

4.10. Преступность в сфере информационно-коммуникационных технологий как проблема информационного общества

©Хамурзов Азамат Тoleвич

Северо-Кавказский институт повышения квалификации (филиал)
Краснодарского университета МВД России, г.Нальчик, КБР, Россия
Khamurzovazamat@gmail.com

Аннотация: Целью данного исследования было изучение влияния глобализации и информатизации на преступность в киберпространстве. В эпоху глобализации и цифровизации все данные, личная информация и большая часть денежных средств людей находится на электронных хранителях, смартфонах и персональных компьютерах. Однако у такой резкой трансформации общества есть большой минус, который выразился в развитии такого негативного феномена, как киберпреступность. Киберпреступность является ещё не до конца изученным явлением и методика борьбы с ним ещё не до конца сформирована. К киберпреступлениям относят преступления, совершенные путём использования персонального компьютера для создания вирусных программ, и совершение компьютерных атак или краж личной информации и денежных средств физических и юридических лиц. Развитие информационно-коммуникационных технологий является первопричиной появления киберпреступников.

Слабость правоохранительной системы в борьбе с киберпреступностью связана с тем, что они не сталкивались с большим количеством хакерских атак и большинство из них осуществлялись некомпетентными хакерами, которые допускали банальные ошибки и отследить их и привлечь к ответственности было легко, в отличие от их западных коллег, которым пришлось бороться со специалистами высочайшего уровня, которые не оставляли никаких следов и работали из тени. Выйти на их след и поймать практически невозможно. Таким образом, становится понятно, что наши правоохранительные органы, не имеют как такового опыта борьбы с киберпреступниками, в результате чего у тех появляется возможность совершать преступления и оставаться в большинстве случаев безнаказанными. Для недопущения таких ситуаций в будущем, необходимо подготавливать будущих сотрудников полиции к борьбе с киберпреступностью. Для этого в процессе обучения они должны изучать опыт западных спецслужб в противодействии киберпреступности. В результате мы получим в штабе специалистов по борьбе с киберпреступностью, задачей которых будет пресечение и предупреждение совершения киберпреступлений.

Ключевые слова: сеть интернет, киберпреступность, кибератака, хакеры, жертва.

Для цитирования: Хамурзов А.Т. Преступность в сфере информационно-коммуникационных технологий как проблема информационного общества // Пробелы в российском законодательстве. 2022. Т. 15. №4. С. 265-269.

Crime in the Sphere of Information and Communication Technologies as a Problem of the Information Society

©Khamurzov Azamat Tolevich

North Caucasus Institute for Advanced Studies (branch)
of the Krasnodar University of the Ministry of Internal Affairs of Russia, Nalchik, Russia
Khamurzovazamat@gmail.com

Abstract: The purpose of this study was to study the impact of globalization and informatization on crime in cyberspace. In the era of globalization and digitalization, all data, personal information and most of the money of people are on electronic custodians, smart phones and personal computers. However, such a sharp transformation of society has a big minus, which was expressed in the development of such a negative phenomenon as cybercrime. Cybercrime is not yet a fully understood phenomenon and the methodology for combating it has not yet been fully formed. Cybercrimes include crimes committed by using a personal computer to create virus programs, and the commission of computer attacks or theft of personal information and funds of individuals and legal entities. The development of information and communication technologies is the root cause of the emergence of cybercriminals.

The weakness of the law enforcement system in the fight against cybercrime is due to the fact that they did not encounter a large number of hacker attacks and most of them were carried out by incompetent hackers who made banal mistakes and it was easy to track them down and bring them to justice, unlike their Western counterparts, who I had to fight with top-level specialists who left no traces and worked from the shadows. It is almost impossible to track them down and catch them. Thus, it becomes clear that our law enforcement agencies do not have, as such, experience in dealing with cybercriminals, as a result of which they have the opportunity to commit crimes and go unpunished in most cases. To prevent such situations in the future, it is necessary to prepare future police officers to fight cybercrime. To do this, in the process of training, they must study the experience of Western intelligence agencies in countering cybercrime. As a result,

we will get specialists in the fight against cybercrime at the headquarters, whose task will be to suppress and prevent the commission of cybercrimes.

Keywords: *Internet network, cybercrime, cyber attack, hackers, victim.*

For citation: *Khamurзов A.T. Crime in the Sphere of Information and Communication Technologies as a Problem of the Information Society // Gaps in Russian Legislation. 2022. Vol. 15. №4. Pp. 265-269. (in Russ.).*

ВВЕДЕНИЕ

Современный этап развития общества характеризуется учеными как постиндустриальное. Отличительными чертами постиндустриального общества являются:

- общественное развитие достигает небывалых доселе высот;
- существует и функционирует правовое государство, в котором все граждане равны перед законом;
- отсутствует чёткое деление на классы;
- развит политический плюрализм;
- в промышленности всё больше используются автоматы и роботы, а ручной труд вытесняется;
- научно-технический прогресс ещё больше ускоряется;
- главным фактором производства становится информация;
- наступает глобализация хозяйственной деятельности;
- растёт внимание к глобальным экологическим проблемам человечества;
- повышается уровень образования;
- растёт доля сферы услуг в экономике;
- производительность труда находится на очень высоком уровне;
- ВВП высока доля качественных, инновационных и технологичных услуг.

Современное общество идеально подходит под эти критерии.

Тенденции мирового развития диктуют условия направления развития будущих поколений. В современном мире производство становится автоматизированным и пропадает необходимость даже в дешевой рабочей силе, более конкурентными индивидами являются уже образованные специалисты в той или иной отрасли.

ТРАНСФОРМАЦИЯ ПРЕСТУПНОСТИ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

В эпоху глобализации и цифровизации все данные, личная информация и большая часть денежных средств людей находится на электронных хранителях, смартфонах и персональных компьютерах. Однако у такой резкой трансформации общества есть большой минус, который выразился в развитии такого негативного феномена, как киберпреступность. Киберпреступность является ещё не до конца изученным явлением и методика борьбы с ним ещё не до конца сформирована. К киберпреступлениям относят преступления, совершенные путём использования персонального компьютера для создания вирусных программ, и совершение компьютерных атак или краж личной информации и денежных средств физических и юридических лиц. Развитие информационно-ком-

муникационных технологий является первопричиной появления киберпреступников. Более масштабная деятельность киберпреступников приходится на середину 2000-х годов. Это время в мировой истории характеризуется переходом общества на постиндустриальный этап и последующим мировым экономическим кризисом. В указанный период времени повсеместное развитие получило глобальное информационное пространство – интернет, и никто бы даже не смог предположить какие масштабные и резонансные события она в себе таит. Примерно в те же годы появился Даркнет – анонимная сеть, состоящая из теневого сайтов и виртуальных адресов, предоставляющую передачу данных в зашифрованном виде, что даёт ее пользователям полную анонимность от вмешательства третьих лиц, в том числе государственных органов. С появлением Даркнета множество преступных синдикатов осуществляющих торговлю оружием, наркотиками и людьми освоили данную сеть и стали активно использовать ее для реализации своей преступной деятельности. Многие теневые сети требуют установки специального программного обеспечения для получения доступа к сети. Существуют такие популярные теневые сети как: Tor, RetroShare, Freenet, GUNet – программы для анонимных сетей, которые также используются для доступа в даркнет.

Использование данных программных обеспечений позволяет пользователям сети интернет обмениваться информацией и файлами путём их шифрования, а также дают возможность пользоваться даркнетом.

Даркнет как детище информационно-коммуникационного развития является глобальной проблемой и опасностью для современного общества, по причине того что оно не контролируется никакими государственными структурами и органами и крупнейшие преступные группировки перенесли свою деятельность на эту платформу и в редких случаях продолжают осуществлять свою деятельность вживую. Они находят клиентов и покупателей на просторах интернета и совершают там же свои сделки, которые никак не отслеживаются. Также и заказчик и исполнитель прилагают множество усилий для сохранения своей анонимности и не выдают никакой личной информацию друг о друге, даже оплата услуг совершается не привычными денежными знаками, а криптовалютой, оборот которых также является бесконтрольным. После завершения сделки на виртуальный кошелек исполнителя поступает необходимая сумма в криптовалюте, которая может быть конвертирована в любую валюту, и снята в любом банкомате.

Таким образом, использование даркнета ставит под угрозу всех людей во всем мире, потому что личная информация и денежные средства каждого из нас не находятся в безопасности и могут быть похищены. На сегодняшний день в даркнете присутствует организованное

количество преступных группировок, которые занимают большим спектром незаконных действий.

Однако большую опасность представляют хакеры, которые действуют, как поодиночке, так и в группах. Основной задачей хакеров является создание вирусных программ, которые они дистанционно размещают на компьютерах своих жертв, и похищают оттуда информацию и деньги жертвы. В середине 2000-х годов самым распространённым методом размещения вредоносного вируса на компьютер жертвы был следующий. На электронную почту жертвы приходило сообщение от службы доставки или банка (основным критерием было то, что оно должно быть отправлено от лица компании, письма которой жертва с вероятностью 100% не проигнорирует и откроет), далее после этого жертва открывала письмо, программа автоматически без подтверждения жертвы устанавливалась на ее компьютер, после чего он мог дистанционно управляться злоумышленником. В результате такой бесхитростной манипуляции хакеры могли совершать покупки с компьютера жертвы используя его деньги, красть и уничтожать необходимую информацию. Таким образом, используя данный метод группе хакеров удалось совершить атаки на банки и физические лица, в результате чего ими были похищены миллионы долларов. После такой масштабной атаки многие банки задумались о своей безопасности и безопасности своих клиентов, в результате чего банковская система была видоизменена, и в каждом банке появился специалист, отвечающий за безопасность от атак хакеров, а также специалист занимающийся созданием программного обеспечения для защиты от хакеров [1, 5, 8-10].

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСКИМ СХЕМАМ И АТАКАМ

На современном этапе такие масштабные атаки практически не совершаются, однако появилось множество менее квалифицированных мошенников. На территории России в последние годы появились злоумышленники, которые используют информационно-коммуникационные технологии для получения информации о людях, в частности их номеров телефонов. На номер телефона жертвы они отправляют сообщения или звонят им, и представляются работниками банка, клиентом которого является жертва. Далее они сообщают жертве, что с ее банковской карты была снята крупная сумма денег, и знает ли что-нибудь жертва о данной покупке. Когда выясняется, что жертва не совершала никаких покупок, мошенник говорит что, скорее всего это сделал какой-то злоумышленник и просит предоставить ему данные карты (номер, срок действия, CVV код безопасности). Ничего не подозревающая жертва предоставляет эти данные мошен-

нику, и таким образом имея эту информацию, злоумышленник совершает покупки и переводы денежных средств с банковской карты жертвы. После огромного количества обращений по всей стране, полиция начала расследование по данному факту. В результате выяснилось, что мошенниками являются заключённые, отбывающие наказание в местах лишения свободы. Они добывали информацию о клиентах банков, затем они разработали этот незамысловатый приём, и совершали покупки в интернете, используя карты своих жертв. Данный факт, отлично показывает два огромные проблемы, с которыми необходимо бороться [2-4, 7].

Первая – недостаточная безопасность банковской системы. Учитывая как легко злоумышленники получали информацию о клиентах банков, можно сказать, что на сегодняшний день люди по всей стране являются потенциальными жертвами мошенников и хакеров. А значит необходимо совершенствовать систему безопасности хранимой информации банками РФ. Одним из факторов сомнительной безопасности может являться то что, уже достаточно долгое время, порядка 10 лет, хакерские атаки сошли на нет, и банки считали, что на этом все закончилось, и они больше не столкнутся с ними, но как показала практика данное суждение могло быть ошибочным.

Вторая - слабость правоохранительной системы в борьбе с киберпреступностью. К сожалению в нашей стране правоохранительные органы не сталкивались с большим количеством хакерских атак и большинство из них осуществлялись некомпетентными хакерами, которые допускали банальные ошибки и отследить их и привлечь к ответственности было легко, в отличие от их западных коллег, которым пришлось бороться со специалистами высочайшего уровня, которые не оставляли никаких следов и работали из тени. Выйти на их след и поймать практически невозможно [3, 9, 10].

ВЫВОД

Таким образом, становится понятно, что наши правоохранительные органы не имеют как такового опыта борьбы с киберпреступниками, в результате чего у тех появляется возможность совершать преступления и оставаться в большинстве случаев безнаказанными. Для недопущения таких ситуаций в будущем, необходимо подготавливать будущих сотрудников полиции к борьбе с киберпреступностью. Для этого в процессе обучения они должны изучать опыт западных спецслужб в противодействии киберпреступности. В результате мы получим в штабе специалистов по борьбе с киберпреступностью, задачей которых будет пресечение и предупреждение совершения киберпреступлений.

ЛИТЕРАТУРА

1. *Абидов Р.Р.* Глобализация информационного пространства, как ресурсная база кибертерроризма // Пробелы в российском законодательстве. 2021. Т. 14. № 4. С. 116-119.
2. *Гедгафов М.М.* Развитие кибертерроризма в условиях глобализации информационного пространства // Образование и право. 2021. № 6. С. 304-308.
3. *Зверева Е.Б.* Киберпреступность как угроза безопасности современного общества: виды, особенности, методы борьбы и профилактики // Молодой ученый. 2020. № 10 (300). С. 35-37.
4. *Камергоев Б.М.* Киберпреступление как явление кибертерроризма в глобальном информационном пространстве // В сборнике: Интеллектуальный капитал XXI века. Сборник статей IV Международного научно-исследовательского конкурса. Пенза, 2021. С. 56-58.
5. *Карелина Е.Ю.* Кибербезопасность банковской сферы как неотъемлемая часть цифровой экономики России // В сборнике: Современные технологии в мировом научном пространстве. Сборник статей Международной научно-практической конференции. 2019. С. 166-175.
6. *Ордоков М.Х., Шафиева Э.Т.* Основные тенденции борьбы с кибермошенничеством // Пробелы в российском законодательстве. 2021. Т. 14. № 4. С. 108-111.
7. *Тхазеплов Т.М.* Интернет как один из способов вовлечения лиц в экстремистскую деятельность // Журнал прикладных исследований. 2022. Т. 1. № 3. С. 81-84.
8. *Факов А.М.* Кибертерроризм в социальных сетях как реальная угроза безопасности государства // Евразийский юридический журнал. 2020. № 5 (144). С. 445-446.
9. *Хамурзов А.Т.* Кибертерроризм: новые вызовы и меры противодействия // Журнал прикладных исследований. 2021. Т. 2. № 3. С. 74-77.
10. *Хачидогов Р.А.* Кибертерроризм в глобальном информационном пространстве: новые вызовы и меры противодействия // Образование и право. 2021. № 6. С. 362-366.

РЕЦЕНЗИЯ

на статью «Преступность в сфере информационно-коммуникационных технологий как проблема цифрового общества», подготовленную преподавателем кафедры огневой подготовки СКИФ КрУ МВД России, майором полиции Хамурзовым Азаматом Толевичем

В статье анализируются подходы к определению понятия «цифровая экономика», исследуется ее взаимосвязь с развитием преступности в киберпространстве. На основе статистических данных автором изложен ряд уголовно-правовых деяний с использованием ИКТ, которые являются доминирующими и, соответственно, приобрели особую актуальность в настоящее время. Также раскрывается механизм совершения некоторых из них.

Как следствие, одной из современных тенденций развития мировой экономики является активизация экономической преступной деятельности, но не в традиционном её понимании. Процесс глобализации, помимо многих положительных тенденций, имеет и ряд негативных черт. Экономическая преступность превратилась в одну из наиболее важных проблем, стоящих перед обществом, оказывая деструктивное воздействие как на экономику отдельных государств, так и на развитие мировой экономики. В её состав входит самая прогрессивная, динамичная и научно подкованная разновидность преступности — киберпреступность, ставшая негативным последствием развития информационных технологий. Компьютеры и телекоммуникационные системы, Всемирная сеть Интернет, ставшие неотъемлемыми атрибутами жизнедеятельности современного человека, сформировали новую разновидность экономической преступности.

REFERENCES

1. *Abidov R.R.* Globalization of the information space as a resource base for cyberterrorism // Gaps in Russian legislation. 2021. V. 14. No. 4. pp. 116-119.
2. *Gedgafov M.M.* The development of cyberterrorism in the context of the globalization of the information space // Education and Law. 2021. No. 6. pp. 304-308.
3. *Zvereva E.B.* Cybercrime as a threat to the security of modern society: types, features, methods of struggle and prevention // Young scientist. 2020. No. 10 (300). pp. 35-37.
4. *Kamergoiev B.M.* Cybercrime as a phenomenon of cyberterrorism in the global information space // In the collection: Intellectual capital of the XXI century. Collection of articles of the IV International Research Competition. Penza, 2021, pp. 56-58.
5. *Karelina E.Yu.* Cybersecurity of the banking sector as an integral part of the digital economy of Russia // In the collection: Modern technologies in the world scientific space. Collection of articles of the International scientific-practical conference. 2019. pp. 166-175.
6. *Ordokov M.Kh., Shafieva E.T.* The main trends in the fight against cyber fraud // Gaps in Russian legislation. 2021. V. 14. No. 4. pp. 108-111.
7. *Tkhazeplov T.M.* The Internet as one of the ways to involve individuals in extremist activities // Journal of Applied Research. 2022. V. 1. No. 3. pp. 81-84.
8. *Fakov A.M.* Cyberterrorism in social networks as a real threat to state security // Eurasian Law Journal. 2020. No. 5 (144). pp. 445-446.
9. *Khamurzov A.T.* Cyberterrorism: New Challenges and Countermeasures // Journal of Applied Research. 2021. V. 2. No. 3. pp. 74-77.
10. *Khachidogov R.A.* Cyberterrorism in the global information space: new challenges and countermeasures // Education and law. 2021. No. 6. pp. 362-366.

В целом рецензируемая статья актуальна, представляет научный и практический интерес и может быть рекомендована к публикации.

Рецензент: начальник кафедры огневой подготовки Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета МВД России, полковник полиции М.М. Хамгоков

Статья прошла проверку системой «Антиплагиат»; оригинальность текста – 93,3%

Статья поступила в редакцию 23.05.2022, принята к публикации 21.06.2022

The article was received on 23.05.2022, accepted for publication 21.06.2022

СВЕДЕНИЯ ОБ АВТОРЕ

Хамурзов Азамат Тoleвич, майор полиции, преподаватель кафедры огневой подготовки, Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России, г. Нальчик, Россия. E-mail: Khamurzovazamat@gmail.com

ABOUT THE AUTHOR

Khamurzov Azamat Tolevich, Police Major, lecturer at the Department of Fire Training, North Caucasian institute of professional development (branch) Krasnodar university Ministry of Internal Affairs of the Russian Federation, Nalchik, Russia. E-mail: Khamurzovazamat@gmail.com