В.[1], Комолов А. А.[2]
[1] Самарский государственный технический университет
443090, г. Самара, ул. Молодогвардейская, д. 244, Российская Федерация
[2] Самарский государственный университет путей сообщения
443066, г. Самара, ул. Свободы, д. 2В, Российская Федерация

Аннотация
Цель. Проанализировать феномен киберпреступности как угрозу безопасности общества и объект нормативно-правового регулирования, обозначить меры проведения эффективной политики по борьбе с киберпреступлениями.
Процедура и методы. Основное содержание исследования составляет анализ причин возникновения и роста киберпреступности в XXI в.; рассматриваются разновидности киберпреступлений и их эволюция; объясняются сложности противодействия им; получает осмысление российский и международный опыт предотвращения киберпреступлений, зафиксированный в соответствующих нормативно-правовых документах; отмечается роль цифровых технологий в проведении наиболее эффективной политики в сфере противодействия киберугрозам.
Результаты. Проведённый анализ показал, что киберпреступность представляет серьёзную угрозу современному обществу и его информационной безопасности. Для проведения эффективной политики в сфере борьбы с киберпреступлениями рекомендованы привлечение и совершенствование цифровых технологий (блокчейн, искусственный интеллект), ужесточение ответственности за совершение киберпреступлений и целенаправленная борьба с кибертерроризмом.
Теоретическая и/или практическая значимость исследования обусловлена его сопряжённостью с новым, не существовавшим вплоть до XXI в. видом преступности – киберпреступностью. Киберпреступность является проблемой личной и социальной, внутригосударственной и международной. Вопросы совершения и раскрытия преступлений в информационной среде требуют пристального внимания и незамедлительного реагирования.

Ключевые слова: киберпреступление, информационные технологии, информационная безопасность, кибертерроризм, хакерская атака, блокчейн, искусственный интеллект

CYBERCRIME AS A SOCIAL THREAT AND AN OBJECT OF LEGAL REGULATION

A. Timofeev[1], A. Komolov[2]
[1]Samara State Technical University
244, Molodogvardeyskaya ul., Samara 443100, Russian Federation
[2]Samara State Transport University
2B Svobody ul., Samara 443066, Russian Federation

Abstract
Aim. To analyze the phenomenon of cybercrime as a threat to the security of the society and an object regulated by legal norms, to identify measures to implement an effective policy to fight cybercrimes.
Methodology. The main content of the research is the analysis of the reasons for the growth of cybercrimes in the XXI century; the types of cybercrimes and their evolution are considered; the difficulties of fighting them are explained; Russian and international experience in cybercrimes' preventing, fixed

in the relevant legal norms is given purport; the role of digital technologies in implementing the most effective policy in the field of counteracting cyber threats is noted.

Results. The analysis showed the cybercrime as a serious threat to modern society and its information security. To implement an effective policy in the field of fighting cybercrimes, it's recommended to attract and improve digital technologies (blockchain, artificial intelligence), increase responsibility for committing cybercrimes and fight cyberterrorism purposefully.

Research implications. The theoretical / practical importance of the study is due to its connection with a new type of crime that hasn't existed until the XXI century – cybercrime. Cybercrime is both a personal and social, state and international problem. The questions of committing and solving crimes in the information field require close attention and immediate reaction.

Keywords: cybercrime, information technology, information security, cyberterrorism, hacker attack, blockchain, artificial intelligence

Введение

В эпоху цифровизации система социального взаимодействия основана на использовании интернета. Согласно отчету Dijital 2020, в течение 2020 г. данной сетью пользовалось 4,54 млрд человек, что составляет 59% пользователей всего мирового сообщества [11]. Интернет делает более доступными общение и коммуникацию, способствует развитию самых разных сфер деятельности человека [10, с. 1043]. Однако данное информационное пространство стало также полем для преступных деяний. В XXI в. человечество впервые столкнулось с новым, ранее неизвестным видом преступности – киберпреступностью.

Киберпреступность основывается на взломе интернет-страниц, распространении вредоносных программ и противоправной информации людьми, осуществляющими преступную деятельность в виртуальном пространстве с помощью информационных технологий. Немаловажную роль для осуществления подобного рода противозаконной деятельности играет компьютер. Он является техническим средством, инструментом, позволяющим злоумышленникам не только похищать информацию, уничтожать или повреждать её, но и размещать вредоносные сайты, на которых содержатся компьютерные вирусы.

Данный вид преступления, как, впрочем, и все другие, таит в себе угрозу информационной безопасности общества. Помимо кражи денежных средств с банковских карт киберпреступники научились похищать персональные данные человека, что может нанести непоправимый урон его репутации в случае опубликования этой информации в сети. Киберпреступность является проблемой не только каждого отдельного взятого интернет-пользователя, – её следует рассматривать в более широком, социальном и даже международном ключе. От роста киберпреступности страдают не только физические, но и юридические лица; жертвами хакерских атак в нашей современности становятся целые страны, государства.

Вопросы совершения и раскрытия преступлений в информационной среде требуют пристального внимания и незамедлительного реагирования, подтверждением чему являются неутешительные статистические данные. Так, в России, начиная с 2013 г., количество нарушений, связанных с применением современных технических устройств, было около 11 тыс., а в 2016 году – уже 66 тыс. Если брать данные в мире, за 2017 г. было похищено около $1,2 млрд в криптовалюте [4, с. 383].

Разновидности киберпреступлений

Серьёзный шаг, направленный на борьбу с киберпреступностью, был сделан 23 ноября 2001 г. В Будапеште была принята подписанная членами Совета Европы Конвенция о преступности в сфере компьютерной информации. По сути, данная Конвенция, действующая на национальном уровне, стала первым документом,

закрепившим необходимость правового преследования киберпреступных деяний. В ней упоминалось четыре основных вида киберпреступности: незаконный доступ, незаконный перехват, вмешательство в данные, вмешательство в систему. Однако за 20 прошедших лет киберпреступность совершенствовалась, и в нашей современности существует множество её разновидностей, таких как фишинг, фарминг, киберторговля наркотиками, кибертерроризм, социальное хакерство (пиратство) и мн. др.

Фишинг – один из самых распространённых видов кибермошенничества, основанный на выявлении и изъятии у человека его персональных данных для доступа к банковским счетам, осуществляемых обманным путём. Чаще всего хакеры присылают пользователям файл или ссылку, содержащие вредоносные шифры. При переходе по таким ресурсам осуществляется считывание данных, взламывается банковский счёт и происходит снятие с него денег.

Фарминг – вид киберпреступлений, направленный на удалённое взламывание компьютера. Благодаря этому хакер получает к нему полный доступ: он может редактировать документы, наблюдать за пользователем компьютера с помощью аудио- и видеонаблюдения, вводить разные вредоносные программы, собирать информацию о пользователе. Главная особенность этого киберпреступления в том, что пострадавший даже не будет догадываться, что в данный момент с его компьютером производятся подобного рода манипуляции.

Киберторговля наркотиками также осуществляется с помощью информационных технологий. С их помощью до клиента доводятся зашифрованные координаты местонахождения товара, осуществляется оплаты за «товар».

Кибертерроризм предполагает осуществление террористических действий с использованием и через посредство информационных технологий. К таким действиям относятся распространение информации о терактах, которые планируются к совершению в будущем, а также призывы к осуществлению террористических действий.

Социальное хакерство, или пиратство представляет собой нелегальный доступ к информационной системе. Хакеры используют различные приёмы, основанные на психическом воздействии на человека с целью получения от него нужной информации. Воздействовать на человеческую психологию неизмеримо проще, чем взламывать компьютерную систему, после чего задачей хакеров становится установление вредоносной программы для управления компьютером жертвы. Далее усилия направляются на то, чтобы вредоносные программы как можно дольше оставались необнаруженными.

Рост киберпреступности и сложности борьбы с ней

С каждым днём киберпреступления получают всё большую распространённость, – их количество увеличивается экспоненциально. Возникает всё больше новых видов преступлений, к каждому из которых требуется подбирать соответствующие методы борьбы, что вызывает известные трудности. Поймать кибермошенника гораздо сложнее, чем обычного преступника.

Борьба с киберпреступностью осложняется целым рядом факторов:

1. Киберпреступники – это не обычные мошенники, а хорошо обученные программисты, которые скрываются за экраном своего компьютера. Такую личность вычислить гораздо сложнее, чем обычного преступника.

2. Сталкиваясь с киберпреступлениями, сотрудники правоохранительных органов нуждаются в помощи высококвалифицированных специалистов в сфере программирования, в которых по-прежнему испытывается нехватка.

3. Немало трудностей возникает и с определением самого факта совершения данного преступления. Ввиду отсутствия возможности проведения квалифицированной экспертизы, зачастую бывает сложно доказать, что за то или иное действие предусмотрено наказание по ст. 273 УК РФ [2, с. 72].

4. Достаточно трудно осуществлять контроль за уже существующими, постоянно обновляющимися и вновь возникающими видами киберпреступности.

Наука, занимающаяся целенаправленным изучением киберпреступлений, – киберкриминология – находится пока на стадии формирования.

Сегодня в Российской Федерации активно разрабатываются и осуществляются меры, направленные на борьбу с киберпреступностью. Данные меры, в основном, опираются на опыт европейских стран. Постепенно повышается информированность населения о таком виде преступных действий, как киберпреступность, совершенствуется применяемое в этой сфере правовое регулирование. Особое внимание уделяется разработке и совершенствованию нормативно-правовых актов о киберпреступности. Так, например, в гл. 28 УК РФ преступления, совершаемые с помощью вирусных программ и средств, не выделены как-то отдельно, а статистические отчёты, разумеется, не могут помочь в выявлении уровня и установлении состава киберпреступления.

Если рассматривать опыт международных договоров, принятых в сфере противодействия киберпреступности, все они требуют определённой доработки. Примером может служить ст. 51 Устава ООН, в которой требуется выделить пункты, определяющие проявление кибератак, а также возможность выявления того, с помощью каких информационных технологий такая атака было проведена.

Правовое регулирование киберпреступности

В сфере правового регулирования киберпреступности отдельного внимания заслуживает проект конвенции ООН «О сотрудничестве в сфере противодействия информационной преступности», созданный российскими разработчиками. В нём представлены цели, заключающиеся в профилактике выявления правонарушений в информационной сфере на ранних стадиях, обеспечение наказуемости данных нарушений, непосредственное сотрудничество стран в решении подобных вопросов, заключающееся в создании и развитии кадров и оказания помощи друг другу (ст. 1).

В данной конвенции подробно раскрываются многие специфичные информационные термины. Например, «бот-сеть» означает два и более устройств ИКТ, в модуль которых скачаны вирусные программы, управление которыми производится тайно. Установлена также ответственность за незаконное получение информации в электронной форме (гл. 2), описываются действия, связанные с раскрытием лиц, подозреваемых в данном нарушении (ст. 48). Для эффективности борьбы с подобными инцидентами, в ст. 57 Конвенции каждому государству предлагается сформировать информационный центр, который будет работать круглосуточно.

Анализируя данную Конвенцию, следует отметить, что в ней собрано значительное количество сведений, благодаря которым можно усовершенствовать меры по борьбе с киберпреступностью. В ней: представлена конкретная программа по осуществлению обучения квалифицированных специалистов, занимающихся осуществлением информационной безопасности; акцентируется внимание на необходимости проведения всеми странами единой политики в борьбе с киберпреступностью и активной взаимопомощи. Исходя из совокупности всех этих факторов, данный проект переведён с русского на многие языки и в электронной форме был официально опубликован на официальных сайтах ООН и МИД России.

К сожалению, против этого проекта выступили представители незначительного числа делегаций, приводившие в качестве главного контраргумента отсутствие необходимости внесения дополнительных изменений в Конвенцию, принятую в Будапеште в 2001 г. По их мнению, представленных в ней положений достаточно, чтобы разрешать все имеющиеся в информационной сфере вопросы. По-видимому, такая неоднозначная реакция обусловлена тем, что не все страны ООН имеют желание проектировать долгосрочный алгоритм сотрудничества в решении вопросов борьбы с киберпреступностью. Вследствие этого российский проект не получил должного уровня одобрения [3, с. 364].

Цифровые технологии как инструмент информационной политики

Для проведения максимально эффективной политики в сфере противодействия киберугрозам необходимо в полной мере использовать достижения и ресурсы набирающего обороты процесса цифровизации. Цифровизация может сыграть немаловажную роль в политике по обеспечению национальной и информационной безопасности страны. Правильное внедрение и использование цифровых нововведений значительно упростит задачу по защите как персональных данных пользователя, так и секретных материалов государственного уровня и значения [9, с. 259].

Одной из наиболее перспективных в этой области представляется технология блокчейн. Она предоставляет новые возможности в борьбе с кибератаками, например, повышенную защиту данных от возможности утечки информации третьим лицам. Если раньше киберпреступнику достаточно было один раз совершить операцию и получить необходимые данные, то теперь блокчейн существенно усложняет для него этот процесс.

Ещё одним важным аспектом является защита процесса обмена информацией. Известно, например, что защита такого мессенджера, как WhatsApp, не даёт стопроцентной гарантии того, что личную переписку не смогут заполучить третьи лица, так как сквозное шифрование несовершенно и имеет слабую сторону (метаданные хранятся в отдельных системах). Для недопущения доступа хакеров, можно использовать технологию блокчейн, способную децентрализовать сеть, разделив метаданные и гарантировав тем самым их совокупную недопустимость [1, с. 172].

Разумеется, только лишь технологии блокчейн будет недостаточно для проведения эффективной информационной политики по пресечению киберпреступной деятельности. В этой сфере могут быть также задействованы ресурсы искусственного интеллекта [6, с. 127]. Например, в США каждый полицейский участок оснащён программой распознавания лиц по изображению. Эта технология активно применяется на практике, что существенно упрощает поиск преступников и ускоряет процесс создания портретов злоумышленников [8, с. 53].

Заключение

В современном мире киберпреступность представляет собой серьёзную угрозу обществу и его информационной безопасности. Киберпреступность порождает комплекс социальных проблем, которые требуют незамедлительного реагирования и эффективного разрешения [12; 13; 14]. С совершенствованием информационных технологий совершенствуется и киберпреступность, находящая проявление во многих сферах жизни и деятельности человека и общества в целом. Защита от данного вида преступлений предполагает корреляцию усилий на уровне международного сотрудничества и взаимодействия [15; 16].

Для проведения эффективной политики по борьбе с информационными правонарушениями и киберпреступлениями могут быть предприняты следующие меры:

1) совершенствование технологий, содействующих выявлению киберпреступлений в сети, а также способов проведения расследований данных правонарушений [5, с. 175];

2) максимально широкое использование технологии блокчейн для противостояния киберугрозам;

3) развитие ресурсов искусственного интеллекта и их последовательное внедрение в сферу расследования киберпреступлений;

4) ужесточение ответственности за совершение киберпреступлений, описанных в гл. 28 УК РФ, вплоть до категории особо тяжких [7, с. 68];

5) целенаправленная борьба с кибертерроризмом во всех его возможных формах и проявлениях.

Статья поступила в редакцию 05.02.2021.

ЛИТЕРАТУРА

1. Антонян Е. А., Аминов И. И. Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2019. № 6 (103). С. 170–175.
2. Волынская О. В Развитие юридической мысли и перспективы в борьбе с киберпреступностью в сфере уголовного судопроизводства // Вестник Московского университета МВД России. 2020. № 3. С. 72–74.
3. Даненьян А. А Международное правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 261–269.
4. Кумышева М. К., Геляхова Л. А. К вопросу о киберпреступности в России и мире // Пробелы в российском законодательстве. 2018. № 4. С. 383–385.
5. Мартьянов Н. Р. Уголовно-правовая борьба с киберпреступлениями на современном этапе // Государственная служба и кадры. 2020. № 1. С. 175–177.
6. Тимофеев А. В. Сущность и проблемы искусственного интеллекта в контексте современных научных и философских представлений // Вестник Московского государственного областного университета. Серия: Философские науки. 2020. № 2. С. 127–133.
7. Тарасик Н. М. Анализ правовых основ борьбы с киберпреступностью // Успехи в химии и химической технологии. 2016. № 5(174). С. 66–68.
8. Тишутина И. В Новые возможности раскрытия и расследования преступлений в условиях глобальной цифровизации // Известия Тульского государственного университета. Экономические и юридические науки. 2019. № 4. С. 46–55.
9. Шинкарецкая Г. Г., Берман А. М., Цифровизация и проблема обеспечения национальной безопасности // Образование и право. 2020. № 5. С. 254–260.
10. Guryanova A. V., Khafiyatullina E., Petinova M., Frolov V., Makhovikov A. Technological prerequisites and humanitarian consequences of ubiquitous computing and networking // Digital economy: complexity and variety vs. rationality. Lecture Notes in Networks and Systems. 2020. Vol. 87. P. 1040–1047.
11. Digital 2020: фиксируем тенденции.URL: https://habr.com/ru/post/497204/ (дата обращения: 25.01.2021).
12. Горбунов А. С. Личность в контексте информационной безопасности государства // Сибирский учитель. 2017. № 5 (114). С. 64–68.
13. Горбунов А. С. Личностная безопасность и рецепция информации в информационном массовом обществе // Философские и методологические проблемы исследования российского общества: сборник трудов Третьей Международной научной конференции. 2019. С. 99–108.
14. Горбунов А. С. Социальная ответственность средств массовой коммуникации в информационном обществе // Вестник Тверского государственного университета. Серия: Философия. 2018. № 4. С. 83–90.
15. Буренков С. В. Феномен неотчужденного труда: автореф. дис. ... канд. филос. наук. М., 2017. 22 с.
16. Родичкин Д. В., Буренков С. В. К вопросу о влиянии культуры на формирование национальной идентичности // Вестник Тверского государственного университета. Серия: Философия. 2020. № 4 (54). С. 167–179.

REFERENCES

1. Antonyan E. A., Aminov I. I. [Blockchain technologies in countering cyber terrorism]. In: *Aktual'nye problemy rossiiskogo prava* [Actual problems of Russian law], 2019, no. 6 (103), pp. 170–175.
2. Volynskaya O. V. [Development of legal thought and perspectives in the fight against cybercrime in the field of criminal proceedings]. In: *Vestnik Moskovskogo universiteta MVD Rossii* [Bulletin of Moscow University of the Ministry of Internal Affairs of Russia], 2020, no. 3, pp. 72–74.
3. Danenyan A. A. [International legal regulation of cyberspace]. In: *Obrazovanie i pravo* [Education and law], 2020, no. 1, pp. 261–269.
4. Kumysheva M. K., Gelyakhova L. A. [On the issue of cybercrime in Russia and in the world]. In: *Probely v rossiiskom zakonodatel'stve* [Gaps in Russian legislation], 2018, no. 4, pp. 383–385.
5. Mart'yanov N. R. [Criminal law fight against cybercrimes at the present stage]. In: *Gosudarstvennaya sluzhba i kadry* [Civil service and personnel], 2020, no. 1, pp. 175–177.
6. Timofeev A. V. [The essence and problems of artificial intelligence in the context of modern scientific and philosophical concepts]. In: *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Filosofskiye nauki* [Bulletin of Moscow Region State University. Series: Philosophy], 2020, no. 2, pp. 127–133.
7. Tarasik N. M. [Analysis of the legal framework for combating cybercrime]. In: *Uspekhi v khimii i khimicheskoi tekhnologii* [Advances in chemistry and chemical technology], 2016, no. 5 (174), pp. 66–68.
8. Tishutina I. V. [New opportunities for solving and investigating crimes in the context of global digi-

talization]. In: *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki* [Bulletin of Tula State University. Economic and legal sciences], 2019, no. 4, pp. 46–55.
9. Shinkaretskaya G. G., Berman A. M. [Digitalization and the problem of ensuring national security]. In: *Obrazovanie i pravo* [Education and law], 2020, no. 5, pp. 254–260.
10. Guryanova A. V., Khafiyatullina E., Petinova M., Frolov V., Makhovikov A. Technological prerequisites and humanitarian consequences of ubiquitous computing and networking. In: D*igital economy: complexity and variety vs. rationality. Lecture Notes in Networks and Systems.* Vol. 87. 2020. pp. 1040–1047.
11. *Digital 2020: fiksiruem tendentsii* [Digital 2020: fixing trends]. Available at: https://habr.com/ru/post/497204 (accessed: 01.25.2021).
12. Gorbunov A. S. [Personality in the context of information security]. In: *Sibirskii uchitel'* [Siberian teacher], 2017, no. 5 (114), pp. 64–68.
13. Gorbunov A. S. [Personal safety and information reception in the informational mass society] In: *Filosofskie i metodologicheskie problemy issledovaniya rossiiskogo obshchestva: sbornik trudov Tret`ej Mezhdunarodnoj nauchnoj konferencii* [Philosophical and methodological problems of the study of Russian society: collection of proceedings of the Third International Scientific Conference], 2019. pp. 99–108.
14. Gorbunov A. S. [Social responsibility of mass media in the information society]. In: *Vestnik Tverskogo gosudarstvennogo universiteta. Seriya: Filosofiya* [Bulletin of Tver' State University. Series: Philosophy], 2018, no. 4, pp. 83–90.
15. Burenkov S. V. *Fenomen neotchuzhdennogo truda: avtoref. dis. ... kand. filosof. nauk* [The phenomenon of non-alienated labor: abstract of PhD thesis in Philosophy sciences]. Moscow, 2017. 22 p.
16. Rodichkin D. V., Burenkov S.V. [On the question of the influence of culture on the formation of national identity]. In: *Vestnik Tverskogo gosudarstvennogo universiteta. Seriya: Filosofiya* [Bulletin of Tver' State University. Series: Philosophy], 2020, no. 4 (54), pp. 167–179.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Тимофеев Александр Вадимович – кандидат педагогических наук, доцент кафедры информационных, развивающих образовательных систем и технологий Самарского государственного технического университета;
e-mail: timofeev_av@list.ru

Комолов Александр Александрович – кандидат технических наук, декан электротехнического факультета Самарского государственного университета путей сообщения;
e-mail: a.komolov@samgups.ru

INFORMATION ABOUT THE AUTHORS

Alexander V. Timofeev – Cand. Sci. (Education) , Assoc. Prof., Department of Information, Developing Education Systems and Technologies, Samara State Technical University,;
e-mail: timofeev_av@list.ru

Alexander A. Komolov – Cand. Sci. (Engineering), Dean, Department of Electrical Engineering, Samara State Transport University;
e-mail: a.komolov@samgups.ru

ПРАВИЛЬНАЯ ССЫЛКА НА СТАТЬЮ

Тимофеев А. В., Комолов А. А. Киберпреступность как социальная угроза и объект правового регулирования // Вестник Московского государственного областного университета. Серия: Философские науки. 2021. № 1. С. 95–101.
DOI: 10.18384/2310-7227-2021-1-95-101

FOR CITATION

Timofeev A. V., Komolov A. A. Cybercrime as a Social Threat and an Object of Legal Regulation. In: *Bulletin of Moscow Region State University. Series: Philosophy*, 2021, no 1. pp. 95–101.
DOI: 10.18384/2310-7227-2021-1-95-101