

УНИВЕРСИТЕТ ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
МОСКОВСКИЙ ФИНАНСОВО-ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ МФЮА

**ПРОТИВОДЕЙСТВИЕ ПРАВОНАРУШЕНИЯМ,
СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

*Сборник статей по материалам
научно-практической конференции
(III школы-семинара молодых ученых-юристов)*

г. Москва, 11 ноября 2020 г.

Москва



2021

УДК 342.7
ББК 67
П 83

Ответственный редактор:

В.В. Казаков – ученый секретарь Университета прокуратуры
Российской Федерации, кандидат юридических наук

Составитель:

К.А. Комогорцева – ведущий научный сотрудник
Научно-исследовательского института Университета прокуратуры
Российской Федерации, кандидат юридических наук

Рецензенты:

Ю.А. Тимошенко – профессор кафедры уголовно-правовых дисциплин Универси-
тета прокуратуры Российской Федерации, доктор юридических наук, доцент

Д.А. Соколов – ведущий научный сотрудник
Научно-исследовательского института Университета прокуратуры
Российской Федерации, кандидат юридических наук

**П 83 Противодействие правонарушениям, совершаемым с использо-
ванием информационных технологий: сборник статей**
по материалам научно-практической конференции (III школы-
семинара молодых ученых-юристов), г. Москва, 11 ноября 2020
г. / отв. ред. В.В. Казаков ; сост. К.А. Комогорцева ; Университет
прокуратуры Российской Федерации ; Московский финансово-
юридический университет МФЮА. – М. : МФЮА, 2021. – 224 с. –
Текст : непосредственный.

ISBN 978-5-94811-342-5

В сборник включены статьи участников научно-практической
конференции «Противодействие правонарушениям, совершаемым с ис-
пользованием информационных технологий», проведенной Университетом
прокуратуры Российской Федерации и Московским финансово-юридиче-
ским университетом МФЮА 11 ноября 2020 г. в заочной форме.

Предназначается для широкого круга читателей, научных и педаго-
гических работников, аспирантов, адъюнктов, студентов и курсантов юри-
дических вузов и факультетов, а также для работников правоохранительных
и контрольно-надзорных органов.

УДК 342.7
ББК 67

© Университет прокуратуры Российской Федерации, 2020
© Московский финансово-юридический
университет МФЮА, 2020

ISBN 978-5-94811-342-5

СОДЕРЖАНИЕ

Г.А. Гундерич

Использование информационных технологий
в качестве способов совершения преступления 11

К.В. Камчатов

Обеспечение средствами прокурорского надзора прав
и законных интересов лиц, потерпевших от преступлений,
в рамках расследования преступлений,
совершенных с использованием
информационно-телекоммуникационных сетей 18

С.А. Яшков

Проблемы квалификации преступлений,
связанных с неправомерным доступом
к компьютерной информации: отдельный аспект 28

А.О. Антонова

Объекты судебных экономических экспертиз
при расследовании преступлений, совершенных
с использованием информационных технологий 33

Д.А. Бородин

О некоторых факторах, способствующих совершению
кибермошенничеств, и их влиянии
на способы совершения данных преступлений 41

М.О. Бренева

О некоторых особенностях совершения преступлений
экстремисткой направленности с использованием
информационно-телекоммуникационной сети Интернет 51

М.В. Винокуров

Использование информационных технологий
в целях противодействия распространению
фальсифицированных, недоброкачественных
и незарегистрированных средств и медицинских изделий 57

<i>К.В. Ворышева, Д.М. Подсветов</i> Производство следственных действий, предполагающих работу с электронными носителями информации: некоторые проблемные аспекты	63
<i>Е.Ю. Горбунова</i> Развитие информационных технологий и нормативного регулирования цифровой среды как факторы, способствующие совершению преступлений в сфере экономической деятельности	68
<i>Е.С. Душков</i> Киберпреступность во время пандемии COVID-19: существующие проблемы и пути решения	74
<i>В.Ю. Егорушкина</i> Органы прокуратуры в системе противодействия преступности в сфере информационно-компьютерных технологий	81
<i>К.С. Кащеева</i> Кибермошенничество: характеристика и способы	88
<i>К.П. Кочеткова</i> Некоторые вопросы противодействия киберпреступлениям в России	94
<i>Ю.О. Кручинова</i> Международное сотрудничество в борьбе с киберпреступностью	104
<i>И.С. Кузнецова</i> Кибербуллинг как серьезная опасность в пространстве современных средств коммуникаций	108
<i>М.С. Курбатова</i> Облачные сервисы хранения данных как объект преступного посягательства в современном мире	115

А.О. Лукашов

О практике судебной защиты деловой репутации
в сети Интернет 121

Э.Г. Мартынюк

Деятельность ФСБ России, СК России и МВД России
по предупреждению, раскрытию и расследованию
преступлений, связанных с использованием
информационных технологий 132

А.С. Медведева

Особенности досудебного производства
по уголовным делам, связанным
с сексуальными домогательствами несовершеннолетних
в сети Интернет 138

М.С. Новикова

Использование массовых информационных технологий
в экстремистской деятельности 144

В.В. Петренко

Проблемы законодательного регулирования,
пресечения, раскрытия и доказывания хищений,
совершаемых с использованием
информационно-телекоммуникационных технологий 150

А.В. Петрякова

Международная интеграция в борьбе
с проявлениями терроризма в Интернете 158

Е.А. Родина

О некоторых проблемах механизма детерминации
преступности и виктимного поведения 163

Г.С. Сабельникова

Киберпреступность в банковской сфере.
Тенденции и особенности расследования 173

И.В. Сорокин

Направления совершенствования противодействия
правонарушениям, совершаемым
с использованием информационных технологий 180

Р.А. Текеев

Состояние преступности, связанной с использованием
информационных технологий 184

С.С. Чепец

Система распознавания лиц в России:
эффективная помощь в противодействии преступности
или нарушение прав и свобод человека? 190

Д.А. Черноусов

Преступления и правонарушения
против интеллектуальной собственности
в сети Интернет и факторы, способствующие им 198

А.П. Чистов

К вопросу о судебной практике по деяниям,
совершенным с использованием
социальной платформы Инстаграмм 204

А.Н. Шанина

Преступления в сфере информационных технологий:
актуальные проблемы противодействия
и современное состояние в Российской Федерации
и субъектах Российской Федерации
(на примере Тамбовской области) 210

А.А. Шепелёва

Использование информационных технологий
в качестве средства вовлечения подростков
в преступную деятельность 217

Список сокращений 223

CONTENTS

G.A. Gunderich

Using information technology as a means of committing a crime11

K.V. Kamchatov

Ensuring the rights and legitimate interests
of victims of crimes by means of prosecutor's
supervision in the investigation of crimes committed
using information and telecommunications networks 18

S.A. Yashkov

Problems of qualification of crimes related to illegal access
to computer information: a separate aspect 28

A.O. Antonova

The objects of forensic economic expert examinations
in the investigation of crimes committed
with the use of information technology 33

D.A. Borodin

On some factors promoting the commission
of «cyber fraud» and their influence
on the ways of the commission of these crimes..... 41

M.O. Breneva

About some features of commission
of crimes of an extremist orientation with use
of the telecommunications network Internet..... 51

M.V. Vinokurov

Use of information technologies to counteract the spread
of counterfeit, substandard
and unregistered medicines and medical devices 57

K.V. Vorysheva, D.M. Podsvetov

Production investigating actions with electronic carriers
of information: about problem aspects 63

<i>E.Y. Gorbunova</i> The development of information technologies and statutory regulation of the digital environment as factors contributing to the commission of crimes in the sphere of economic activity	68
<i>E.S. Dushkov</i> Cybercrime during the COVID-19 pandemic: existing problems and ways of solution	74
<i>V.Yu. Egorushkina</i> Prosecutor's offices in the system of combating crime in the field of information and computer technologies	81
<i>K.S. Kashcheeva</i> Cyber fraud: characteristics and methods of its commitment	88
<i>K.P. Kochetkova</i> Some problems of counteraction cybercrime in Russia.....	94
<i>Y.O. Kruchinova</i> International cooperation in fight against cybercrime	104
<i>I.S. Kuznetsova</i> Cyberbullying as a serious danger in the space of modern means of communication.....	108
<i>M.S. Kurbatova</i> Cloud data storage services as an object of criminal encroachment in the modern world.....	115
<i>A.O. Lukashov</i> About the practice of judicial protection of business reputation on the Internet	121
<i>E.G. Martyniuk</i> Activities of the Federal security service of Russia, the Investigative committee of Russia	

and the Ministry of Internal Affairs of Russia about prevent, solve and investigation crimes related to the use of information technology	132
<i>A.S. Medvedeva</i>	
Peculiarities of pre-trial proceedings in criminal cases related to sexual harassment of minors in the Internet	138
<i>M.S. Novikova</i>	
Use of mass information technologies in extremist activities	144
<i>V.V. Petrenko</i>	
Problems of legislative regulation, suppression, disclosure and proving of theft committed using information and telecommunications technologies	150
<i>A.V. Petryakova</i>	
International integration in the countering terrorism on the Internet...	158
<i>E.A. Rodina</i>	
Some problems of the mechanism of determination of crime and victim behavior.....	163
<i>G.S. Sabelnikova</i>	
Cybercrime in the banking sector. Trends and features of the investigation	173
<i>I.V. Sorokin</i>	
Directions for improving the counteraction to offenses committed with the use of information technology.....	180
<i>R.A. Tekeev</i>	
State of crime related to the use of information technologies	184
<i>S.S. Chepets</i>	
The system of face recognition in Russia: effective assistance in combating crime or violation of human rights and freedoms?	190

<i>D.A. Chernousov</i> Crimes and offenses against intellectual property on the Internet and promoting factors.....	198
<i>A.P. Chistov</i> On the issue of judicial practice on acts committed using the social platform Instagram.....	204
<i>A.N. Shanina</i> Crimes in the sphere of information technologies: current problems of counteraction and the current state in the Russian Federation and the subjects of the Russian Federation (on the example of the Tambov region).....	210
<i>A.A. Shepeleva</i> Using information technology as a means of involving adolescents in criminal activity.....	217
<i>List of abbreviations</i>	223

Галина Альбертовна ГУНДЕРИЧ
доцент кафедры уголовного процесса, криминалистики
и участия прокурора в уголовном судопроизводстве
Крымский юридический институт (филиал)
Университета прокуратуры Российской,
кандидат технических наук

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В КАЧЕСТВЕ СПОСОБОВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ

Аннотация. Статья посвящена исследованию основных способов использования информационных технологий в преступной деятельности, анализу возможности применения конкретных информационных технологий в совершении некоторых видов преступлений. Отмечаются особенности преступлений, совершаемых с использованием информационных технологий.

Ключевые слова: информационные технологии, способ совершения преступления, киберпреступность.

Galina Albertovna GUNDERICH
associate professor of the Department of state and legal disciplines
Crimean Institute of Law (branch)
of the University of Prosecutor's Office of the Russian Federation,
candidate of technical sciences

USING INFORMATION TECHNOLOGY AS A MEANS OF COMMITTING A CRIME

Abstract. The article is devoted to the study of the main ways of using information technologies in criminal activities, the analysis of the possibility of using specific information technologies in the Commission of certain types of crimes are analyzed. Features of crimes committed with the use of information technologies are taking notice.

Keywords: information technology, method of committing a crime, cybercrime.

Современные информационные технологии находят свое применение не только в профессиональной и повседневной деятельности людей, но и в криминальной среде. По оценкам и российских и зарубежных ученых, все чаще высокие технологии используются в преступных целях¹. Такая популярность информационных техноло-

¹ Goodman M. International Dimensions of Cybercrime // Cybercrimes: A Multidisciplinary Analysis / ed. by S. Ghosh E. Turrini. Berlin: Heidelberg, 2010. P. 17–18.

гий обусловлена возможностью осуществлять преступные действия удаленно, не находясь в прямом контакте с потерпевшим или третьими лицами. А кроме этого, у лиц появляются возможности для координации преступной деятельности, избегая непосредственного взаимодействия, тем самым снижая риски быть обнаруженными².

По данным Генеральной прокуратуры РФ, на деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, приходится одно из четырех регистрируемых в текущем году преступлений (363 тыс.). Ранее отмечавшиеся практически двукратные темпы их увеличения несколько замедлились и составляют 77 %. Отмечается, что больше половины всех киберпреступлений совершается с использованием сети Интернет (209,7 тыс.), свыше 42 % – при помощи средств мобильной связи (155,2 тыс.)³.

Однако даже эти показатели не отражают объективную картину киберпреступности в РФ, поскольку используемое в отчетности понятие «преступление, совершенное с использованием информационно-телекоммуникационных технологий» охватывает около 10 составов преступлений (ст. 158, 159, 159³, 159⁶, 183, 272–274 УК РФ), а ряд преступлений против личности, например доведение до самоубийства (ст. 110 УК РФ), склонение к совершению самоубийства или содействие совершению самоубийства (ст. 110¹ УК РФ), организация деятельности, направленной на побуждение к совершению самоубийства (ст. 110² УК РФ), угроза убийством или причинением тяжкого вреда здоровью (ст. 119 УК РФ), принуждение к изъятию органов и тканей человека для трансплантации (ст. 120 УК РФ), клевета (ст. 128¹ УК РФ), понуждение к действиям сексуального характера (ст. 133 УК РФ) и иные преступления, совершаемые дистанционным способом в отчет не попадают⁴.

² Шевко Н.Р., Читая З.И. Вестник Казанского юридического института МВД России. 2016. № 3 (25). С. 76.

³ Статистический сборник «Состояние преступности в России за сентябрь 2020 г.» // Официальный сайт Генеральной прокуратуры Российской Федерации. URL: <http://genproc.gov.ru/stat/data/1892820/> (дата обращения: 01.11.2020).

⁴ Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. М., 2019. Ч. 1. С. 6.

Необходимо отметить, что использование информационных технологий при совершении преступлений представляет собой целенаправленное использование лицом методов и средств хранения, обработки, передачи либо уничтожения компьютерной информации, с помощью которых облегчается совершение преступления или сокрытие следов преступления⁵.

Способы совершения преступлений с использованием информационных технологий отличаются в зависимости от вида преступления. В то же время анализ практики показывает, что все эти способы обобщенно можно разделить на три группы. Так, рассматриваемые преступления могут быть совершены с применением: методов социальной инженерии, вредоносного программного обеспечения, специальных технических средств⁶.

Методы социальной инженерии, основываясь на постулате рассмотрения пользователя как самого слабого звена в системе информационной безопасности, способны обойти самые мощные системы информационной безопасности⁷. На практике применение указанных методов сводится к обманному получению данных платежных карт (номер, CVV, PIN-коды и пр.). Обман пользователя может быть совершен путем представления сотрудниками кредитных организаций либо иными лицами, имеющими возможность получить данные карты или коды для подтверждения совершения операции в системе дистанционного банковского обслуживания. Полученные данные используются преступниками для совершения неправомерных транзакций от имени законного держателя банковской карты, преимущественно для списания денежных средств со счетов потерпевших.

Указанные методы наиболее распространены поскольку не требуют финансовых затрат, особых технических знаний и по характеру

⁵ Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительная практика: дис. ... канд. юрид. наук. М., 2015. С. 9.

⁶ Захаров Д.Н., Щерба В.В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. 2017. № S2 (20). С. 73.

⁷ Ламинина О.Г. Возможности социальной инженерии в информационных технологиях // Гуманитарные, социально-экономические и общественные науки. 2017. URL: <https://cyberleninka.ru/article/n/vozmozhnosti-sotsialnoy-inzhenerii-v-informatsionnyh-tehnologiyah> (дата обращения: 04.11.2020).

действий проще, чем обход системы безопасности иными способами.

Самая распространенная категория способов противоправной деятельности с использованием информационных технологий – это применение вредоносных программ. Такое программное обеспечение позволяет получить доступ к банковским счетам, иным данным потерпевших. Назначение вредоносного программного обеспечения зависит от характера информации, которую требуется получить злоумышленнику. Так, определенные вредоносные программы осуществляют сбор и передачу информации о реквизитах входа в систему дистанционного банковского обеспечения либо выполнение несанкционированных законным пользователем функций как в тайне от последнего, так и в явном виде. Некоторые программы предполагают дестабилизацию деятельности ранее установленного программного обеспечения.

Вредоносные компьютерные программы находят свое применение в фишинговой деятельности. «Фишинговые» сайты или рассылаемые электронные письма, содержащие вредоносные эксплойты, активируясь через действия пользователя, открывают доступ преступникам в информационную систему, вследствие чего у преступников появляется возможность перехватывать данные, осуществлять переводы денежных средств на подконтрольные им банковские счета.

За счет использования преступниками программ типа «тройанский конь», совершающих в тайне от законного пользователя незапланированные им функции, как например, блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей, преступникам также открывается возможность вымогательства за возврат к исходному состоянию системы.

Вредоносное программное обеспечение усиленно используется при организации распределенных сетевых атак (Distributed Denial of Service, или DDoS), направленных на блокирование доступа к серверу потерпевшего внешними пользователями. В основе таких атак лежит технологическое ограничение пропускной способности сетевой инфраструктуры, поддерживающей Интернет-сайт потерпевшего, перегрузка которого вследствие атаки приводит к задержке при формировании ответа на запросы либо к полному отказу в обслуживании запроса. Такое уязвимое положение потерпевшего

предоставляет возможность преступникам требовать передачи денежных средств в обмен на прекращение DDoS-атаки и восстановление работоспособности сайта потерпевшего.

Отдельно следует выделить использование вредоносного программного обеспечения для операционных систем современных смартфонов. Внедрение такого программного обеспечения на смартфон, где хранятся конфиденциальные сведения о привязанной к номеру телефона банковской карте, имя и пароль входа в систему банковского обслуживания, SMS-сообщения, подтверждающие совершение транзакций и др.), дают большой простор для преступной деятельности.

Вредоносное программное обеспечение «тройного» типа, предоставляет преступникам возможность получить практически полный контроль над мобильным устройством: осуществлять запись, блокирование или перенаправление телефонных звонков; копировать данные из адресной книги; отправлять данные о местоположении; копировать фотографии; использовать микрофон для подслушивания; отправлять и получать SMS; отключать антивирусное программное обеспечение; получать доступ к истории чатов (Skype, Viber, WhatsApp); просматривать историю браузера и выполнять иные функции. Такие возможности создают благоприятные условия для совершения вымогательства под угрозой распространения сведений о частной жизни лица.

Применение специальных технических средств в преступной деятельности предполагает применения оборудования для незаконного доступа к конфиденциальной информации. Наиболее распространенным примером совершения преступлений с использованием специальных технических средств является прочно утвердившийся в криминальной практике скимминг. Скиммеры – специальные накладки на картоприемник и клавиатуру банкомата, позволяют фиксировать и передавать информацию о введенном ПИН-коде. В совокупности с применением другого специального устройства – энкодера, с помощью которого копируется информация с магнитной полосы банковской карты и переносится на магнитные полосы заготовок банковских карт, фактически создаются копии банковских карт, используемые в дальнейшем для хищения денежных средств. Применение специальных технических средств в преступной де-

тельности ограничивается только воображением и технической подготовкой преступников, предоставляя последним возможность беспрепятственного доступа к интересующей информации.

Информационные технологии играют существенную роль в преступлениях, связанных с незаконным распространением объектов, изъятых из гражданского оборота. Для данной категории преступлений первостепенное значение имеет дистанционный способ реализации таких предметов. В частности, такая деятельность предполагает использование социальных сетей, специализированных сайтов на серверах вне юрисдикции государства, возможности которых используются для распространения информации о наличии у продавцов соответствующего запрещенного товара, а также для информирования покупателя о способах и порядке расчетов, времени и месте получения товара.

Информационные технологии активно применяются и в целях сокрытия преступлений. Целевое назначение компьютерных технологий в указанной сфере преимущественно сводится к сокрытию личности преступника и следов его пребывания в сети. Достижение этих целей предполагает использование для входа в Интернет зарубежных IP-адресов, находящихся вне юрисдикции РФ, применение ремейлеров – специальных серверов, получающих почтовые сообщения и переправляющих их по адресам, указанным отправителем, одновременно удаляющим информацию об отправителе, а также использование анонимайзеров – средств, позволяющих изменять данные об обратном адресе и службе электронной почты отправителя. Кроме этого, сокрытие своего присутствия в сети возможно через применение средств Rootkit – программного кода или техники, направленной на сокрытие присутствия в системе заданных объектов, системы VPN (Virtual Private Network), обеспечивающей сетевые соединения поверх другой сети. Тщательное сокрытие IP-адреса компьютера преступника возможно через применение сети луковой маршрутизации Tor, которая позволяет получить анонимный удаленный доступ, пропуская исходные данные субъекта через три различных прокси-сервера шифруя данные разными ключами после каждого перехода⁸.

⁸ Деятельность органов внутренних дел... Ч. 1. С. 158–160.

Существуют и иные виды программного обеспечения, позволяющего скрыть все данные о преступнике, и, что особенно важно, указанные способы совершенствуются с каждым днем.

Быстро развивающаяся динамика преступности с использованием информационных технологий свидетельствует о необходимости совершенствования системы противодействия указанным преступлениям со стороны как законодательных, так и правоохранительных органов. Поскольку появление новых способов противоправной деятельности с использованием высоких технологий требует не только быстрого реагирования правоохранительных органов, но и своевременного правового обеспечения, создающего необходимую правовую базу противодействия киберпреступности.

Кирилл Викторович КАМЧАТОВ
*заведующий отделом научного обеспечения
прокурорского надзора за исполнением законов
при осуществлении оперативно-розыскной деятельности
и участия прокурора в уголовном судопроизводстве
Научно-исследовательский институт
Университета прокуратуры Российской Федерации,
кандидат юридических наук*

**ОБЕСПЕЧЕНИЕ СРЕДСТВАМИ ПРОКУРОРСКОГО
НАДЗОРА ПРАВ И ЗАКОННЫХ ИНТЕРЕСОВ ЛИЦ,
ПОТЕРПЕВШИХ ОТ ПРЕСТУПЛЕНИЙ,
В РАМКАХ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ,
СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ**

Аннотация. В статье приводятся обобщенные сведения о практике прокурорского надзора за процессуальной деятельностью органов предварительного расследования при приеме, рассмотрении и разрешении сообщений о преступлении и расследовании уголовных дел о преступлениях, совершенных с использованием информационно-коммуникационных сетей, направленной на обеспечение прав и законных интересов лиц, потерпевших от преступлений. Автор приходит к выводу о необходимости комплексного реформирования нормативно-правового обеспечения, касающегося возмещения вреда, причиненного преступлением.

Ключевые слова: прокурорский надзор, потерпевший, возмещение вреда, компьютерные преступления, доступ к правосудию.

Kirill Viktorovich KAMCHATOV
*head of the Department of scientific support of Prosecutor's supervision
over the implementation of laws in the implementation
of operational investigative activities and participation
of the Prosecutor in criminal proceedings
Research Institute University of the Prosecutor's office
of the Russian Federation, candidate of legal sciences*

**ENSURING THE RIGHTS AND LEGITIMATE INTERESTS
OF VICTIMS OF CRIMES BY MEANS OF PROSECUTOR'S
SUPERVISION IN THE INVESTIGATION OF CRIMES
COMMITTED USING INFORMATION
AND TELECOMMUNICATIONS NETWORKS**

Abstract. The article provides General information about the practice of Prosecutor's supervision over the procedural activities of preliminary investigation

bodies when receiving, reviewing and resolving reports of a crime and investigating criminal cases of crimes committed using information and communication networks aimed at ensuring the rights and legitimate interests of victims of crimes. The author comes to the conclusion that there is a need for a comprehensive reform of the legal framework related to compensation for damage caused by a crime.

Keywords: prosecutor's supervision, victim, compensation for harm, computer crimes, access to justice.

Интеграция современных информационных и коммуникационных технологий¹ привела к тому, что с помощью компьютерных средств и систем совершаются преступления, затрагивающие все сферы жизнедеятельности человека, особенно это проявляется в последние годы в сфере цифровых платежей и иных финансовых услуг. Специфика механизма совершения преступлений в сфере ИКТ влияет на своевременность и законность принятия процессуальных решений при приеме, регистрации и разрешении сообщений о преступлениях и предварительного расследования.

Данные прокуратур субъектов РФ и компаний, специализирующихся на информационной безопасности, подтверждают, что не менее 80 % хищений с использованием ИКТ, совершаются посредством так называемой социальной инженерии², например, при помощи отправки сообщений потенциальным жертвам или звонков с номеров SIM-карт, приобретенных без регистрации или оформленных на третье лицо. Выведение похищенных денег осуществляется через подставные банковские карты, счета в Интернет-магазинах, лицевые счета мобильного телефона. Действия преступников нацелены на слабости человеческого характера и личности (доверчивость, невнимательность, неграмотность и др.).

К примеру, в производстве СЧ СУ УМВД России по Брянской области находилось уголовное дело по обвинению Х. в совершении 29 преступлений, предусмотренных ч. 2 ст. 159 УК РФ. Расследованием уголовного дела установлено, что в период с февраля по июнь 2018 г. Х. путем случайного набора абонентских номеров посредством мобильного телефона звонил гражданам и, представляясь сотрудни-

¹ Далее – ИКТ.

² В контексте современного понимания информационной безопасности и настоящего исследования под социальной инженерией понимается психологическое манипулирование людьми с целью совершения определенных действий.

ком полиции, сообщал о том, что якобы их родственник совершил дорожно-транспортное происшествие, при котором пострадал человек. За решение проблемы «родственника» он требовал деньги. Таким образом фигурант похитил у 29 жителей Брянской области денежные средства в сумме 1 126 000 руб. По результатам расследования 9 января 2019 г. уголовное дело направлено в областной суд, приговором которого Х. назначено наказание в виде лишения свободы на срок 4 года 6 месяцев с отбыванием наказания в исправительной колонии общего режима. Приговор вступил в законную силу.

Необходимо отметить, что криминальные методы «удаленного» хищения денежных средств постоянно эволюционируют, при этом преступниками активно применяются современные IT-технологии, которые зачастую просты в использовании и доступны неограниченному числу пользователей глобальной сети. Очень часто потерпевшие в силу незначительности причиненного вреда не заявляют о правонарушении в правоохранительные органы. Преступники отлично осведомлены об этом и успешно пользуются, вместе с тем посредством незначительного хищения у десятков и сотен потерпевших причиняется в сумме значительный ущерб.

Положительная динамика рассматриваемых преступлений отмечалась во время применения карантинных мер, вызванных глобальным распространением пандемии COVID-19. Ограничения перемещений, изоляция отразились на психологическом состоянии граждан, увеличении спроса на определенные товары, расширении использования онлайн-сервисов для решения повседневных вопросов, а также значительных объемах электронной торговли (преимущественно Интернет-магазины). В последнее время в Интернете появилось много фейковых страниц, предлагающих работающую проверенную вакцину от COVID-19.

За последние годы характерными сложностями, возникающими у органов предварительного расследования при проверках сообщений о компьютерных преступлениях, являются³ длитель-

³ Информационно-аналитический обзор «Прокурорский надзор за процессуальной деятельностью органов предварительного следствия при расследовании преступлений в сфере компьютерной информации», Научно-исследовательский институт Университета прокуратуры Российской Федерации, 2018 год.

ность исполнения запросов Интернет-провайдером, кредитными учреждениями и администрациями электронных платежных систем по движению денежных средств по банковским картам, зачастую неисполнительность запросов банками и организациями.

Например, по сведениям из прокуратуры Ненецкого автономного округа, сроки исполнения запросов следователей, направленных в банки и владельцам платежных систем (ООО ПС «Яндекс Деньги», ЗАО «QIWI-банк», ООО «Одноклассники», АО «Моби деньги») составляют 3–4 недели.

Следует отметить, что запросы в финансовые и кредитные учреждения могут направляться только после возбуждения уголовного дела, поскольку в рамках проведения доследственной процессуальной проверки это невозможно в виду положений Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности».

Прокурорами отмечается, что качество проводимых проверок сообщений о преступлениях в сфере ИКТ находится на недостаточном с учетом общественной опасности и распространенности уровне.

Значительное количество выявленных прокурорами нарушений обусловлены ненадлежащим ведомственным контролем за их проведением со стороны руководителей. Материалы, находящиеся в производстве следователей, до принятия по ним процессуального решения практически не изучаются. Указания в ходе проверок сообщений о преступлениях о выполнении конкретных мероприятий с целью предупреждения нарушений и исключения фактов вынесения незаконных решений не даются. Отмечается отсутствие должной последовательной и системной организации работы, низкая эффективность тактики и выработанной методики производства проверочных мероприятий, определение ошибочных и не вытекающих из фактических исследуемых обстоятельств направлений проверки, неправильное применение норм уголовного и уголовно-процессуального законодательства.

Отмечены неединичные факты рассмотрения сообщений о преступлениях не в соответствии с положениями УПК РФ, а по нормам Федерального закона от 2 мая 2016 г. № 59-ФЗ «О порядке рассмотрения обращения граждан Российской Федерации», списание сообщений в номенклатурное дело как не содержащих поводов для

проведения процессуальной проверки, возвращение заявителю или перенаправление сообщений в другой орган без регистрации, необоснованный отказ в возбуждении уголовного дела, фальсификация материалов проверки по сообщению о преступлении. Не всегда регистрировались выявленные в ходе проверки новые преступления⁴.

Наиболее характерным нарушением законов при проведении процессуальных проверок о преступлениях анализируемого вида является нарушение ст. 6¹, ч. 2 ст. 21, ч. 4 ст. 41, ст. 144, ч. 6 ст. 148 УПК РФ, закрепляющих обязанность правоохранительных органов принимать достаточные и эффективные меры, направленные на своевременное осуществление уголовного преследования и соблюдение разумных сроков уголовного судопроизводства, что влечет за собой нарушение конституционных прав заявителей на защиту и доступ к правосудию в разумные сроки.

Имели место случаи, когда по сообщениям о преступлениях следователями принимались решения об отказе в возбуждении уголовных дел на том основании, что в срок доследственной проверки не получены сведения о движении похищенных денежных средств, собственниках банковских счетов. Нередко за установленный в УПК РФ срок не опрашиваются все участники событий происшествия, не приобщается необходимая документация, подтверждающая размер причиненного ущерба.

В некоторых случаях прокурорами при проверке законности принятых процессуальных решений отмечаются многочисленные нарушения требований закона, прежде всего в установлении обстоятельств проверяемого факта, что не составляет особого труда и временных затрат.

Так, 21 мая 2019 г. в прокуратуру г. Белово поступило постановление следователя от 20 мая 2019 г. о возбуждении уголовного дела по признакам преступления, предусмотренного ч. 3 ст. 159 УК РФ, по факту хищения путем обмана денежных средств в сумме 670 000 руб. при заключении договора кредитования от имени Л.

⁴ Информационное письмо Генеральной прокуратуры Российской Федерации «О состоянии законности при принятии органами предварительного расследования решений об отказе в возбуждении уголовного дела, приостановлении предварительного следствия и прекращении производства по уголовным делам» от 10 февраля 2016 г. № 36-11-2016.

Вместе с постановлением поступили материалы процессуальной проверки, при изучении которых установлено, что постановление следователя является незаконным, подлежит отмене, поскольку в нарушение требований ст. 73, 144 УПК РФ в ходе процессуальной проверки исследованы не все имеющие значение для принятия законного решения обстоятельства.

Не установлено лицо, которому принадлежат деньги в сумме 670 000 руб. и которому причинен ущерб. Выводы следователя о том, что пострадавшей является Л., не соответствовали действительности, поскольку денежные средства на ее банковский счет не поступали, с него не списывались. В рамках процессуальной проверки не приняты меры по установлению лица, которому причинен ущерб. Не проверена информация Л. о поступлении в ее адрес сообщения о наличии задолженности по кредиту. С учетом выявленных нарушений постановление о возбуждении уголовного дела 22 мая 2019 г. отменено прокурором⁵.

Выявляются нарушения требований УПК РФ об информационном обеспечении заявителей о преступлении, когда ему не направляется уведомление о принятом по результатам проведенной проверки процессуальном решении и копия процессуального решения.

На стадии предварительного расследования одно из самых распространенных нарушений выражается в несоблюдении требования ст. 6¹ УПК РФ, что в ряде случаев грубо нарушало право потерпевших от преступлений, препятствуя их доступу к правосудию. Примеры данных нарушений более всего отмечены прокурорами. Встречались факты повторного нарушения прав потерпевших уже после принятия прокурором мер реагирования, вынесения заочного постановления о признании лица потерпевшим без объявления заинтересованному лицу. Прокурорами отмечались факты нарушения прав и законных интересов потерпевших, препятствующих их доступу к правосудию, к окончанию производства по уголовному делу.

Например, прокуратурой Ленинского района г. Иваново 22 октября 2019 г. отменено незаконное постановление от 18 октября 2019 г. о приостановлении предварительного расследования на основании п. 1 ч. 1 ст. 208 УПК РФ по уголовному делу о преступлении,

⁵ По материалам деятельности прокуратуры Кемеровской области.

предусмотренном ч. 1 ст. 128¹ УК РФ. При проверке законности принятого решения о приостановлении предварительного расследования установлено, что в нарушение требований ст. 6¹, 42, 73, ч. 5 ст. 208 УПК РФ в ходе проведенного дознания при наличии сведений о лице, которому преступлением причинен моральный вред, постановление о признании потерпевшим не вынесено, данное лицо в качестве потерпевшего не допрошено, свидетели, о которых в материалах уголовного дела имелись данные, не допрошены, мер для получения сведений о лице, использовавшем аккаунт «ВКонтакте» для совершения преступления, не принято.

Анализ надзорной деятельности на стадии изучения уголовных дел, поступивших с обвинительным заключением, показал, что основными нарушениями являются неполнота следствия, отсутствие достоверных доказательств размера причиненного ущерба, непринятие следователем обеспечительных мер по гражданскому иску.

В ходе предварительного расследования немаловажным остается и вопрос о возмещении причиненного компьютерными преступлениями ущерба.

В целом прокуроры оценивают деятельность органов предварительного следствия по обеспечению ущерба по данной категории уголовных дел как достаточную. В ходе расследования с обвиняемыми (подозреваемыми) проводится работа, направленная на инициирование добровольного возмещения причиненного преступлением ущерба, разъясняются положения действующего уголовного и уголовно-процессуального законодательства о правовых последствиях, смягчающих положение виновного лица при добровольном возмещении причиненного ущерба⁶. В добровольном порядке ущерб, как правило, возмещался лишь частично.

С целью обеспечения гражданского иска и исполнения наказания в виде штрафа следователи обращаются в суд с ходатайствами о наложении ареста на имущество обвиняемых. В ряде регионов прокурорами налажена комплексная работа по обеспечению возмещения вреда от преступлений в сфере ИКТ.

Так, в целях обеспечения прав потерпевших на возмещение вреда, причиненного преступлением, а также исполнения приговора

⁶ По материалам деятельности прокуратуры Магаданской области.

в части возможной конфискации и иных взысканий по уголовным делам следователями территориальных органов СУ УМВД России по Ярославской области проводились обыски по месту жительства обвиняемых, запрашивались сведения о наличии у привлекаемых к ответственности лиц имущества (в частности недвижимости, автотранспорта, оружия и другого подлежащего обязательной регистрации имущества), счетов в банках, на которые может быть наложен арест, направлялись поручения в подразделения МВД России, уполномоченные проводить оперативно-розыскные мероприятия.

Работа в рассматриваемой сфере организована в соответствии с совместным приказом прокуратуры Ярославской области, СУ СК России по Ярославской области, УФСБ России по Ярославской области, УМВД России по Ярославской области, УФССП России по Ярославской области, ГУ МЧС России по Ярославской области от 25 апреля 2019 г. № 40/36/30/223/209/211 «Об организации межведомственного взаимодействия при возмещении причиненного преступлениями ущерба».

Вопросы возмещения причиненного преступлениями ущерба обсуждены 23 апреля 2019 г. на заседании межведомственного совещания руководителей правоохранительных органов Ярославской области «О результатах анализа состояния работы правоохранительных и иных уполномоченных органов по возмещению ущерба, причиненного преступлениями».

В соответствии с решением указанного межведомственного совещания прокуратуры, изучая уголовные дела, поступившие с обвинительным заключением (актом, постановлением), устанавливают полноту принятых правоохранительными органами мер по возмещению ущерба, причиненного преступлениями, а также пресечению фактов возможной легализации (отмывания) денежных средств или иного имущества, приобретенного преступным путем. Нарушение прав потерпевших на возмещение причиненного преступлением ущерба рассматривается как самостоятельное основание для возвращения уголовного дела на дополнительное расследование.

Работа по возмещению ущерба, причиненного преступлениями, ведется в тесном взаимодействии с органами, осуществляющими оперативно-розыскную деятельность. В ходе расследования уголовных дел для отыскания имущества подозреваемых и обвиняемых запрашиваются необходимые сведения в органах Росреестра о на-

личии у подозреваемого прав на недвижимое имущество и земельные участки; в органах ГИБДД – о наличии зарегистрированных транспортных средств, прицепов; в органах Ростехнадзора – о наличии прав на спецтехнику; в Инспекции по маломерным судам – о наличии прав на плавательные средства; в органах Федеральной налоговой службы РФ – о том, является ли лицо руководителем либо учредителем юридического лица, индивидуальным предпринимателем; в организациях, оказывающих услуги держателей реестра акционеров – о наличии у лица в собственности акций; в банках – о наличии счетов, банковских карт, а также банковских ячеек. В целях повышения эффективности возмещения ущерба органами следствия принимаются меры к своевременному проведению обысков и выемок, устанавливается имущество, на которое возможно наложить арест. Потерпевшим при наличии данных о причинении им преступлением имущественного вреда разъясняется порядок заявления иска⁷.

Вместе с тем анализ следственной и судебной практики демонстрирует ряд примеров, когда принимаемые органами предварительного расследования меры по возмещению материального ущерба, причиненного преступлением, являются недостаточными.

По некоторым уголовным делам наличие недвижимости, банковских вкладов не проверяется, отдельные поручения о проведении соответствующих проверок не даются. В планах расследования уголовных дел не указываются мероприятия, направленные на розыск похищенного и установление наличия имущества у подозреваемых и обвиняемых с учетом их связей. Кроме того, дознаватели пренебрегают такой важной процессуальной мерой, как наложение ареста на имущество, хотя своевременное ее применение дает возможность обеспечить сохранность разысканного имущества преступника и возместить материальный ущерб потерпевшим⁸.

Меры к установлению имущества, за счет которого может быть возмещен причиненный ущерб, предпринимаются не на стадии предварительных оперативных мероприятий, а в ходе проведения процессуальной проверки или расследования уголовного дела, когда имущество уже легализовано⁹.

⁷ По материалам прокуратуры Кемеровской области.

⁸ По материалам прокуратуры Ставропольского края.

⁹ По материалам прокуратуры Тверской области.

Также прокурорами констатировалось отсутствие инициативы в работе следственных органов по направлению запросов об оказании международной правовой помощи, относящихся к установлению имущества обвиняемых по уголовным делам, находящегося за рубежом.

Нельзя не отметить также объективные сложности, присущие всем категориям уголовных дел: на момент раскрытия преступления и установления лица, совершившего преступление, похищенные денежные средства израсходованы; отсутствие у виновных лиц какого-либо дохода, либо имущества, на которое возможно наложение ареста¹⁰.

Обобщение практики прокурорского надзора за процессуальной деятельностью органов предварительного расследования позволяет говорить о том, что каких-либо существенных факторов правообеспечительного характера, препятствующих эффективно и в разумный срок осуществлять расследования преступлений в сфере ИКТ, в настоящее время нет. В абсолютном большинстве случаев формальные нарушения требований уголовно-процессуального закона связаны с отсутствием наступательности и инициативности следователей и дознавателей при проведении уголовных процедур. Как и по уголовным делам иных категорий, ведомственный контроль не несет существенной компенсационной функции, а создает дополнительную организационную нагрузку на надзирающих прокуроров.

Для повышения эффективности процессуальной деятельности, направленной на возмещение причиненного преступлением вреда, необходимо: создание единой системы учета наличия имущества, вкладов (счетов) в банках и т.п. (например, для отыскания вклада (счета) в банковских учреждениях сотрудникам органов предварительного расследования необходимо направлять соответствующие запросы в десятки банков, филиалов и отделений банков, для отыскания недвижимости – в территориальные регистрирующие органы); внедрение возможности оперативной блокировки расчетных счетов, куда были перечислены похищенные денежные средства (установленный в настоящее время порядок нередко приводит к невозможности своевременно заблокировать их перечисление и, соответственно, вернуть потерпевшим (эта особенность хорошо известна преступникам); включение в УПК РФ правовых возможностей по принятию обеспечительных мер на стадии процессуальной проверки.

¹⁰ По материалам прокуратур Забайкальского края, Иркутской области.

Сергей Александрович ЯШКОВ
*доцент кафедры уголовного права,
криминологии и уголовного процесса
Екатеринбургский филиал Московской академии
Следственного комитета Российской Федерации,
кандидат юридических наук, доцент*

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕПРАВОМЕРНЫМ ДОСТУПОМ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ОТДЕЛЬНЫЙ АСПЕКТ

Аннотация. Статья посвящена квалификации преступлений, связанных с неправомерным доступом к компьютерной информации. Автором предпринята попытка поставить и разрешить вопрос об уголовно-правовой оценке действий виновного, осуществившего неправомерный доступ к охраняемой законом компьютерной информации, не повлекших уничтожения, блокирования, модификации либо копирования компьютерной информации.

Ключевые слова: блокирование, модификация, копирование, компьютерная информация, неправомерный доступ.

Sergey Alexandrovich YASHKOV
*associate professor of the Department of criminal law,
criminology and criminal procedure
Yekaterinburg branch Federal State Educational Institution
of Higher Education «Moscow Academy
The Investigative Committee of the Russian Federation»,
candidate of legal sciences, associate professor*

PROBLEMS OF QUALIFICATION OF CRIMES RELATED TO ILLEGAL ACCESS TO COMPUTER INFORMATION: A SEPARATE ASPECT

Abstract. The article is devoted to the classification of crimes related to illegal access to computer information. The author made an attempt to raise and resolve the issue of the criminal-legal assessment of the actions of the guilty person who carried out illegal access to the computer information protected by law, which did not entail the destruction, blocking, modification or copying of computer information.

Keywords: Blocking, modification, copying, computer information, illegal access.

Современная жизнедеятельность человечества немыслима без техники, технологий, связи, коммуникации. С одной стороны, они

существенно облегчают нашу жизнь, а, с другой, – создают новые уникальные возможности для совершения уголовно-наказуемых деяний.

Среди них можно выделить преступления в сфере компьютерной информации, ответственность за которые предусмотрена гл. 28 УК РФ. Среди четырех составов преступлений, нашедших свое место в данной главе, наиболее интересным представляется ст. 272 УК РФ, устанавливающая ответственность за неправомерный доступ к охраняемой законом компьютерной информации.

О распространенности совершения анализируемого преступления могут свидетельствовать статистические данные, изложенные на официальном сайте Министерства внутренних дел РФ. Так, в 2019 г. в России было зарегистрировано 2 883 преступления в сфере компьютерной информации, из которых 2 420 связаны с неправомерным доступом к компьютерной информации. В январе – августе 2020г. – 3 063 преступления в сфере компьютерной информации, из которых 2 742 касаются ст. 272 УК РФ¹.

Поскольку состав преступления, предусмотренного ст. 272 УК РФ, материальный, не последнюю роль в нем играют последствия: уничтожение, блокирование, модификация либо копирование компьютерной информации (далее – последствия, указанные в законе).

Судебная практика РФ показывает, что проблем с привлечением к уголовной ответственности лиц, чьи действия повлекли за собой указанные в законе последствия, в общем-то, не имеется.

Например, М. была признана виновной в совершении преступления, предусмотренного ч. 1 ст. 272 УК РФ. Она, будучи сотрудницей профессионального образовательного учреждения, не желая продолжать трудовую деятельность с новым руководством, решила удалить новостные сообщения о деятельности организации с официального сайта учреждения.

С этой целью, используя собственный ноутбук, она осуществила выход в Интернет, открыла страницу сайта учреждения, а потом путем незаконного ввода аутентификационной информации, а именно пароля и логина, которые у нее имелись в связи с ранее занимаемой должностью, обеспечила себе доступ к сайту в режиме

¹ URL: <https://мвд.рф> (дата обращения: 28.10.2020).

администратора. После чего М. осуществила уничтожение с сайта новостной ленты путем ее удаления².

В другом примере В., работая в салоне сотовой связи, используя биллинговую программу, осуществила неправомерный доступ к аккаунту социальной сети, принадлежащему другому лицу, после чего изменила от него пароль, а впоследствии удалила данный аккаунт. В. также была осуждена по ч. 1 ст. 272 УК РФ. В приговоре было отражено, что ее действия повлекли модификацию и блокирование компьютерной информации³.

Еще в одном случае приговором суда Б. осужден за неправомерный доступ к охраняемой законом компьютерной информации, повлекший копирование компьютерной информации. Так, у Б., работавшем в отделе безопасности исправительной колонии УФСИН России по Республике Мордовия, возник умысел осуществить неправомерный доступ к базам данных УФСИН России по Республике Мордовия с целью их дальнейшего копирования в скрытую папку служебного компьютера для личного просмотра, что им и было осуществлено с помощью выхода в сеть Интернет и использования компьютерной программы для сканирования сети «IPScan»⁴.

Как видно, приведенные примеры судебной практики показывают то, что трудностей с привлечением к ответственности по ст. 272 УК РФ в РФ не имеется при условии, если неправомерный доступ к компьютерной информации приводит к последствиям, указанным в законе.

Вместе с тем, возникает вопрос: какую уголовно-правовую оценку дать действиям лица, если неправомерный доступ к компьютерной информации им был осуществлен, однако анализируемых последствий не наступило?

² Приговор Октябрьского районного суда г. Саранска Республики Мордовия от 9 сентября 2019 г. (по делу № 1-226/2019) // ГАС «Правосудие». URL: <https://bsr.sudrf.ru> (дата обращения: 28.10.2020).

³ Приговор Бугурусланского районного суда Оренбургской области от 18 июля 2019 г. (по делу № (1)-149/2019) // ГАС «Правосудие». URL: <https://bsr.sudrf.ru> (дата обращения: 28.10.2020).

⁴ Приговор Зубово-Полянского районного суда Республики Мордовия от 11 сентября 2019 г. (по делу № 1-123/2019) // ГАС «Правосудие». URL: <https://bsr.sudrf.ru> (дата обращения: 28.10.2020).

Например, судебной практике известен такой случай. В., используя компьютер, подобрав пароль доступа к почтовому ящику общества с ограниченной ответственностью, получил возможность ознакомиться с находящимися в нем входящими и исходящими сообщениями. После этого с целью дальнейшего ознакомления с перепиской, осуществляемой по данному почтовому ящику, В. создал фильтр для пересылки копий входящих и исходящих электронных писем с данного почтового ящика на другой почтовый ящик. Кроме того, получив возможность администрирования указанного электронного почтового ящика, он впоследствии удалил с него несколько писем, а также поменял ранее привязанный к нему законным владельцем абонентский номер к другому абонентскому номеру.

Как видно, в результате действий В. наступил целый «букет» последствий, указанных в законе. Здесь имеется и копирование компьютерной информации, и ее уничтожение, и модификация. За содеянное В., конечно, был осужден⁵. Вместе с тем возникает вопрос: как квалифицировать его действия, если бы он остановился на стадии незаконного доступа к почтовому ящику и только лишь ознакомился с его содержимым, например, входящими или иными сообщениями?

Объективная сторона состава анализируемого преступления – неправомерный доступ – может быть представлена, с одной стороны, как действие, а, с другой, – как определенный результат этих действий – состояние. Если виновный занимается непосредственно доступом к компьютерной информации, например, подбирает пароль или пытается «взломать» систему защиты, то указанные в законе последствия могут наступить. Вместе с тем можно ли говорить о составе преступления, если эти последствия не наступили?

Так, в приведенном выше случае субъект преступления подобрал пароль к почтовому ящику. Представляется, что нет смысла утверждать, что здесь имели место такие последствия как уничтожение и блокирование компьютерной информации.

Про модификацию тоже вряд ли приходится говорить, поскольку к почтовому ящику с помощью какого-либо программного

⁵ Приговор Кировского районного суда г. Перми Пермского края от 10 октября 2019 г. (по делу № 1-355/2019) // ГАС «Правосудие». URL: <https://bsr.sudrf.ru> (дата обращения: 28.10.2020).

обеспечения был подобран «родной» пароль и вход в него осуществлен именно с его использованием.

Вопрос же о последствиях «копирования» в данном случае требует более глубокого анализа. Копирование компьютерной информации можно рассматривать, с одной стороны, как копирование файла, а, с другой стороны, как копирование информации, содержащейся в файле. Копирование файла – процедура достаточно простая, которая заключается в его переносе с одного хранилища (например, жесткого диска) на другой (например, флэшку).

Очевидно, что когда виновное лицо в приведенном (или подобном) случае ознакомилось с экраном монитора, например, с содержанием писем электронной почты, оно не осуществило копирования компьютерной информации, поскольку не копировало никаких файлов.

Копирование информации – создание стопроцентно идентичной ее копии. Нетрудно догадаться, что чтение писем электронной почты не является копированием информации постольку, поскольку мозг человека не сможет воспроизвести прочитанную информацию в стопроцентной идентичности, вплоть до запятой.

Таким образом, следует признать, что в правоприменительной практике могут возникнуть проблемы с квалификацией действий, которые не повлекли за собой указанных в законе последствий. Вместе с тем можно предположить, что они могут рассматриваться как неоконченная преступная деятельность. Например, как покушение. В данном случае вопрос также достаточно неоднозначный.

Неправомерный доступ может быть рассмотрен и как действие и как результат этих действий – состояние. Очевидно, что «чтение компьютерной информации» с монитора – это процедура, которая реализуется и после «действия» и после «состояния». Следовательно, такое «чтение» вряд ли можно назвать даже окончанным покушением.

Следует сделать вывод, что в настоящее время является затруднительной квалификация действий, связанных с неправомерным доступом к компьютерной информации, не повлекших последствий, указанных в законе. При наличии оснований их можно квалифицировать по ст. 19 или гл. 28 УК РФ.

Анастасия Олеговна АНТОНОВА

студент

*Московский государственный юридический университет
им. О.Е. Кутафина*

ОБЪЕКТЫ СУДЕБНЫХ ЭКОНОМИЧЕСКИХ ЭКСПЕРТИЗ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В статье на основе статистических данных МВД России за 6 месяцев 2020 г. подтверждается возникновение новых – цифровых объектов судебной экономической экспертизы. Исследуются мнения ученых о современном состоянии и видах объектов рассматриваемого класса судебных экспертиз. Обосновываются выводы о необходимости и порядке привлечения сведущих лиц, обладающих специальными знаниями как в области экономики, так и компьютерной техники для обнаружения, фиксации, изъятия и исследования компьютерной информации, необходимой для производства судебной экономической экспертизы.

Ключевые слова: судебная экономическая экспертиза, объекты экспертизы, цифровые следы, компьютерная техника.

Anastasia Olegovna ANTONOVA

student

Kutafin Moscow State Law University

THE OBJECTS OF FORENSIC ECONOMIC EXPERT EXAMINATIONS IN THE INVESTIGATION OF CRIMES COMMITTED WITH THE USE OF INFORMATION TECHNOLOGY

Abstract. The article confirms the emergence of new digital objects of forensic economic expertise based on statistical data of the Ministry of internal Affairs of Russia for 6 months of 2020. The article examines the opinions of scientists about the current state and types of objects of the considered class of forensic examinations. Conclusions about the necessity and procedure for attracting knowledgeable persons with special knowledge both in the field of Economics and computer technology to detect, record, withdraw and study computer information necessary for the production of forensic economic expertise are substantiated.

Keywords: forensic economic expertise, objects of expertise, digital traces, computer equipment.

В настоящее время можно отметить две тенденции криминальной обстановки в России. Первая – стабилизация экономической

преступности: за 6 месяцев 2020 г. по сравнению с январем – июнем 2019 г. на 3,0 % сократилось число преступлений экономической направленности, выявленных правоохранными органами. Всего выявлено 63,5 тыс. преступлений данной категории, удельный вес этих преступлений в общем числе зарегистрированных составил 6,3 %. Вторая – МВД России полагает, что существенным фактором, оказывающим негативное влияние на криминогенную ситуацию в стране, продолжает оставаться рост IT-преступности. За январь–июнь 2020 г. он составил 91,7 % по сравнению с аналогичным периодом прошлого года, а удельный вес указанных противоправных деяний в общей структуре преступности достиг 22,3 %. При этом вторая тенденция превалирует над первой, поскольку существенная часть преступлений экономической направленности, предварительное следствие по которым обязательно, совершается с использованием компьютерных и телекоммуникационных технологий (9 028 от выявленных преступлений, рост составил 38,8 %)¹.

Традиционно в ходе расследования экономических преступлений требуется назначение и производство судебных экономических экспертиз, с помощью которых устанавливаются обстоятельства, подлежащие доказыванию по конкретному делу, посредством разрешения вопросов, требующих специальных знаний о финансово-хозяйственных операциях, экономических показателях на основе изучения документов бухгалтерского учета. Однако в связи с указанным совершением экономических преступлений с использованием информационных технологий происходит определенное видоизменение объектов судебных экономических экспертиз и, соответственно, методического обеспечения их производства.

Данные экспертизы являются достаточно распространенными в уголовном судопроизводстве, их производство организовано во всех государственных судебно-экспертных учреждениях. В теории судебной экспертологии и практической судебно-экспертной деятельности экономические экспертизы являются широким понятием, под которым подразумевается целый класс судебных экспертиз. Предметом исследования судебно-экономической экспертизы является

¹ Официальный сайт МВД России. Состояние преступности в РФ: январь-июнь 2020 г. URL: <https://media.mvd.ru/files/application/1899165> (дата обращения: 07.11.2020).

содержание операций, в которых указана информация о состоянии, движении, наличии или отсутствии материальных ценностей и денежных средств, их источниках, сведения о фактических данных, характеризующих образование, распределение и использование на предприятии доходов, денежных средств (фондов), негативные отклонения в этих процессах. Также, эксперт может прийти к выводам о нарушениях (отсутствии нарушений) в ведении бухгалтерского учета, влияние исходных данных на показатели хозяйственной деятельности или способствовавшие совершению преступлений, связанных с несоблюдением финансовой дисциплины².

Судебная экономическая экспертиза предполагает изучения различного рода документов, электронных носителей информации и других материалов и объектов, обнаруженных при расследовании уголовного дела. Следует отметить, что экономический эксперт изучает не внешние признаки документов и других предметов материального мира, а их содержание.

В Федеральном законе от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» установлено, что объектами исследований являются вещественные доказательства, документы, предметы, животные, трупы и их части, образцы для сравнительного исследования, а также материалы дела, по которому производится судебная экспертиза, также исследование может проводиться в отношении живых лиц. Таким образом, как обоснованно считает Е.Р. Россинская, объект экспертного исследования – это просто материальный объект, содержащий информацию, необходимую для решения экспертной задачи³.

Применительно к судебно-экономической экспертизе в качестве объектов, как полагает В.А. Тимченко, следует понимать «материальные носители, содержащие регламентируемую и не регламентируемую нормативными актами информацию о фактах хозяйственной жизни в отношении средств организации и их ис-

² Князева Н.В. Совершенствование методики проведения судебной экономической экспертизы определения чистых активов организации в процессуальном поле // Бизнес в законе. Экономико-юридический журнал. 2016. № 3. С. 148.

³ Россинская Е.Р., Галышина Е.И., Зинин А.М. Теория судебной экспертизы: учебник / под ред. Е.Р. Россинской. М., 2009. С. 90.

точников, позволяющие идентифицировать лиц, составивших эти носители информации, лиц, ответственных за имевшие место факты хозяйственной жизни в отношении средств организации и их источников, а также проверить достоверность информации, содержащейся на материальных носителях»⁴.

В судебной экспертологии выделяют несколько классификаций объектов судебных экономических экспертиз. Так, А.А. Савицкий классифицирует их следующим образом: бухгалтерская (финансовая) отчетность, первичные учетные документы, регистры бухгалтерского учета, договоры на поставку товаров, работ, оказания услуг, платежные документы, иные документы (учредительные документы организации (устав, учредительный договор, решение собрания учредителей, реестр акционеров и др.), материалы проведенной инвентаризации (инвентаризационные и сличительные ведомости, акт инвентаризации) и т.п.)⁵.

М.А. Асташов с точки зрения методики производства экспертиз классифицирует объекты исследования судебно-экономической экспертизы по следующим видам:

- первичные учетные документы;
- иные первичные документы, используемые при ведении учета (договоры, составленные в письменной форме; письменная корреспонденция, раскрывающая, изменяющая или дополняющая существо операции и т.п.);
- регистры бухгалтерского учета (аналитического и синтетического);
- бухгалтерская отчетность;
- налоговая отчетность (налоговые декларации, расчеты по налогам);
- иные материалы, содержащие фактические данные (заключения экспертов других специальностей; показания подозреваемых (обвиняемых); показания свидетелей; акты документальных проверок как юридического (физического) лица, чья деятельность

⁴ Тимченко В.А. Объекты судебно-экономической экспертизы // Вестник Нижегородского университета им. Н.И. Лобачевского. 2020. № 2. С. 200–206.

⁵ Савицкий А.А. К вопросу об объектах исследования судебной экономической экспертизы // Вестник университета им. О.Е. Кутафина (МГЮА). 2019. № 5 (57). С. 105–114.

исследуется, так и его контрагентов по хозяйственным операциям; документы, неофициального учета (черновые записи и т.п.)⁶.

Приведенные классификации авторов разнятся по некоторым критериям. Так, А.А. Савицкий считает, что документы, содержащие «чужое» мнение: отчеты об оценке, заключения аудиторов, акты налоговых проверок, акты ревизии следует относить к недопустимым объектам судебной экономической экспертизы и эти объекты не могут являться основанием для выводов экспертного исследования. Также он не согласен с тем, что протоколы допроса подозреваемых (обвиняемых), свидетелей следует относить к объектам экономической экспертизы, так как объектами экспертного исследования являются исключительно документы бухгалтерского учета, непонятно, на каком основании экспертами используются не первичные и сводные документы, а протоколы допроса свидетелей, помимо этого у процессуального лица существует возможность изменить показания, что автоматически укажет на недостоверность выводов, сделанных с учетом показаний, указанных в предыдущем протоколе допроса⁷.

По нашему мнению, нельзя полностью согласиться с тем, что вышеуказанные объекты нельзя использовать при производстве судебной экономической экспертизы, так как эти документы могут содержать информацию о фактах финансово-хозяйственной деятельности организации в отношении ее средств и их источников, необходимых для исследования всех представленных объектов в совокупности с целью решения экспертных задач.

В настоящее время все больше информации о ведении бухгалтерского учета и финансово-хозяйственной деятельности организации, в том числе свидетельствующих о совершении преступлений, связанных с использованием информационных технологий, располагается на электронных носителях информации. Сами электронные носители можно отнести к объектам исследования, так как на них могут содержаться документы и материалы, относящиеся к традиционным объектам судебной экономической экспертизы.

М.Г. Нерсисян и А.И. Семикаленова отмечают большое количество автоматизированных бухгалтерских систем, которые

⁶ Астахов М.А. Особенности назначения судебно-экономической экспертизы при расследовании преступлений // Территория науки. 2013. № 6. С. 104.

⁷ Савицкий А.А. Указ. соч. С. 112.

используются при ведении бухгалтерской отчетности: «1С» (серия программ 1С: Бухгалтерия), «АйТи» (семейство «БОСС»), «Атлант-Информ» (серия «Аккорд»), «Галактика – Парус» (серия программ «Галактика» и «Парус»), «ДИЦ» («Турбо-бухгалтер»), «Интеллект-сервис» (серия «БЭСТ»), «Инфин» (серия программных продуктов от «мини» до «макси»), «Информатик» («Инфо-бухгалтер»), «Инфософт» («Интегратор»), «Омега» (серия «Abacus»), «Цифей» («Эталон») и «R-Style Software Lab» («Универсальная бухгалтерия Кирилла и Мефодия», серия RS-Balance)⁸.

Информация на электронных носителях не закреплена на законодательном уровне как объекты для исследования, поэтому в научной литературе существуют прямо противоположные мнения о том, что данный объект будет являться недопустимым для получения выводов⁹, или его необходимо использовать при производстве экономической экспертизы с целью уменьшения объема работы и сокращения сроков производства исследования¹⁰.

На наш взгляд, более оптимальной представляется позиция Е.Г. Беляковой, считающей, что документы и программы, содержащие информацию, относящуюся к традиционным объектам судебной экономической экспертизы, представленные в цифровой форме, призваны прийти на замену бумажному документообороту, ускорить и сделать более прозрачным процесс взаимодействия хозяйствующих субъектов как между собой, так и в отношениях с органами государственной власти, поэтому они будут являться объектами исследования судебно-экономической экспертизы¹¹.

⁸ *Нерсесян М.Г., Семикаленова А.И.* Проблемы производства судебных финансово-экономических экспертиз, объектом которых выступают программные продукты автоматизации бухгалтерского и финансового учета // Теория и практика судебной экспертизы. 2011. № 2 (22). С. 131.

⁹ *Савицкий А.А.* Указ. соч. С. 112.

¹⁰ *Бондарь Н.Н., Виноградова М.М.* Некоторые особенности исследования объектов судебной экономической экспертизы, в том числе документов неофициального учета и электронных документах // Теория и практика судебной экспертизы. М., 2011. № 2 (22). С. 89.

¹¹ *Белякова Е.Г.* О некоторых особенностях цифровых следов в судебной финансово-экономической экспертизе по делам о преднамеренном банкротстве юридических лиц // Цифровой след как объект судебной экспертизы: материалы Международной научно-практической конференции. М., 2020. С. 26.

В связи с этим можно отметить существование проблемы обнаружения, фиксации, изъятия и последующего исследования цифровых объектов судебной экономической экспертизы. Так, Е.Р. Россинская приводит следующий пример из своей экспертной практики: эксперту было необходимо произвести снятие информации с удаленного сервера, но он, игнорируя методические рекомендации, допустил прямое подключение к серверу. Так как эксперт обнаружил необходимые файлы без защиты от внесения изменений, система Windows внесла изменения в анализируемые данные. В результате таких действий уничтожаются цифровые следы логически стертой информации, которая могла свидетельствовать о вносимых в базу данных изменениях. Таким образом, он нарушил методику проведения исследования информации на машинных носителях, поскольку это могло повлечь за собой потерю данных, имеющих логическую пометку как удаленные, но фактически присутствующие на диске¹².

На данном примере можно сделать вывод о необходимости привлечения специалиста в области информационных технологий с целью обнаружения объектов экономической экспертизы, содержащих сведения для экспертного исследования и разрешения поставленных вопросов, которые находятся на удаленных серверах.

По мнению Е.Р. Россинской и Т.А. Саакова, участие специалиста обязательно, когда следователю требуется осуществить изъятие компьютерной и/или цифровой информации либо непосредственно с электронного носителя (персонального компьютера, мобильного телефона, электронного планшета и т.п.), либо с удаленных серверов (например, с определенного контент-сайта), а не с самого электронного устройства (системного блока персонального компьютера, ноутбука, мобильного телефона и т.п.), так как фиксация и изъятие цифровых данных предопределяет необходимость соблюдения определенного порядка действий со стороны правоприменителя, вызванного спецификой данных объектов, с целью обеспечения их сохранности, достоверности и дальнейшей возможности приобщения в качестве вещественных доказательств по делу¹³.

¹² Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета им. О.Е. Кутафина (МГЮА). 2019. № 5 (57). С. 41.

¹³ Россинская Е.Р., Сааков Т.А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 111.

Оптимальной процессуальной формой использования специальных знаний в целях поиска и обнаружения компьютерной информации в ходе расследования экономических преступлений является участие в следственном осмотре компьютерной техники специалиста в области экономики совместно со специалистом в области компьютерной техники. Первый обладает знаниями в области экономической деятельности, а второй – знаниями о способах обнаружения и изъятия информации об этой деятельности, необходимой для расследования преступлений¹⁴.

Таким образом, в настоящее время для ведения бухгалтерского учета и организации финансово-хозяйственной деятельности предприятий используются различные информационные технологии, поэтому материалы, необходимые для экспертного исследования, могут находиться на электронных носителях информации. Соответственно, объектами при проведении экономической экспертизы может служить криминалистически значимая информация на компьютерной технике, изъятая в организации. К таким объектам можно отнести автоматизированные программы, а также выделенную из них информацию, находящуюся на удаленных серверах.

В настоящее время не многие следователи могут найти необходимую криминалистически значимую информацию для проведения исследования, которая расположена на электронных носителях, поэтому существует необходимость привлечения сведущих лиц, обладающих специальными знаниями как в области экономики, так и компьютерной техники, для обнаружения, фиксации, изъятия и исследования компьютерной информации, необходимой для производства судебной экономической экспертизы.

Стоит согласиться с мнением М.Г. Нерсесян и А.И. Семикаленовой о том, что в настоящее время недостаточно разработана методическая база для исследования экономической информации, создающейся, обрабатываемой и хранящейся в различных информационно-компьютерных системах¹⁵. Поэтому разработка таких методических рекомендаций является чрезвычайно актуальной и должна проводиться с привлечением специалистов обоих направлений.

¹⁴ Антонов О.Ю., Себякин А.Г. Особенности использования специальных знаний в области экономики и компьютерной техники при расследовании экономических преступлений // Вестник Удмуртского университета. Серия экономика и право. 2017. Т. 27. Вып. 5. С. 109.

¹⁵ Нерсесян М.Г., Семикаленова А.И. Указ. соч. С. 132.

Даниил Анатольевич БОРОДИН

студент

*Санкт-Петербургский юридический институт (филиал)
Университета прокуратуры Российской Федерации*

О НЕКОТОРЫХ ФАКТОРАХ, СПОСОБСТВУЮЩИХ СОВЕРШЕНИЮ КИБЕРМОШЕННИЧЕСТВ, И ИХ ВЛИЯНИИ НА СПОСОБЫ СОВЕРШЕНИЯ ДАННЫХ ПРЕСТУПЛЕНИЙ

Аннотация. В рамках затронутой темы рассмотрен вопрос о состоянии преступности, связанной с использованием информационных технологий. Проанализированы актуальные факторы, опосредующие сложившуюся криминогенную ситуацию в данной области. Выдвинуты положения о сущности таких факторов и приведены возможные меры по противодействию электронных мошенничеств.

Ключевые слова: электронное мошенничество, информационные технологии, криптовалюта.

Daniil Anatolevich BORODIN

student

*Saint-Petersburg Law Institute (branch)
of the University of the Office of the Prosecutor of the Russian Federation*

ON SOME FACTORS PROMOTING THE COMMISSION OF «CYBER FRAUD» AND THEIR INFLUENCE ON THE WAYS OF THE COMMISSION OF THESE CRIMES

Abstract. Within the framework of the topic raised, the issue of the state of crime associated with the use of information technologies was considered. The actual factors mediating the current crime situation in this area are analyzed. Provisions on the nature of such factors are put forward and possible measures to counter electronic fraud are given.

Keywords: electronic fraud, information technology, cryptocurrency.

Бурное развитие информационных технологий, плоды которого непосредственно влияют на жизнь, без преувеличения, каждого человека, в то же время явилось и причиной не менее скоротечного появления и трансформации способов совершения преступлений, связанных с использованием таких технологий.

На это красноречиво указывает статистика МВД России: с января по сентябрь 2020 г. количество зарегистрированных преступлений, совершенных с использованием информационно-комму-

никационных технологий или в сфере компьютерной информации, увеличилось на 77 % по сравнению с аналогичным периодом 2019 г. и составило 363 034¹. Пандемия, вероятно, выступила неким катализатором совершения преступлений данного рода, побуждая преступников использовать ее неблагоприятные последствия для более успешного совершения преступлений.

Вместе с тем информационные технологии продолжают совершенствоваться, появились новые факторы, опосредующие трансформацию некоторых способов совершения преступлений. Действие таких факторов имеет комплексное воздействие, непосредственно способствуя совершению преступлений в сфере информационных технологий в целом и электронных мошенничеств в частности, что осложняет осуществление расследования таких преступлений. К таким факторам относятся следующие.

1. Появление криптовалют. Криптовалюты в современном их понимании с присущими им свойствами анонимности, децентрализованности, использования технологии блокчейн, консенсусного реестра и т.д.² появились в 2009 г. с разработкой платежной системы «Биткойн». Впоследствии как «биткойн», так и ряд «альткойнов» приобрели большую популярность, о чем, как минимум, свидетельствует стоимость одного «биткойна» на мировом финансовом рынке в период своего исторического максимума – 20 089 долл.³ Криптографические методы, используемые при создании механизма генерации «адреса» криптовалюты, делают возможность полной анонимности участников транзакций – в системе нет никакой информации о владельце адреса и даже о самом факте создания адреса. В результате практически невозможно установить, кому принадлежит «биткойн-кошелек».

Такие свойства сделали криптовалюты центральным средством платежа на черных онлайн-рынках, специализирующихся на неле-

¹ Состояние преступности в России за январь-сентябрь 2020 года // Министерство внутренних дел Российской Федерации. ФКУ «Главный информационно-аналитический центр». М., 2020. С. 30.

² Лагутенков А. Криптовалюты. Правила применения // Наука и жизнь. 2018. № 2. С. 22–26.

³ Биткойн график курсов за всю историю с 2008 по 2020 гг. URL: <https://bytwork.com/articles/btc-chart-history> (дата обращения: 03.11.2020).

гальной продаже оружия, наркотических средств и психотропных веществ и т.д. Стоит отметить, что большинство таких рынков работает на системе прокси-серверов, позволяющих устанавливать анонимное сетевое соединение, под названием «Тог»⁴.

Проведение финансовых операций с криптовалютами при совершении преступлений имеет цель обеспечить конспирацию преступных действий, что отчетливо видно при ознакомлении с судебной практикой.

Так Г., узнав через Интернет о том, что гражданин РФ является потерпевшим по уголовному делу, имеющему широкий общественный резонанс на территории РФ, и дает показания о совершении противоправных действий высокопоставленным сотрудником МВД России, решил путем обмана похитить денежные средства в особо крупном размере. Для конспирации своих преступных действий Г. зарегистрировал «биткойн-кошелек», на который потребовал от потерпевшего перевести криптовалюту «биткойн», эквивалентную 50 тыс. долл., за предоставление информации о якобы планируемом убийстве последнего⁵.

2. Хранение персональных данных и ключи шифрования. В научной литературе можно встретить мнение о наличии проблемы в виде слабой коммуникации между правоохранительными органами и операторами связи, компаниями, владеющими социальными сетями и другими операторами персональных данных⁶. Но одно дело, когда такие компании находятся в юрисдикции РФ, и совсем другое, когда они представлены иностранными технологическими гигантами наподобие Google и Facebook. Запрос значимой для расследования уголовного дела информации при таком положении дел становится еще более труднореализуемым.

В связи с этим в Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Федеральный закон от 27 июля

⁴ Подробнее см.: *Dingledine R., Mathewson N., Syverson Naval Tor P.* Луковский маршрутизатор второго поколения / пер. А. Абакумкина и Р. Инфлянскаса. М., 2014.

⁵ Приговор Калининского районного суда г. Чебоксары от 6 февраля 2018 г. по делу № 1-46/2018 // Судебные и нормативные акты РФ. URL: <https://sudact.ru> (дата обращения: 03.11.2020).

⁶ *Гончар В.В.* Совершенствование расследования преступлений в сфере информационных технологий // Эпоха науки. 2017. № 11. С. 28.

2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в июле 2014 г. законодателем приняты поправки, согласно которым лица, подпадающие под действие Федерального закона «О персональных данных», обязаны обеспечить условия, при которых любые операции с персональными данными гражданами России будут осуществляться с использованием баз данных, находящихся на территории РФ.

Кроме того, в конце 2019 г. приняты изменения в ст. 13.11 КоАП РФ, предусматривающие введение ответственности за невыполнение вышеуказанной обязанности, причем штраф за повторное совершение административного правонарушения, предусмотренного ч. 8 ст. 13.11 КоАП РФ может достигать восемнадцати миллионов рублей⁷.

Очевидно, что указанные изменения не принесут мгновенного результата в виде перенесения части серверов иностранных компаний, осуществляющих обработку персональных данных граждан РФ, и создания иных условий для такой обработки именно на территории России. Однако это лишь одни из первых шагов, направленных, в том числе, и на более эффективное расследование преступлений в сфере информационных технологий.

Следует обозначить и сложности, возникающие по причине непредставления ключей шифрования как иностранными компаниями, так и некоторыми отечественными.

Отказ передать правоохранительным органам ключи шифрования был одной из главных причин блокировки сервиса Telegram на территории России. Наличие ключей шифрования существенно повышает скорость расследования правоохранительными органами преступлений в сфере информационных технологий, а в определенных случаях и просто опосредует возможность их расследования. Однако при разрешении данной проблемы необходимо учитывать и мнение ИТ-компаний, поскольку ряд пользователей отказываются от услуг сервиса, если понимают, что их приватность может быть нарушена. При решении как данной, так и других затронутых в работе

⁷ Федеральный закон от 2 декабря 2019 г. № 405-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/> (дата обращения: 23.09.2020).

проблем необходимо находить некий баланс интересов – публичных и частных, что требует тщательного анализа принимаемых на законодательном уровне решений в данной сфере.

3. Утечки персональных данных. Для совершения кибермошенничества злоумышленникам необходима информация о потенциальном пострадавшем, например, его фамилия, имя, отчество, номер мобильного телефона, данные банковской карты или данные о программном обеспечении, а если преступление направлено на организацию, государственный орган, то необходимы сведения о сотрудниках организации и т.д. Большое количество физических лиц чуть ли не ежедневно предоставляют свои персональные данные различным коммерческим организациям при использовании электронных сервисов и приложений. При этом не редки случаи, когда целые базы данных о клиентах организации становятся доступны для широкого круга лиц из-за «утечек» персональных данных.

В августе 2020 г. Центральный банк России и платежная система Visa предупредили кредитные организации об утечке данных 55 тыс. карт⁸. Помимо самих данных карт, в открытом доступе находились данные о фамилии, имени, отчестве, адресе электронной почты и даже месте жительства клиентов сервиса Joom. Вероятно, что ставшие доступными данные могут быть использованы злоумышленниками для совершения мошенничеств с применением методов социальной инженерии. Во избежание использования персональных данных для совершения преступлений операторам их обработки необходимо особенно внимательно подходить к вопросам обеспечения собственной информационной безопасности.

Так, лицо приискало для реализации преступного умысла ряд других лиц, распределив между ними преступные роли. При этом один из участников группы неустановленным образом получал сведения о реквизитах банковских карт, наличии денежных средств на счетах данных карт и их владельцах. Именно наличие таких сведений позволило преступной группе путем обмана, направленного на хищение чужого имущества, осуществить телефонный

⁸ Чернышова Е. ЦБ и Visa предупредили банки об утечке данных 55 тыс. карт // РБК. 2020. URL: <https://www.rbc.ru/finances/27/08/2020/5f468fa59a7947858f2c197e?> (дата обращения: 03.11.2020).

звонок на телефонный номер потерпевшей и сообщить ей ложные сведения о попытках хищения денежных средств с ее банковского счета, представившись сотрудниками службы безопасности банка. Потерпевшая выполнила действия, указанные ей неустановленными лицами, действующими от имени представителей банка, в результате чего участники преступной группы получили возможность путем обмана распорядиться похищенными денежными средствами по своему усмотрению⁹.

4. Развитие инструментов социальной инженерии. Данный фактор требует пристального рассмотрения сразу по двум причинам:

- в отличие от подавляющего большинства других он имеет не техническую, а психологическую основу;
- он стал особенно актуален в реалиях периода борьбы общества с негативными последствиями распространения инфекции COVID-19.

Под социальной инженерией в области информационной безопасности понимается «метод получения необходимого доступа к информации, основанный на особенностях психологии людей»¹⁰. Использование методов социальной инженерии злоумышленниками особенно актуализировалось в связи с пандемией инфекции COVID-19: общая психологическая напряженность, необходимость граждан в дополнительных денежных средствах на покрытие возникших расходов – эти и другие факторы используются преступниками, прежде всего, для завладения денежными средствами потерпевших. Рассмотрим примеры применения методов социальной инженерии в период пандемии.

1. Взлом аккаунтов социальных сетей известных личностей. Данный пример показывает комплексность применения способов совершения преступлений в сфере информационных технологий, вызывающих особую сложность как в плане их предотвращения, так и расследования. В июле 2020 г. «хакеры» подкупили сотрудника социальной сети Twitter, чтобы получить доступ к аккаунтам из-

⁹ Постановление Домодедовского городского суда Московской области от 9 января 2020 г. по делу № 1-85/2020 // Судебные и нормативные акты РФ : сайт. URL: <https://sudact.ru> (дата обращения: 03.11.2020).

¹⁰ Казыханов А.А., Байрушин Ф.Т. К вопросу о социальной инженерии // Символ науки. 2016. № 11-3. С. 79.

вестных личностей, таких как Билл Гейтс, Илон Маск, Барак Обама и др. Используя служебные инструменты Twitter, «хакерам» удалось поменять адреса электронной почты, прикрепленные к аккаунтам. В аккаунтах появились отправленные «хакерами» сообщения, в которых известные личности якобы организуют раздачу денежных средств из-за пандемии. Пользователям предлагалось отправить на указанный в сообщении адрес «биткойн-кошелек» любое их количество с обещанием вернуть их в удвоенном размере, и в течение нескольких часов на эти электронные кошельки были перечислены более 110 тыс. долл.¹¹. Комплексное применение технических приемов и методов социальной инженерии обеспечило достижение злоумышленниками преступного результата и позволило на данный момент оставаться безнаказанными.

2. Использование функций рекламы в социальных сервисах. Практически все социальные сервисы предоставляют возможность продвигать создаваемую пользователями информацию (видеоролики, публикации и т.д.) посредством использования рекламных функций сервиса. Однако указанная функция используется и злоумышленниками для рекламирования публикаций, в которых они призывают пользователей совершить определенные действия, в результате которых злоумышленники путем обмана смогут завладеть денежными средствами пострадавших.

В одном из таких видеороликов в сервисе Youtube сначала транслируются отрывки из выступлений действующих государственных деятелей РФ, в которых они говорят об экономическом положении дел, связанном с пандемией инфекции COVID-19, и необходимости выплаты от лица государства стимулирующих выплат. Фрагменты выступлений монтируются таким образом, чтобы пользователь не смог понять о каких именно выплатах, кому и в каких размерах идет речь. Если обратиться к полной записи выступления, то сразу становится понятно, что имеются в виду стимулирующие выплаты медикам, работающим с больными COVID-19 в период пандемии. Затем авторы видео обещают, что каждому гражданину

¹¹ *Тадтаев Г.* Хакеры сообщили СМИ детали взлома аккаунтов в Twitter // РБК. 2020. URL: https://www.rbc.ru/technology_and_media/16/07/2020/5f100f219a7947afa17c6c91 (дата обращения: 03.11.2020).

России полагается выплата в размере до 300 тыс. руб., нужно всего лишь зайти на сайт «Единого компенсационного центра», в котором можно вернуть уплаченный налог на добавленную стоимость. Далее пользователя просят ввести свои личные данные, данные наиболее часто используемой банковской карты, после чего якобы производится расчет положенной компенсации на основе информации «официальных баз данных». Для получения же самой выплаты необходимо предварительно дважды оплатить консультационные услуги юриста, который дистанционно помогает с заполнением заявления. В конце видеоролика отображается, что автор ролика, подав заявление на указанном сайте, якобы получил выплату в сумме около 200 тыс. руб. Очевидно, что транслирование получения суммы является постановочным.

Применяя методы социальной инженерии, путем использования фрагментов из выступлений государственных деятелей, пытаюсь тем самым придать «официальность» размещаемой информации, а также негативные последствия пандемии как основу для якобы предоставляемого возврата налога на добавленную стоимость, злоумышленники пытаются путем обмана завладеть денежными средствами пользователей сервиса.

3. Мошенничество с использованием предварительно одобренных кредитов. Развитие инструментов дистанционного предоставления банковских услуг действительно упростило взаимодействие клиентов и банка – теперь оформить кредит можно сразу в специализированном мобильном приложении или на официальном Интернет-сайте банка. Более того, на сайтах некоторых банков, зная фамилию, имя, отчество и номер телефона клиента, можно сразу узнать, кредит в каком размере ему может быть предоставлен. Как раз этим и решили воспользоваться мошенники, задействовав при этом методы социальной инженерии.

Ранее упоминалась проблема утечки персональных данных. Для совершения указанного преступления используется минимальный объем информации: фамилия, имя, отчество, номер телефона и банк, в котором у клиента есть счет. Мошенники звонят клиентам банка, представляясь банковскими сотрудниками, зачастую пользуясь программой по подмене номера исходящего вызова, чтобы не вызвать подозрений. Они говорят, что клиенту в данный момент одобрен кредит, и он находится в стадии оформления. Как только клиент банка

говорит, что он не оформлял никакой кредит, мошенники настаивают на установке специального приложения, которое якобы защитит клиента. На самом же деле установленное приложение предоставляет мошенникам удаленный доступ к мобильному телефону клиента банка, после чего с помощью такого доступа уже в официальном приложении банка берется кредит. После оформления кредита мошенники убеждают пострадавших перевести деньги на «защитный» счет банка, чтобы уберечь деньги от мошенников, в результате чего реализуют свой преступный умысел на хищение денежных средств. В иных случаях, помимо мошенников под видом сотрудников банка, потерпевшим также звонят мошенники с подменного номера МВД России под видом сотрудников полиции, которые также убеждают клиента перевести деньги на «защитный» счет банка. Способом хищения в таком случае выступает обман в виде сообщения заведомо ложных сведений «с целью введения в заблуждение лица, в собственности или владении которого находится имущество, чтобы таким образом добиться от него «добровольной» передачи имущества в пользу обманщика или других лиц»¹².

Вероятно, количество совершаемых электронных мошенничеств, в частности в связи с дальнейшим осложнением эпидемиологической ситуации, лишь увеличится. В связи с этим необходимо обозначить возможные меры по противодействию совершению данного вида преступлений.

Для этого необходимо еще раз подчеркнуть, что факторы, способствующие совершению кибермошенничеств, имеют под собой разные основания: технические и психологические. Соответственно, преодоление технических факторов требует дальнейшего развития материально-технической и технологической базы правоохранительных органов, осуществления поддержки развития отечественных ИТ-компаний, специализирующихся на обеспечении информационной безопасности, совершенствования законодательной базы в части определения правового статуса криптовалют и реализации иных мер.

¹² Цит. по: Научно-практический комментарий к постановлению Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» / Д.А. Безбородов, А.В. Зарубин, Р.М. Кравченко [и др.]. СПб., 2020. С. 6–7.

В то время как фактор в виде появления новых методов социальной инженерии имеет под собой психологическую основу, а, значит, приоритетные меры по нивелированию действия данного фактора будет состоять в профилактических мерах, в частности информировании населения о наиболее типичных способах электронных мошенничеств, предупреждения о потенциальной опасности передачи персональных данных третьим лицам посредством публикаций в СМИ, размещения социальной рекламы, а также информации самими кредитно-финансовыми учреждениями, что направленно на повышение осведомленности людей в области информационной безопасности.

Мария Олеговна БРЕНЕВА

студент

Институт права и национальной безопасности

Тамбовского государственного университета им. Г.Р. Державина

О НЕКОТОРЫХ ОСОБЕННОСТЯХ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТКОЙ НАПРАВЛЕННОСТИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ

Аннотация. Статья посвящена рассмотрению особенностей совершения преступлений экстремистского характера, совершенных посредством глобальной телекоммуникационной сети Интернет. Автор формулируется общая характеристика преступлений экстремистской направленности, совершаемых с использованием сети Интернет. Также проводится уголовно-правовой анализ публичных призывов к осуществлению экстремистской деятельности, результат которого отражается в приведенной автором статистике.

Ключевые слова: преступления экстремистской направленности, телекоммуникационная сеть, экстремистское сообщество, публичный призыв.

Maria Olegovna BRENEVA

student

Institute of Law and National Security

of Tambov State University named after G.R. Derzhavin

ABOUT SOME FEATURES OF COMMISSION OF CRIMES OF AN EXTREMIST ORIENTATION WITH USE OF THE TELECOMMUNICATIONS NETWORK INTERNET

Abstract. The article deals with the peculiarities of committing extremist crimes committed through the global telecommunications network Internet. The author formulates such concepts as computer information and telecommunications network. In addition, the article contains a General description of extremist crimes committed using the Internet. The criminal law analysis of public calls to carry out extremist activities is also carried out, the result of which is reflected in the statistics provided by the author.

Keywords: crimes of the extremist direction, a telecommunication network, an extremist community, a public call.

Проблема противодействия экстремизму на сегодняшний день имеет ярко выраженную актуальность. В свете последних новостей довольно часто можно слышать о постоянно создающихся террористических группировках, о различных формах проявления

экстремистской деятельности, среди которых отмечаются такие как национализм, ксенофобия и иные формы притеснения прав и законных интересов людей по каким-либо признакам.

На сегодняшний день особая опасность экстремизма обусловлена тем, что такие преступления все чаще совершаются посредством глобальной сети Интернет, обладающей чертами открытости и отсутствия цензуры размещаемых материалов.

Реализация преступного умысла экстремистов на такой информационной платформе несет в себе большую угрозу, поскольку Интернет обладает рядом преимуществ, которые злоумышленники используют в преступных целях. Среди данных характеристик стоит назвать такие как широкий охват аудитории, возможность анонимного размещения информации, свободный доступ и высокая скорость распространения экстремистского материала, наличие различных хакер-программ, позволяющие обходить процедуру обработки на безопасность вбрасываемого в Интернет материала, что способствует свободной пропаганде сепаратизма и других форм экстремизма¹, широкая распространенность в географической плоскости, которая дает возможность сохранять контакт на больших расстояниях, что преобразовывает процедуры обсуждения, планирования и координирования будущих акций в достаточно скрытый режим.

С учетом перечисленных фактов, экстремистские группировки видят в данной информационной платформе идеальный инструмент, при помощи которого экстремистские и террористические организации, радикально настроенные на смещение установленного государством правопорядка, осуществляют вербовку молодежи для реализации своей идеологии, носящей экстремистский характер.

Распространение преимущественно молодежного экстремизма в интернете сегодня является острой проблемой, беспокоящей мирных граждан. День за днем увеличивается число преступлений данного характера, безостановочно растет уровень насилия, экстремизм переходит в профессиональную жестокую деятельность, которой подвергаются огромные массы людей.

«Идеологи экстремизма, учитывая потенциал и коммуникативные преимущества Интернета, видят в нем некую виртуальную

¹ Кубякин Е.О. Основания социологического обоснования феномена экстремизма. Экстремпарантность. Краснодар, 2014. С. 76.

площадку, скрытый характер которой значительно усложняет работу при расследовании преступлений экстремистской направленности»².

Сегодня экстремизм, осуществляемый посредством распространения вредоносных материалов, является масштабной проблемой, угроза которой распространяется на информационную безопасность как общественных структур в частности, так и государственного аппарата в целом. Важно понимать, что экстремистская идеология, распространяемая в сети Интернет, – это большая проблема общегосударственного значения, представляющая масштабную угрозу для национальной безопасности страны, несвоевременное решение которой может привести к разрушительным последствиям, как в рамках конкретного государства, так и для всего цивилизованного мира.

В связи с этим анализ и характеристика системы преступлений, связанных с осуществлением экстремистской деятельности с использованием Интернета видится как никогда актуальным и требует детального и всестороннего обзора.

На сегодняшний день в действующем уголовном законодательстве содержится ряд норм, предусматривающих ответственность за совершение преступлений экстремистского характера: ст. 280 «Публичные призывы к осуществлению экстремистской деятельности», ст. 280¹ «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации», ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства», ст. 282¹ «Организация экстремистского сообщества», ст. 282² «Организация деятельности экстремистской организации» УК РФ.

Поскольку конструкция диспозиций перечисленных статей является бланкетной, для полного понимания используемого понятия обратимся к Федеральному закону от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности», в котором закреплено, что экстремистская деятельность – это деятельность общественных и религиозных объединений, либо иных организаций, либо средств массовой информации, либо физических лиц по пла-

² *Валеев А.Х.* Проявление экстремизма в сети интернет // Бизнес в законе. Экономико-юридический журнал. 2011. № 6. С. 125.

нированию, организации, подготовке и совершению действий, направленных на насильственное изменение основ конституционного строя и нарушение целостности РФ, подрыв безопасности РФ, захват или присвоение властных полномочий, создание незаконных вооруженных формирований, осуществление террористической деятельности, возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию. Как правило, проявления экстремизма носят публичный характер, нацелены на общественность, откуда вытекает такой признак экстремизма как социальность.

Отметим, что, несмотря на принимаемые правоохранительными органами усиленные меры, направленные на пресечение экстремистской деятельности, число такого характера преступлений неуклонно растет. Сегодня экстремизм – это не просто посягательство на общественные отношения. Он характеризуется интенсивностью, жестокостью, разнообразностью форм его проявления, что представляет собой острую проблему глобального масштаба.

Особую значимость в контексте постановки проблемы данного исследования имеет осуществление экстремистской деятельности с использованием Интернета, а потому, с учетом изложенных характеристик норм уголовного закона, рассмотрим подробнее составы преступлений, объективная сторона которых сосредоточена на реализации преступных действий при помощи Интернета.

Так, предусмотренные ч. 2 ст. 280 УК РФ публичные призывы к осуществлению экстремистской деятельности, совершенные с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети Интернет, являются одним из распространенных преступлений, совершаемых экстремистами. Востребованность данной информационной площадки в преступных целях обоснована свободным доступом к Интернету, а также усложненным механизмом раскрытия и выявления такого рода преступлений.

Под призывом стоит понимать воздействие на сознание, поведение, мнение и волю людей, осуществляемое, прежде всего, в целях побудить человека к совершению конкретных действий либо же воздержаться от таковых. Экстремистские течения, оперируя всем арсеналом возможностей сети Интернет, пропагандируют

идеи осуществления действий экстремистской направленности, при этом подача призывной информации, их высказывания, порядок изложения идеологической позиции не имеют единой формы и носят самый различный характер.

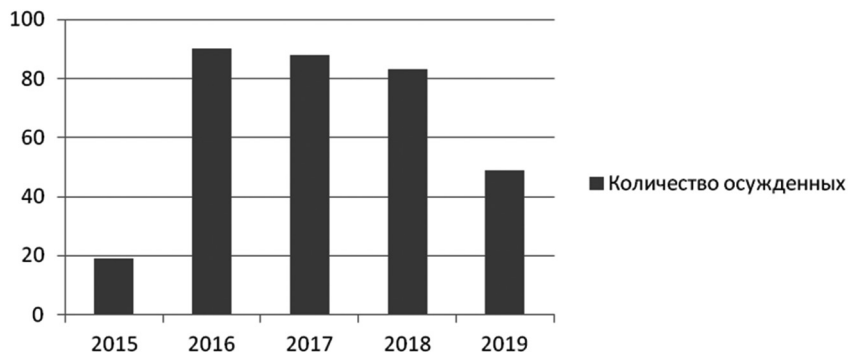
Публичность призывов к осуществлению экстремистской деятельности выражается в обращении к широкой аудитории, в данном случае ко всем пользователям сети Интернет, и имеет главной целью вовлечь как можно больше людей в экстремистское сообщество. Повторимся, что состав данного преступления носит формальный характер, что означает окончание преступления с момента публичного призыва посредством сети Интернет: репост или опубликование экстремистского материала в формате фото или видео документа, и не важно, была ли подвержена экстремистской идеологии и Интернет-аудитория в результате данного призыва или же отнеслась к ней равнодушно.

Использование Интернета в контексте публичного призыва к экстремистской деятельности регламентировано ч. 2 ст. 280 УК РФ, предусматривающей повышенную опасность преступного деяния. Почему законодатель выделяет те же деяния, предусмотренные ч. 1 ст. 280 УК РФ, в отдельную часть и акцентирует внимание на повышенной опасности публичного призыва с использованием такой информационной площадки, как Интернет?

Отвечая на поставленный вопрос, необходимо принимать во внимание некоторые характеристики, которыми обладает сеть Интернет. С позиции граждан – это большие преимущества данной сети, а с точки зрения мышления экстремистского течения – слабые стороны, которые преобразуют данную информационную площадку в благоприятное место, пригодное для свободной и крупномасштабной экстремистской деятельности. В связи с этим уголовный закон выделяет данное преступное посягательство в отдельную часть, обозначает его особую опасность.

Динамику совершаемого преступления, предусмотренного ч. 2 ст. 280 УК РФ, можно отследить на основе приведенных в диаграмме статистических данных³.

³ Судебный департамент при Верховном суде Российской Федерации: официальный сайт. URL: <http://www.cdep.ru/index.php?id=79> (дата обращения: 27.10.2020).



**Рисунок 1. Количество осужденных по ч. 2 ст. 280 УК РФ
«Публичные призывы к осуществлению
экстремистской деятельности»**

На основе анализа статистических данных отметим, что динамика совершения преступления, предусмотренного ч. 2 ст. 280 УК РФ, постепенно снижается. Сравнивая показатели, отмеченные в 2018 и 2019 гг., видим, что количество осужденных сократилось почти в два раза. Государство в лице правоохранительных органов должно на регулярной основе проводить профилактические меры, направленные на минимизацию совершения рассматриваемого преступного деяния, что благоприятно скажется на общественной безопасности.

Максим Владимирович ВИНОКУРОВ

аспирант

*Университет прокуратуры Российской Федерации;
помощник прокурора Куйбышевского района г. Иркутск*

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ФАЛЬСИФИЦИРОВАННЫХ, НЕДОБРОКАЧЕСТВЕННЫХ И НЕЗАРЕГИСТРИРОВАННЫХ СРЕДСТВ И МЕДИЦИНСКИХ ИЗДЕЛИЙ

Аннотация. В статье исследованы современные методы использования информационных технологий в целях противодействия распространению фальсифицированных лекарств и проанализирована их эффективность. Предложены методы по улучшению качества противодействия распространению фальсифицированных лекарств при использовании информационных технологий. Поднята проблема отсутствия методов использования информационных технологий при обращении медицинских изделий и биологически активных добавок.

Ключевые слова: фальсифицированные, недоброкачественные, лекарственные средства, медицинские изделия, противодействие, информационные технологии.

Maxim Vladimirovich VINOKUROV

postgraduate student

*University of the Prosecutor's Office of the Russian Federation;
assistant prosecutor of the Kuibyshevsky district of Irkutsk*

USE OF INFORMATION TECHNOLOGIES TO COUNTERACT THE SPREAD OF COUNTERFEIT, SUBSTANDARD AND UNREGISTERED MEDICINES AND MEDICAL DEVICES

Abstract. The article examines modern methods of using information technology to counter the spread of counterfeit drugs and analyzes their effectiveness. Methods for improving the quality of countering the spread of counterfeit drugs using information technologies are proposed. The problem of the lack of methods of using information technologies in the circulation of medical devices and biologically active additives is raised.

Keywords: counterfeit, substandard, medicines, medical devices, counteraction, information technology.

Когда речь заходит о болезни, первое что приходит в голову каждого человека – это каким образом и с помощью чего ее вылечить.

Трудно представить лечение какого-либо недуга без использования лекарственных средств. Но бывают случаи, когда лекарства не помогают, поскольку являются фальсифицированными или недоброкачественными.

Попасть в ситуацию использования фальсифицированных лекарств не хочется никому, поэтому все желают, чтоб государственные органы разработали и ввели универсальную систему отслеживания качества лекарственных средств.

Первые меры по внедрению такой системы органы власти начали принимать после поручения Президента РФ от 4 февраля 2015 г. № Пр-285. В 2015 г. разработана концепция «Федеральная государственная информационная система мониторинга движения лекарственных препаратов от производителя до конечного потребителя» (далее ФГИС МДЛП).

Постановлением Правительства РФ от 31 декабря 2019 г. № 1954 предусмотрено поэтапное внедрение системы мониторинга до 1 июля 2020 г. В настоящее время указанная программа успешно запущена на всей территории РФ.

Порядок нанесения средств идентификации и внесения в систему информации о движении лекарственных препаратов указан в положении «О системе мониторинга движения лекарственных препаратов для медицинского применения», утвержденном постановлением Правительства РФ от 14 декабря 2018 г. № 1556.

Для реализации маркировки и прослеживаемости лекарств разработана информационная система мониторинга движения лекарственных препаратов (ИС МДЛП) для медицинского применения, оператором которой с 1 ноября 2018 г. является Центр развития перспективных технологий (ЦРПТ)¹.

Продвигается указанная система под брендом национальной системы цифровой маркировки «Честный знак». Оператором системы разработан сайт и одноименное приложение для проверки маркировки с помощью смартфона.

В настоящее время для отслеживания движения лекарственных препаратов на каждую вторичную (потребительскую) упаковку лекарственного препарата, произведенного после 1 июля 2020 г.

¹ URL: https://xn--80ajghhoc2aj1c8b.xn--p1ai/business/projects/medicines/medicines_traceability/ (дата обращения: 10.11.2020).

в обязательном порядке должен быть нанесен код маркировки Data Matrix. Также кодом Data Matrix должны быть промаркированы все ввезенные из-за границы лекарственные препараты.

После формирования партии и ее отгрузки дистрибьютору, производитель обязан сформировать сведения о наименовании и количестве лекарственных препаратов и выгрузить данные сведения в базу данных. В свою очередь дистрибьютор должен отметить данные о получении указанных лекарственных препаратов. И только после проверки системой соответствия представленных данных дистрибьютор сможет дальше реализовывать лекарственные препараты. Дальнейшая цепочка реализации через посредников строится таким же образом вплоть до конечной аптеки или больницы.

При реализации лекарственного препарата конечному потребителю информация о его реализации заносится в базу данных. После выбытия (использование в больнице, выдача по рецепту, продажа покупателю) лекарственных препаратов, сведения о них выбывают из системы.

Такой подход позволяет не только контролировать подлинность лекарств, но и обладать сведениями о количестве тех или иных лекарств в какой-либо области, и размерах их продажи. Оборот незарегистрированных лекарственных препаратов в таком случае полностью уйдет в теневой рынок, поскольку аптеки не смогут реализовывать такие товары, что имеет существенное значение при осуществлении противодействия распространению фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств.

В рамках разработки концепции ФГИС МДЛП предполагалось, что на каждую пачку лекарственного препарата будет наноситься уникальный идентификационный код, позволяющий отслеживать движение данной пачки от производителя через всех посредников и аптеки до конечного потребителя. Такой подход обеспечил бы полное отслеживание каждой пачки лекарственного препарата и полностью исключил бы шанс приобретения фальсифицированного препарата при условии проверки маркировки.

Практика использования маркировки свидетельствует о том, что при считывании кода Data Matrix приложение показывает сведения о подлинности кода, наименовании товара, срока годности, текущего состояния реализации, описания, серии и производителя. Таким образом, код Data Matrix формируется и наносится для опре-

деленной партии лекарственных препаратов. То есть одинаковый код может быть нанесен на несколько пачек одной партии. Очевидно такой подход связан с технической сложностью маркировки каждой пачки лекарственного препарата уникальным кодом.

Именно тут и возникают первые проблемы в противодействии распространению фальсифицированных лекарственных средств. Лица, занимающиеся фальсификацией лекарственных средств, имеют возможность скопировать Data Matrix, распечатать его на ярлыках, наклеить на упаковку, либо распечатать прямо на упаковку, и сканер будет показывать, что данный товар соответствует качеству. Проверить указанный способ можно легко, сфотографировав код Data Matrix на один телефон и отсканировав его другим.

В условиях пандемии, которая имеет место в настоящее время, а также недостатка лекарств и высокого спроса на них таким образом можно реализовать более тысячи пачек, выдавая их за одну партию. К примеру, препарат «Арепливир» можно будет приобрести в аптеках за 12 320 руб.² Из нехитрого подсчета следует, что, реализовав тысячу пачек указанного препарата, недобросовестные граждане (преступники) смогут получить более 12 млн руб. Указанная сумма многим покажется стоящей того, чтобы разобраться в том, каким образом изготовить аналогичную пачку и разместить на ней код Data Matrix.

Самое негативное заключается в том, что при проверке указанных лекарственных препаратов потребителем приложение покажет, что лекарственный препарат является подлинным и относится к определенной партии лекарственного препарата. Увидеть, что не стоит покупать лекарственный препарат, потребитель сможет только в том случае, когда информация о фальсификации станет известна и партию снимут с продажи. С учетом того, что препараты действуют на всех по-разному, многие потребители даже не поймут, что принимали фальсификат, следовательно, забьют тревогу не сразу. О том, что упаковка фальсифицированного лекарственного средства отличается от оригинальной, определяют не сразу даже контролирующие органы.

При проверках аптек и мест хранения лекарственных препаратов, становится очевидным, что выявленные без маркировки лекарства, реализуются с нарушением действующего законодатель-

² URL: <https://iz.ru/1062557/2020-09-18/nazvana-rekomendovannaia-icena-rossiiskogo-preparata-ot-koronavirusa> (дата обращения: 10.11.2020).

ства, либо произведены до 1 июля 2020 г. С учетом ограниченного срока годности лекарств, к концу 2022 г. лекарственные препараты без маркировки кодом Data Matrix исчезнут с прилавков.

Интересным и закономерным представляется тот факт, что законом не оговорена ответственность за подделку кода Data Matrix, и возникает, соответственно, вопрос – можно ли такую подделку приравнивать к фальсификации лекарственных средств? Поскольку оригинальный препарат и так получит возможность официального нанесения кода Data Matrix, то необходимость в его подделке возникнет только в том случае, если выдаваемое за лекарственный препарат средство является фальсифицированным.

Вместе с тем изготовление поддельного кода Data Matrix свидетельствует о подделке первичной упаковки и (или) вторичной (потребительской) упаковки лекарственного препарата, следовательно, такие действия должны охватываться квалификацией по ч. 2 ст. 327² УК РФ.

Также необходимо не забывать про сбои, которые периодически могут возникать в системе, когда случайно нанесли код от другой партии или другого лекарства. При таких ситуациях ответственность по нормам УК РФ возникать не должна. При этом следует учесть, что партия со случайно нанесенным неверным кодом должна быть возвращена еще при получении дистрибьютером или аптекой и до потребителя дойти не должна, поскольку информация в кодах должна совпадать с товарной накладной, а значит и самим лекарством.

Следовательно, если лекарство с неверным кодом Data Matrix реализуется в аптеке, то это фальсифицированное лекарственное средство. Значит, его продажа должна преследоваться по ст. 6.33 КоАП РФ или ст. 238¹ УК РФ в зависимости от объема, по совокупности с ч. 2 ст. 327² УК РФ.

Одновременно продажа лекарственного препарата без кода Data Matrix не образует состава уголовно наказуемого деяния, а квалифицируется по ст. 15.12 КоАП РФ. Также необходимо отметить, что хранящиеся с нарушением правил оборота лекарственные средства подлежат безусловному изъятию и, возможно, последующей проверке качества.

В настоящее время система МДЛП позволит устранить фальсификацию лекарственных препаратов в масштабах серийного производства и затруднит реализацию фальсифицированных

лекарственных препаратов внутри отдельных партий, но не сможет ее полностью устранить.

В целом указанные способы мониторинга движения лекарственных препаратов упрощают поиск фальсифицированных лекарств и позволяют контролирующим органам более эффективно их выявлять, следовательно, указанная система способствует противодействию оборота фальсифицированных лекарственных средств.

Вместе с тем описанная в настоящей статье система позволяет отслеживать только лекарственные препараты, не охватывая прочие лекарственные средства, а также медицинские изделия и биологически активные добавки.

В настоящее время национальной системой маркировки «Честный знак» в обязательном порядке маркируются такие товары как шубы, табак, обувь, лекарственные препараты³. До конца 2020 г. вводится обязательная маркировка фотоаппаратуры и шин.

Такой подход к выбору товаров представляется странным, поскольку приоритеты общественной значимости товаров, по нашему мнению, расставлены неверно. О том, когда планируется ввести обязательную маркировку медицинских изделий и биологически активных добавок официальными источниками не сообщается.

Отсутствие обязательной маркировки на биологически активных добавках позволит недобросовестным продавцам реализовывать незарегистрированные лекарственные средства под видом БАДов.

В целях повышения качества работы системы по выявлению фальсифицированных лекарств предлагается разработать и внедрить техническую возможность индивидуальной маркировки каждой пачки лекарственных препаратов. Также предлагается среди сведений, доступных потребителю, отображать сведения о том, в какую конкретно аптеку или сеть поступила проверяемая пачка или партия лекарственных препаратов. В целях предотвращения реализации фальсифицированных, недобросовестных и незарегистрированных медицинских изделий и биологически активных добавок необходимо принять меры к обязательной их маркировке.

³ URL: <https://xn--80ajghhoc2aj1c8b.xn--p1ai/potrebityam/tovari-s-markirovkoj> (дата обращения: 10.11.2020).

Кира Владимировна ВОРЫШЕВА
Данила Михайлович ПОДСВЕТОВ

студенты

*Санкт-Петербургский юридический институт (филиал)
Университета прокуратуры Российской Федерации*

ПРОИЗВОДСТВО СЛЕДСТВЕННЫХ ДЕЙСТВИЙ, ПРЕДПОЛАГАЮЩИХ РАБОТУ С ЭЛЕКТРОННЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ: НЕКОТОРЫЕ ПРОБЛЕМНЫЕ АСПЕКТЫ

Аннотация. В статье рассматриваются проблемы, возникающие при производстве следственных действий с электронными носителями информации. Анализируя действующее законодательство и научную литературу по проблематике исследования, авторами делается вывод о необходимости внесения изменений в нормативные акты, а именно, а введении законодательного определения «электронные (цифровые) доказательства», уточнения порядка применения специальных знаний при работе с электронными носителями информации и некоторые другие.

Ключевые слова: электронный носитель информации, цифровое доказательство, следственное действие, доказательство.

Kira Vladimirovna VORYSHEVA
Danila Mikhailovich PODSVETOV

students

*St. Petersburg Law Institute (branch)
of the University of the Prosecutor's Office of the Russian Federation*

PRODUCTION INVESTIGATING ACTIONS WITH ELECTRONIC CARRIERS OF INFORMATION: ABOUT PROBLEM ASPECTS

Abstract. The article deals with the problems arising in the production of investigative actions with electronic media. Analyzing the current legislation and scientific literature on research issues, the authors conclude that it is necessary to amend regulations, namely, the introduction of a legislative definition of «electronic (digital) evidence», clarification of the procedure for applying special knowledge when working with electronic data carriers and some others.

Keywords: electronic data carrier, digital evidence, investigative action, evidence.

В XXI в. невозможно не сказать о стремительном развитии науки и техники. В современном обществе непрерывно совершенствуются средства передачи информации, появляются новые технические устройства и средства для их фиксации, обработки и хранения.

В современной криминалистической науке все чаще звучат термины «цифровая доказательственная информация» или «цифровые (электронные) доказательства». Можно предположить, что если в доктрине употребление данных терминов становится все более популярно, то они должны быть закреплены на законодательном уровне.

Однако в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и других законах и подзаконных нормативных правовых актах, посвященных этим вопросам, значение указанных терминов не определяется. В федеральном законодательстве речь идет об информационных технологиях, информационных системах и т.п.

Также УПК РФ не содержит понятия «цифровые (электронные) доказательства», а оперирует термином «электронные носители информации» или «информация на электронных носителях».

Предполагается, что такой подход законодателя не является верным, так как при проведении следственных действий больший интерес вызывает содержание данных электронных носителей, а именно цифровая информация. В данном случае, стоит принять во внимание опыт законодательства иностранных государств, где термин «электронные доказательства» употребляется не только в доктрине, но и нормативно закреплены. Таким образом, считаем необходимым дополнить ст. 74 УПК РФ новым видом доказательств.

С точки зрения современной системы доказательств, предусмотренной УПК РФ, электронные носители можно отнести либо к вещественным доказательствам, либо к иным документам.

Электронные доказательства в отличие от иных видов доказательств обладают определенной спецификой. Во-первых, стоит согласиться с мнением Н.А. Зигуры, который утверждает, что «предоставление подобной информации и использование ее в качестве доказательств по уголовному делу возможно исключительно в электронно-цифровой форме»¹, то есть данная информация находится на определенных электронных носителях, например, флеш-карте, дискете, диске, сервере. Во-вторых, изучение электронных доказательств требует наличие специального оборудования, например, компьютера, ноутбука, дисководов, CD-привода и др.

¹ Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис. ... канд. юрид. наук. Челябинск, 2010.

Данная специфика порождает определенные особенности обнаружения, фиксации и изъятия данных доказательств.

Для решения названных проблем в уголовно-процессуальном законе закреплены новые положения. Федеральным законом от 27 декабря 2018 г. № 533-ФЗ. УПК РФ дополнен ст. 164¹, регламентирующей особенности изъятия электронных носителей информации и копирования данных с них при производстве предварительного расследования.

Ч. 1 ст. 164¹ УПК РФ устанавливает запрет на изъятие электронных носителей на общих условиях по категориям дел, указанных в ч. 4¹ ст. 164 УПК РФ. Данное положение, на наш взгляд, полностью обосновано с точки зрения невмешательства и продолжения нормальной деятельности хозяйствующих субъектов.

Однако имеется нормативное исключение из правила:

- имеется постановление о производстве судебной экспертизы с электронными носителями;
- имеется судебное решение на производство изъятия электронных носителей;
- наличие на электронных носителях информации, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает;
- данная информация может применяться для совершения новых преступлений;
- копирование и изъятие информации может повлечь ее утрату.

Интересным и одновременно проблемным, на наш взгляд, кажется положение о возможности утраты информации.

Возникает логичный вопрос о том, каким же образом специалист на месте происшествия будет определять возможность утраты информации, ведь для этого, по мнению И.П. Родивилина и А.А. Шаевича, необходимо проведение, как минимум, экспертизы². Ответов на данный вопрос не дает ни закон, ни правоприменительная практика.

² Родивилин И.П., Шаевич А.А. Об участии специалиста при изъятии электронных носителей информации в ходе производства обыска и выемки // Криминалистика: вчера, сегодня, завтра: сборник научных трудов. 2013. Вып. 3, 4. Иркутск, С. 153.

Согласно ч. 2 ст. 164¹ УПК РФ при производстве следственных действий с электронными носителями информации необходимо обязательное участие специалиста. Так, исходя из принципов уголовного судопроизводства, изъятие в ходе производства следственных действий с электронными носителями без участия специалиста будет считаться нарушением требований УПК РФ и повлечет за собой их недопустимость.

При этом судебная практика по данному вопросу противоречива. Т.С. Крюкова указывает, что «только в 10 % судебных решений отсутствие специалиста было признано существенным нарушением порядка следственных действий (обыска и выемки), связанных с изъятием электронных носителей, и повлекло за собой признание протоколов следственных действий недопустимыми доказательствами»³.

Однако возникает вопрос целесообразности участия специалиста при производстве отдельных следственных действий с электронными носителями информации. Как считает М.В. Старичков, не вызывает сомнений, что изъятие электронных носителей информации, которые являются частью других электронных устройств, либо подключенных к другому оборудованию, а также копирование информации с изымаемых электронных носителей в интересах третьих лиц должно производиться только специалистом⁴.

Тем не менее, не является, на наш взгляд, необходимым участие специалиста, к примеру, при изъятия мобильного телефона, фотоаппарата и иных подобных технических средств, так как они являются единым целым и не требуют подключения к другим техническим устройствам для своего функционирования. Полагаем, это является существенным изъяном действующего уголовно-процессуального законодательства, ведь поиски и привлечение специалиста может занять так нужное для расследования время.

³ Крюкова Т.С. Некоторые вопросы изъятия электронных носителей информации в ходе производства следственных действий: анализ судебной практики // Использование информационных технологий в уголовном судопроизводстве: проблемы теории и практики. 2016. № 4. С. 62.

⁴ Старичков М.В. Особенности изъятия электронных носителей информации // Деятельность правоохранительных органов в современных условиях: материалы XIX Международной научно-практической конференции. М., 2014. С. 225.

В связи с этим предлагаем дополнить ст. 164¹ УПК РФ ч. 2¹, изложив ее в следующей редакции:

«В случаях изъятия электронных носителей информации целиком (без нарушения целостности) и без копирования содержащейся на них информации, допускается проведение следственного действия без участия специалиста».

Данные суждения находят свое отражение в судебной практике. До введения в действие ст. 164¹ УПК РФ суды шли по иному пути. Доказательства признавались допустимыми в случаях, если изъятие электронных носителей информации проводилось с носителя, который не требовал вмешательства в его функционирование (изымались диски, фотоаппараты без копирования с них информации).

Так, апелляционным постановлением Приморского краевого суда признано правомерным изъятие при производстве обыска электронных носителей без участия специалиста, так как не производилось копирование информации⁵. Данное положение, выраженное в позиции суда апелляционной инстанции, подтверждает необходимость включения названных изменений в действующую редакцию уголовно-процессуального закона.

Таким образом, УПК РФ не отражает специфики и роли электронных доказательств в следственной практике. В связи с этим вопросы, связанные с производством следственных действий, должны быть более детально отражены в нормах уголовно-процессуального закона. Отсутствие детальной регламентации влечет за собой противоречивость применения норм УПК РФ правоприменителями, а также усложняет производство следственных действий.

⁵ Апелляционное постановление Приморского краевого суда от 24 сентября 2015 г. № 22-5674/15. URL: <https://sudact.ru> (дата обращения: 15.10.2020).

Елена Юрьевна ГОРБУНОВА
*эксперт отдела компьютерных экспертиз
Экспертно-криминалистический центр
УМВД России по Мурманской области*

РАЗВИТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И НОРМАТИВНОГО РЕГУЛИРОВАНИЯ ЦИФРОВОЙ СРЕДЫ КАК ФАКТОРЫ, СПОСОБСТВУЮЩИЕ СОВЕРШЕНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Цифровые технологии играют важнейшую роль в инновационном развитии России. В последнее десятилетие цифровые технологии и цифровизация стремительно охватывают в России все области жизнедеятельности, экономика переходит в цифровой вид. Становление цифровой экономики сопровождается принятием правовых актов, регулирующих как направления развития, так и формирование компонентов новой экономики. Цифровизация, новые информационные технологии, цифровая экономика повлияли и на криминальную деятельность в целом. Злоумышленники стали применять Интернет, компьютеры для совершения практически всех преступлений в сфере экономической деятельности. Появилась новая разновидность экономической преступности, преступления совершаются с использованием компьютерных и телекоммуникационных технологий. Электронная среда, затрудняет идентификацию правонарушителя, исследование преступлений становится сложнее, превращая экономическую преступность в одну из наиболее важных проблем, которые стоят перед современным обществом.

Ключевые слова: цифровизация, цифровая экономика, цифровая бухгалтерия, облачная бухгалтерия, экономические преступления.

Elena Yuryevna GORBUNOVA
*expert of the computer
Department Forensic Science Center Ministry
of internal Affairs of Russia in the Murmansk region*

THE DEVELOPMENT OF INFORMATION TECHNOLOGIES AND STATUTORY REGULATION OF THE DIGITAL ENVIRONMENT AS FACTORS CONTRIBUTING TO THE COMMISSION OF CRIMES IN THE SPHERE OF ECONOMIC ACTIVITY

Abstract. Digital technologies play a crucial role in the innovative development of Russia. In the last decade, digital technologies and digitalization have rapidly covered all areas of life in Russia, and the economy itself is moving to a digital

form. The formation of the digital economy is accompanied by the adoption of legal acts regulating both the development directions and the formation of components of the new economy. Digitalization, new information technologies, and the digital economy have also affected criminal activity in general. Lawbreakers began to use the Internet and computers to commit almost all crimes in the field of economic activity. There is a new type of economic criminality, crimes are committed using computer and telecommunications technologies. The electronic environment makes it difficult to identify the offender. Therefore, the investigation of crimes becomes more difficult, making economic criminality one of the most important problems facing modern society.

Keywords: digitalization, digital economy, digital accounting, cloud accounting, economic crimes.

В послании Федеральному собранию в 2016 г. Президент РФ В.В. Путин отвел ключевую роль цифровым технологиям в инновационном развитии государства, а также впервые сформулировал один из стратегических принципов развития РФ – «цифровая экономика»¹. Президент России также предложил запустить масштабную программу по формированию в стране общества знаний, новой, технологической, цифровой экономики, которая обеспечит национальные интересы и реализацию стратегических национальных проектов. Тем самым был сформулирован посыл для дальнейших указов Президента России, согласно которым цифровизация экономики должна стать основным путем становления конкурентоспособного государства на мировом рынке.

Так, основополагающим нормативно-правовым актом, регламентирующим цифровую трансформацию в России, является «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы»². Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»

¹ Послание Президента Российской Федерации от 1 декабря 2016 г. «О положении в стране и основных направлениях внутренней и внешней политики государства» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/> (дата обращения: 23.09.2020).

² Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/> (дата обращения: 23.09.2020).

определены и основные направления государственной политики по формированию и внедрению цифровых технологий, развитию цифровой экономики для реализации национальных приоритетов и конкурентоспособного участия в глобальной экономической системе.

Современная цифровая экономика включает следующие компоненты: цифровая инфраструктура (устройства, программное обеспечение, сети и др.), электронные процессы в организациях (автоматизация основной деятельности, учета), онлайн торговля. Ключевым фактором производства в цифровой экономике являются: цифровые данные, быстрая обработка больших объемов (качественный сбор и хранение информации), а также их анализ, что, безусловно, повышает эффективность хозяйственной деятельности. Современные физические принципы представления цифровой информации позволяют без потери точности постоянно наращивать вовлеченность различных организаций в процессы цифровизации.

Преимущественным значением подобного направления развития является совершенствование средств вычислительной техники, автоматизация как простых, так и сложных процессов, различных направлений хозяйственной деятельности, переход от бумажных документов к электронным (безбумажные технологии), увеличение скорости и простоты генерации документов, принятия их к учету, формирование требуемых форм балансов – и, что имеет не менее важное значение, – автоматизированное составление документов бухгалтерской и финансовой отчетности.

Цифровые технологии и цифровизация стремительно охватывают в РФ все области, включая документооборот, экономику, бухгалтерский учет. Теперь цифровая экономика работает без бумаги, происходит переход к юридически значимому электронному документообороту.

Бухгалтерия и документооборот переводятся в электронный вид в соответствии с появляющейся нормативно-правовой базой:

- п. 5 ст. 9 и п. 6 ст. 10 Федерального закона от 6 декабря 2011 г. № 402-ФЗ «О бухгалтерском учете» (первичные документы и регистры, соответственно)³;

³ Ст. 10. Регистры бухгалтерского учета // Федеральный закон от 6 декабря 2011 г. № 402-ФЗ «О бухгалтерском учете».

- ст. 6 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»⁴;
- ст. 169, 314, 93 НК РФ (счет-фактура, аналитические регистры бухгалтерского учета, истребование документов при проведении налоговой проверки).

На этом фоне появляется множество компаний, разрабатывающих программное обеспечение для нужд цифровой экономики. Что касается компаний, разрабатывающих программное обеспечение для автоматизации функций бухгалтерского, налогового, управленческого учетов, то несомненным лидером в данном сегменте является фирма «1С», программными продуктами которой пользуются несколько миллионов пользователей.

Стремительное развитие информационных технологий привело к появлению и новых технологий – «облачных», которые активно используются в цифровой экономике. Облачные технологии предоставили возможность не зависеть от места нахождения, как пользователю услуг, так и провайдеру. Развитие возможностей сети Интернет и облачных вычислений также способствовали развитию экономической деятельности, техники бухгалтерского учета. Программы, созданные для автоматизации учета, стали сервисом в Интернете и развитие этому направлению придает пандемия COVID-19, вынудившая миллионы пользователей работать из дома.

Цифровизация общества, новые информационные технологии, создание «цифровой» экономики – это хороший тренд, но он повлиял и на криминальную деятельность в целом.

Экономическая преступность превратилась в одну из наиболее важных проблем, стоящих перед мировым сообществом, а определяющим мотивом для совершения преступлений в сфере цифровой экономики является обогащение.

Прогресс в информационных технологиях повлек за собой умышленное злоупотребление этими достижениями. Злоумышленники стали применять Интернет, компьютеры, средства телекомму-

⁴ Ст. 6. Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью / Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/> (дата обращения: 23.09.2020).

никации, возможности современного программного обеспечения для автоматизации процессов, электронного документооборота, бухгалтерского учета с использованием цифровых, «облачных» технологий для совершения практически всех преступлений в сфере экономической деятельности. Появилась новая разновидность экономической преступности, прогрессивная, динамичная и научно подкованная, которая активно использует компьютеры и Интернет, которые стали неотъемлемыми атрибутами жизнедеятельности современного человека.

Таким образом, современные экономические преступления все чаще стали совершаться в двух мирах, один из них – цифровой (виртуальный), а средства и способы совершения преступлений и объекты посягательств постоянно трансформируются, становятся изощреннее.

Данное обстоятельство стало учитываться и в официальной статистике МВД РФ, среди общей преступности экономической направленности с 2017 г. выделяются деяния, которые совершаются с использованием компьютерных и телекоммуникационных технологий. Также можно отметить, что всеобщая цифровизация вызывает латентность экономической преступности, препятствует ее выявлению и получению объективной информации о противоправных деяниях.

Низкая раскрываемость, прежде всего, связана с технической сложностью таких деяний, поскольку способы совершения преступлений и объекты посягательств постоянно трансформируются, происходит это под воздействием эволюции способов хранения, передачи и обработки цифровой информации. Нельзя не отметить и то, что цифровая среда затрудняет индивидуализацию, идентификацию правонарушителя и в этой сфере существует правовой вакуум.

Расследование высокотехнологичных преступлений в сфере экономической деятельности требует от сотрудников правоохранительных органов колоссальных знаний «норм права, бухгалтерского учета, финансов, экономики»⁵, а также основывается на знании

⁵ Федичев Г.Г., Энтю В.А. Расследования преступлений в сфере экономической деятельности посредством применения экономических познаний // Вестник Института дружбы народов Кавказа. Теория Экономики и управления народным хозяйством. 2016. № 4 (40) С. 23.

«информационных технологий, особенностей и принципов работы специализированного программного обеспечения, используемого хозяйствующими субъектами»⁶ и практическом опыте.

Основываясь на положительном опыте зарубежных стран, где цифровая экономика прошла все этапы развития, правоохранными органами накоплен значительный опыт, необходима реализация комплекса мер, направленных на эффективное противодействие экономической преступности, среди которых можно выделить:

- разработка законодательства, регламентирующего активное внедрение цифровых технологий и, соответственно, законодательства, позволяющего правоохранным органам противодействовать преступности в цифровой среде;
- техническое оснащение правоохранных органов, включающее в себя приобретение и регулярное обновление компьютерной техники и инновационного программного обеспечения;
- обучение лиц, принимающих участие в расследовании экономических преступлений, совершаемых с использованием средств вычислительной техники;
- межведомственное взаимодействие по вопросам противодействия преступлениям, совершаемым в сфере экономической деятельности;
- повышение уровня осведомленности общества о возможных преступных схемах и способах противодействия им;
- повышение ответственности бизнеса за отсутствие средств и методов, ограничивающих несанкционированный доступ или утрату информации, которую они собирают, хранят и обрабатывают.

⁶ Там же. С. 23.

Евгений Степанович ДУШКОВ

студент

Институт права и национальной безопасности

Тамбовского государственного университета им. Г.Р. Державина

КИБЕРПРЕСТУПНОСТЬ ВО ВРЕМЯ ПАНДЕМИИ COVID-19: СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Аннотация. В данной статье анализируется текущее состояние преступности в условиях распространения всемирной пандемии. Автором проведен анализ киберпреступлений, совершаемых в современных непростых условиях, когда большинство работников и учащихся переведены в режим онлайн. Как никогда раньше, угроза киберпреступности в настоящее время достигла пика своего развития. Изучается зарубежный опыт борьбы с данным явлением. Предлагается уделить данной проблеме особое внимание и принимать меры для уменьшения распространения киберпреступности.

Ключевые слова: киберпреступность, пандемия, компьютерное мошенничество, дистанционный формат, преступление, доступ к информации.

Evgeny Stepanovich DUSHKOV

student

Institute of Law and National Security

of Tambov State University named after G.R. Derzhavin

CYBERCRIME DURING THE COVID-19 PANDEMIC: EXISTING PROBLEMS AND WAYS OF SOLUTION

Abstract. This article analyzes the current state of crime in the context of the spread of a global pandemic. The author has analyzed cybercrimes committed in today's difficult conditions, when the majority of workers and students are transferred online. As never before, the threat of cybercrime is now at its peak. It is proposed to pay special attention to this problem and take measures to reduce the spread of cybercrime.

Keywords: Cybercrime, pandemic, computer fraud, remote format, crime, access to information.

Преступления в сфере компьютерных и информационных технологий получили в настоящее время большое распространение. Незаконная преступная деятельность, основной целью которой является неправомерное использование компьютерных технологий, компьютерной сети или сетевого устройства называется киберпре-

ступлением¹. Огромное количество киберпреступлений совершается хакерами с целью обмануть людей и заработать на этом деньги. Киберпреступная деятельность осуществляется как отдельными лицами, так и организациями. Однако иногда киберпреступники объединяются в организованные преступные группы, используя при этом усовершенствованные и передовые методы и обладают технической квалификацией².

В современном мире все процессы изменяются быстро, но особенно кардинально это произошло в текущем 2020 г. Исследования показывают, что в настоящее время в условиях распространения пандемии Covid-19 все реже стали совершаться традиционные преступления, такие как грабежи, разбои и мошенничества. В первую очередь, это связано с ограничениями, введенными властями страны для предотвращения распространения вируса. То есть карантин и контроль за перемещением людей снизил уровень уличной преступности. С другой стороны, переход всего мира в виртуальную реальность, в частности, на удаленную работу через компьютер, или учебу в дистанционном формате, что привело к распространению другого преступления – киберпреступности. Говоря о статистике, заместитель председателя Совета Безопасности РФ Д.А. Медведев отметил: «За последние пять месяцев количество преступлений с использованием интернета, информационных технологий, мобильной связи составило более 180 тысяч»³. Это примерно на 85 % больше, чем за такой же период 2019 г. В общем количестве правонарушений удельный вес киберпреступлений также увеличился почти в 2 раза. Именно в это время у мошенников появляются новые схемы, приемы совершения преступлений, а под ударом оказываются простые пожилые граждане, которые не всегда могут правильно сориентироваться в этой обстановке.

¹ Бондарь Е.О. Киберпреступность как новая криминальная угроза // Вестник Московского университета МВД России. 2020. С. 18.

² Долженко Н.И., Ярошук И.А. Киберпреступность как одна из ключевых проблем современности // Правовая парадигма. 2020. № 1. С. 151.

³ Рост киберпреступности во время пандемии. URL: <https://rg.ru/2020/06/09/medvedev-rasskazal-o-rote-kiberprestupnosti-v-rf-vo-vremia-pandemii.html> (дата обращения: 02.11.2020).

Практика указывает на следующие факты. Если мошенничество в интернете, вымогательство в сети нацелено на конкретные группы лиц, то программы-вымогатели и программы-взломщики, созданные в период пандемии Covid-19, в первую очередь, подрывают работу организаций. Эти факты свидетельствуют о том, что и в дальнейшем они будут становиться жертвами этих вредоносных программ. Вместе с этим увеличился рост распространения ложной, недостоверной информации, которая вводит в заблуждение все общество и ставит под угрозу научные меры реагирования. Как уже было отмечено, удаленная работа увеличивает число жертв киберпреступности. Работая дома онлайн, человек подвергается большему риску, тем самым ставя под угрозу корпоративное программное обеспечение, что делает его более уязвимым для киберпреступников. Фишинг продолжает предоставлять злоумышленникам, а также другим продвинутым пользователям несанкционированный доступ к их системам.

В настоящее время во всем мире властями предпринимаются комплексные и важнейшие меры перевода всех граждан в дистанционный формат. Эти меры привели к существенному использованию средств онлайн-связи государственными органами, предприятиями и частными лицами в огромных масштабах. Для большого количества людей, особенно для тех категорий граждан, для которых Интернет и в целом компьютерная техника являются вещами малознакомыми, переход на данную дистанционную систему обучения или работы является непривычным и очень опасным. Данная аудитория представляет собой обширную, легкодоступную и уязвимую целевую группу для киберпреступников.

Преступники в сфере компьютерных технологий в последние несколько месяцев 2020 г. все чаще используют в своих целях страх людей перед вирусом Covid-19. Например, они выставляют на продажу в Интернете поддельные лекарственные препараты, несуществующие дезинфицирующие средства, средства индивидуальной защиты (СИЗ), медицинские аппараты и средства гигиены. Другие виды мошенничества включают предложения об инвестиционном консультировании, в том числе по криптовалютам, а также ложные медицинские консультации и диагностику. Люди пожилого возраста, которые чаще всего менее осведомлены и не готовы к опасностям

в Интернете, становятся легкой добычей для киберпреступников, использующих их для загрузки и пересылки вредоносных ссылок через электронные спам сообщения о Covid-19, а также в целях распространения ложной информации среди друзей и членов семьи.

Одним из самых известных и распространенных посягательств в Интернете являются ВЕС-атаки – это атаки с использованием компрометации деловой переписки, в которой, как правило, мошенники представляются должностными лицами организации, выбранной для преступления. Продолжают использовать методы социальной инженерии, пользуясь при этом обострившейся ситуацией вокруг пандемии, для перемещения денежных средств на иностранные валютные и криптовалютные счета, а также для получения конфиденциальной информации с целью неправомерного использования, включая шпионаж. Форумы Даркнет пестрят скомпрометированными и ложными данными, в том числе высокопоставленных чиновников и знаменитостей. Начинающие кибепреступники ищут возможности, как лучше и полезнее всего использовать пандемию для получения незаконной прибыли. Известны случаи, когда отдельные киберпреступники пытались отговорить других киберпреступников от DDoS-атак, а также от атак вредоносными программами на больницы и лаборатории по тестированию вакцин⁴.

Вместе с традиционными видами и целями киберпреступности, ведущие целенаправленные угрозы (APT – Advanced Persistent Threats) продолжают совершенствоваться и использоваться для получения нелегальной выгоды из ситуации с пандемией Covid-19. Главной целью APT атак являются критические объекты инфраструктуры, включая больницы и лаборатории по разработке вакцин. При этом применяются вредоносные программы, программы-вымогатели, а также DDoS-атаки. Мотивом для подобных атак служит не только получение прибыли, но и возможность доступа к персональным данным и другой конфиденциальной информации, представляющей ценность (например, в качестве оперативных разведывательных данных).

⁴ URL: https://www.unodc.org/documents/Advocacy-Section/Russian_-_UNODC_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED (дата обращения: 02.11.2020).

Достижение поставленных преступных целей киберпреступников, связанных с Covid-19, может быть осуществлено с помощью фишинговых атак по электронной почте в качестве первоначального этапа заражения операционной системы устройства. Как только пользователи переходят по вредоносной ссылке или загружают документ, учетная запись становится подконтрольной мошеннику. Компрометация учетной записи может быть замечена пользователем, но чаще всего она остается зашифрованной и скрытой от глаз жертвы и позволяет установить долгосрочный доступ к учетной записи, организации и связанным с ней программным обеспечением. Кроме сбора конфиденциальной информации, АРТ атаки могут нарушить работу вебсайтов, вносить изменения в документы, удалять данные, а также распространять ложную или провокационную информацию.

Зарубежный опыт борьбы с данным явлением свидетельствует, что в большинстве государств сотрудники специальных подразделений правоохранительных органов по борьбе с киберпреступностью вынуждены уделять основное внимание не расследованию киберпреступлений, а поддержке правительственных мер, таких как обеспечение соблюдения карантина во время вспышки коронавируса Covid-19. Некоторые специалисты сами стали жертвами болезни. С массовым распространением вируса, потенциал правоохранительных органов снижается, негативно сказываясь на способности государств, противостоять новым усиливающимся киберугрозам. В зарубежных странах, в которых распространение вируса является катастрофическим, нарушено функционирование следственных и судебных процедур из-за необходимости проводить эти процедуры лично и непосредственно по закону, что не представляется возможным в связи с принятыми мерами в области общественного здравоохранения. Другие страны решили не отказываться полностью от данного института правосудия и перешли на судебные процедуры в режиме онлайн. Например, управление по наркотикам и преступности Организации Объединенных Наций в сложившейся ситуации рекомендует проведение, по мере возможности, судебных процедур онлайн обеспечивая при этом соблюдение международных стандартов и норм, надлежащих правовых процедур, а также верховенство права.

Исследования показывают, что ложная и недостоверная информация относительно вируса продолжает распространяться, главным

образом, через социальные сети, а также через сервисы с зашифрованной передачей сообщений. Социальные сети также столкнулись с проблемой перехода сотрудников на удаленную работу и пытаются справиться с большими объемами дезинформации и фейковых новостей, принимая во внимание внутренние политики компаний и местное законодательство. Вследствие чего дезинформация и кибератаки на важнейшие объекты инфраструктур подрывают к ним общественное доверие граждан и ослабляют в общем эффективность проводимых ими мер для общественной безопасности.

Например, управление по наркотикам и преступности Организации Объединенных Наций рекомендует правительствам стран и представителям частного сектора активно проводить кампании и программы по повышению уровня информированности населения, с учетом культурной специфики. Также рекомендуется операторам социальных сетей прилагать больше усилий для борьбы с распространением так называемой «инфодемии» обусловленной Covid-19, обеспечивая при этом свободу слова⁵.

В результате можно сделать несколько важнейших выводов и сформулировать некоторые предложения по уменьшению распространения киберпреступности в это и без того сложное для всего человечества время. В условиях пандемии многие страны перешли от физических операций в режим онлайн, также поступили и преступники. В то время как масштабы и изощренность киберпреступлений возрастает, увеличивается и количество пострадавших от них. В некоторых странах представители правоохранительных органов вынуждены исполнять другие обязанности, связанные не с борьбой с этим явлением, а с охраной общественного порядка. Усугубляет ситуацию для общественности и правительств экономическое влияние Covid-19. Таким образом, складываются идеальные условия для потенциальных киберпреступлений. Нельзя не отметить, что угроза киберпреступности во время пандемии, как и угроза самого вируса, является глобальной проблемой, соответственно, ответные меры по противодействию тоже должны быть глобальными и масштабными. В данной ситуации, на наш взгляд, необходимо наладить обмен

⁵ URL: <https://www.unodc.org/> (дата обращения: 02.11.2020).

информацией между государствами о появившихся новых угрозах и типах рассматриваемых преступлений.

Полагаем, дальнейшая возможность активных и результативных расследований случаев киберпреступности будет ограничена, учитывая вероятную нагрузку на оперативную деятельность правоохранительных органов. Киберпреступники продолжают использовать сложную ситуацию в своих целях. Но не смотря на это, публичная отчетность об успешных арестах киберпреступников или предотвращении кибератак в современных условиях должна быть усилена. Например, сложная масштабная операция по закрытию и ликвидации 15 серверов для DDoS-атак по найму в Нидерландах в течение одной недели⁶. Этот факт демонстрирует возможности и работу правоохранительных органов, а также оказывает профилактическое влияние на киберпреступников. Практика показывает, что международная и внутригосударственная деятельность, повышение информативности населения в данной ситуации играют ключевую роль в процессе предотвращения угроз и расширении возможностей в борьбе с данным явлением. В особенности, это касается наиболее уязвимых групп населения: детей и пожилых людей.

В заключении отметим, что меры по противодействию киберпреступности должны носить пропорциональный, правовой, подотчетный и обоснованный характер. В сложившейся обстановке органы власти должны развивать доверительные киберотношения с общественностью и организовать совместную работу с целью противодействия насущным угрозам, а также укрепления доверия к ним. Способность и потенциал противодействия преступности являются важнейшими компонентами защиты наиболее значимых объектов национальной инфраструктуры, обеспечения безопасности детей в Интернете, расширения возможностей организаций и предприятий, обеспечения безопасности больниц и содействия экономическому восстановлению после Covid-19.

⁶ URL: <https://www.zdnet.com/article/dutch-police-take-down-15-ddos-services-in-a-week> (дата обращения: 02.11.2020).

Вероника Юрьевна ЕГОРУШКИНА

магистрант

Саратовская государственная юридическая академия

ОРГАНЫ ПРОКУРАТУРЫ В СИСТЕМЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Аннотация. При осуществлении надзора в органах прокуратуры существует множество проблемных вопросов, в том числе при противодействии преступности в сфере информационно-компьютерных технологий. В статье рассмотрены проблемы прокурорского надзора за исполнением законов органами дознания и предварительного следствия при осуществлении ими деятельности по расследованию, предупреждению, пресечению киберпреступлений.

Ключевые слова: киберпреступность, прокуратура, информационно-компьютерные технологии, предупреждение преступности, правоохранительные органы.

Veronika Yurevna EGORUSHKINA

student

Saratov State Academy of Law

PROSECUTOR'S OFFICES IN THE SYSTEM OF COMBATING CRIME IN THE FIELD OF INFORMATION AND COMPUTER TECHNOLOGIES

Abstract. The Prosecutor's office still does not have a specific definition of activities aimed at suppressing crime in the field of information and computer technologies. This article will address the problems of Prosecutor's supervision of cybercrime, as well as the imperfection of the activities of law enforcement agencies under their supervision.

Keywords: cybercrime, prosecutor's office, information and computer technologies, crime prevention, law enforcement agencies.

Организация защиты информации в настоящее время осуществляется различными способами: путем предотвращения ее разглашения, несанкционированного доступа, копирования, искажения, уничтожения, сбоя технических и программных средств информационных систем и многим другим. Однако при самых сложных и серьезных способах защиты информации преступность в сфере информационно компьютерных технологий растет.

Как отмечал Генеральный прокурор РФ И.В. Краснов на заседании Координационного совещания руководителей правоохрани-

нительных органов, где в том числе обсуждались вопросы роста киберпреступности: «За последние 5 лет число таких преступлений возросло в 25 раз», – сказал он, добавив, что в 2019 г. было зафиксировано 294 тыс. киберпреступлений. Причем это касается деятельности всех правоохранительных органов, поскольку новые технологии все чаще выступают средством совершения самого широкого круга преступлений, от хищений денежных средств с расчетных пластиковых карт, до угроз критической инфраструктуре страны и обеспечению ее безопасности». По его словам, эта негативная тенденция усилилась в первом полугодии текущего года, был зафиксирован рост числа киберпреступлений на 92 %¹.

Для борьбы с данным видом преступлений созданы подразделения в рамках структур МВД и ФСБ России. Управление «К» МВД России в пределах своей компетенции осуществляет выявление, предупреждение, пресечение и раскрытие преступлений в сфере компьютерной информации, преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) и направленных против здоровья несовершеннолетних и общественной нравственности, преступлений, связанных с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации, преступлений, связанных с незаконным использованием объектов авторского права или смежных прав².

При осуществлении начального этапа расследования преступлений – оперативно-розыскной деятельности, органами правопорядка производятся различные оперативно-розыскные мероприятия, которые, в основном, носят общий характер.

Такие мероприятия, как, например, сбор образцов для сравнительного исследования, контроль почтовых отправлений, телеграфных и иных сообщений, снятие информации с технических

¹ Генпрокурор России Игорь Краснов провел совещание по теме борьбы с преступлениями, связанными с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий. URL: <https://genproc.gov.ru/smi/news/genproc/news-1880616/> (дата обращения: 06.11.2020).

² Управление «К» МВД России. URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (дата обращения: 07.11.2020).

каналов связи, оперативный эксперимент и, особенно, оперативное внедрение, в условиях информационного общества требуют от оперативных сотрудников, как минимум, специальной подготовки, а часто и технического образования по специальности «компьютерная безопасность», «информационная безопасность» и т.п.

Криминалистическая тактика расследования преступления также имеет свои особенности: при сборе следов «электронного преступления» (а это как и физические следы – отпечатки пальцев на клавиатуре, например, так и электронные следы – отражающие изменения в хранящейся в них информации по сравнению с исходным состоянием), используется как и стандартные криминалистические приемы сбора следов преступлений, так и компьютерно-техническая экспертиза (для исследования отпечатков электронных следов), которая позволяет, к примеру, получить сведения об IP-адресах, с которых производится администрирование Интернет-сайта, доменного имени и/или IP-адреса, выявление сторонних заходов, сведения о запросах, посылаемых при обращениях к Интернет-сайту, и поиск среди них тех, что могли использоваться для поиска, следы подбора пароля, сведения о загрузке/выгрузке файлов на/с сервера и другие³.

Приказом ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» создан национальный координационный центр по компьютерным инцидентам (НКЦКИ), который является составной частью сил, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Задачей НКЦКИ является обеспечение координации деятельности субъектов критической информационной инфраструктуры РФ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты⁴.

³ Аносов А.В. и др. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие. М., 2019. Ч. 1. С. 111–112.

⁴ ФСБ России создан Национальный координационный центр по компьютерным инцидентам. URL: <http://www.consultant.ru/law/hotdocs/54965.html/> (дата обращения: 08.11.2020).

Помимо активной деятельности правоохранительных органов по расследованию мошеннических действий в сфере ИКТ, Банк России также принимает участие в предупреждении и пресечении преступлений. Так, на основании жалоб потребителей финансовых услуг на мошеннические действия посредством телефонных звонков от имени службы безопасности кредитных организаций количество заблокированных по инициативе Банка России мошеннических телефонных номеров за первое полугодие 2020 г. выросло почти в 4 раза в сравнении с тем же периодом 2019 г. и превысило 9,7 тыс.

Как правильно отметил директор Департамента информационной безопасности Банка России В.А. Уваров: «Не менее важно повышение финансовой киберграмотности и кибергигиены. Банк России совместно с финансовыми организациями, прокуратурой и правоохранительными органами через все доступные каналы коммуникации постоянно разъясняет людям, как безопасно пользоваться современными платежными инструментами»⁵.

Помимо этого, специальное структурное подразделения Банка России ФинЦЕРТ создано для системного информационного обмена между участниками финансового рынка, правоохранительными органами, провайдерами и операторами связи, системными интеграторами, разработчиками антивирусного программного обеспечения и другими компаниями, работающими в сфере информационной безопасности.

Участники информационного обмена сообщают о выявленных ими угрозах и совершенных на них атаках, ФинЦЕРТ дает рекомендации по противодействию этим рискам. Это помогает оперативно реагировать на возникающие угрозы в финансовой сфере, не допускать их распространения, минимизировать потери финансовых организаций и их клиентов⁶.

В рамках деятельности вышеуказанных организаций прокуратура при осуществлении надзора играет особую роль. Надзорные

⁵ На фоне пандемии COVID-19 выросла активность телефонных мошенников и киберпреступников в Интернете. URL: <http://www.cbr.ru/press/event/?id=8238> (дата обращения: 07.11.2020).

⁶ ФинЦЕРТ. URL: http://www.cbr.ru/information_security/fincert/?utm_source=w&utm_content=page (дата обращения: 07.11.2020).

функции прокурора в любом из предметов надзора, указанных в разд. 3 Федерального закона «О прокуратуре» (так как было выяснено ранее предупреждением, например, занимаются не только государственные органы, но и юридические лица, которые подпадают под надзор прокуратуры), требуют специальных знаний, умений и навыков для проверки законности тех или иных действий поднадзорных органов/организаций в сфере информационно-компьютерных технологий – начиная с проверки уголовных дел в пределах ст. 37 УПК РФ заканчивая проверкой законности деятельности отдельных подразделений.

С 2010 по 2020 гг. прокуратурой было предпринято несколько попыток организовать новые способы пресечения преступлений для минимизирования мошеннических действий и упрощения расследования. Так, в 2015 г. Правительство РФ отклонило законопроект, который предоставляет прокурорам право получать в банках сведения о счетах и операциях граждан и компаний без соответствующего решения суда. Правительство указало, что Генеральный прокурор РФ сейчас может обращаться с запросами в банк по его клиентам без решения суда, а расширение полномочий рядовых прокуроров нарушит конституционные права россиян⁷.

В марте 2018 г. внесен законопроект, который предусматривал предоставление прокуратуре полномочия получать информацию в банках о движениях по счетам юридических лиц и индивидуальных предпринимателей, а также по операциям, счетам и вкладам физических лиц. Этот законопроект также был отклонен Комитетом Госдумы по финансовому рынку по причине отсутствия конкретики в полномочиях прокурора при получении доступа к банковской тайне⁸.

В рамках структуры прокуратуры нет отдельного подразделения, специалисты которого все свои знания и навыки воплощали бы в противодействии и надзоре за киберпреступлениями. Как, например, в Израиле с 2015 г. существует отдел по делам киберпреступле-

⁷ Правительство отказало прокурорам в банковских тайнах граждан. URL: <https://www.banki.ru/news/bankpress/?id=8218992> (дата обращения: 08.11.2020).

⁸ В Думе не поддержали законопроект о доступе прокуроров к данным о счетах. URL: <https://www.interfax.ru/russia/727167> (дата обращения: 09.11.2020).

ний, который занимается тремя основными видами деятельности: организационная работа в государственной прокуратуре в сфере киберпреступлений и радиоэлектронной разведки (SIGINT), ведение уголовных дел в области киберпреступлений и преступлений, связанных со сбором информации, осуществление действий в области альтернативного надзора по предотвращению и ликвидации ущерба⁹.

Для правовой системы РФ данная система, на наш взгляд, не подходит. В России прокуратура выполняет контрольно-надзорные функции и не принимает участие в расследовании уголовных дел. Таким образом, создание отдела прокуратуры по надзору за киберпреступлениями нецелесообразно: все киберпреступления – уголовно наказуемые деяния. А надзор в пределах ст. 37 УПК РФ осуществляется прокуратурой каждым из уровней.

Основной проблемой правоохранительной системы, в том числе и прокуратуры, является именно недостаток знаний в сфере IT-грамотности как органов предварительного расследования, так и органов прокуратуры для эффективного надзора.

Для этого необходимо дополнительное обучение в программах образования по направлению подготовки юриспруденция базисным положениям об информационно-компьютерных технологиях, а также предоставление правоохранительным органам, работающим с киберпреступлениями, методических рекомендаций по расследованию преступлений, постоянное повышение квалификации и возможность использовать нестандартные и современные методы сбора доказательственной базы при расследовании преступлений.

Исходя из этого, необходимо, соответственно, также обучение сотрудников прокуратур с позиции надзора, отражения ключевых моментов в инструкциях и приказах Генерального прокурора РФ по надзору за исполнением уголовного законодательства в сфере информационно-компьютерных технологий.

Однако первые шаги к борьбе с преступностью начались уже в этом году. Так, глава государства в марте 2020 г. попросил Генеральную прокуратуру РФ совместно с МВД России и другими заинтересованными структурами проанализировать, насколько

⁹ Об отделе по борьбе с киберпреступностью. URL: <https://www.gov.il/ru/Departments/General/cyber-about> (дата обращения: 09.11.2020).

эффективно построена работа в сфере защиты от киберугроз и выработать систему борьбы с киберпреступностью¹⁰. Генеральная прокуратура РФ после этого уже предложила подумать о создании центра сбора данных о киберпреступлениях¹¹.

В настоящее время трудно судить о перспективе эффективности избранных мер для борьбы с киберпреступлениями. Но то, чем занимается прокуратура в настоящее время – в основном это предупреждение преступлений, требует неукоснительного применения для профилактики распространения киберпреступности и защиты прав граждан от преступных посягательств.

¹⁰ Путин поручил создать систему по борьбе с киберпреступлениями. URL: <https://regnum.ru/news/2886810.html> (дата обращения: 09.11.2020).

¹¹ Генпрокуратура предлагает подумать о создании центра по сбору данных о киберпреступности. URL: <https://tass.ru/obschestvo/7983073> (дата обращения: 09.11.2020).

Кристина Сергеевна КАЩЕЕВА

студент

Тамбовский государственный университет им. Г.Р. Державина

КИБЕРМОШЕННИЧЕСТВО: ХАРАКТЕРИСТИКА И СПОСОБЫ

Аннотация. Статья посвящена изучению такого вида преступлений как мошенничество, совершаемое с использованием информационных технологий. В частности, автором рассматриваются и анализируются наиболее популярные способы осуществления кибермошенничества. По мнению автора, кибермошенничество представляет собой угрозу как отдельному человеку, так и всему обществу и государству в целом, ведь количество мошенничеств, совершаемых с использованием информационных технологий, увеличивается пропорционально числу пользователей информационных и компьютерных сетей. Вместе с тем вычислить таких преступников с каждым годом становится все сложнее. Данный вывод исходит из того, что развитие компьютерных и информационных технологий оказывает влияние и на преступную среду, в том числе снабжая мошенников новыми формами и средствами проявления их криминальной деятельности.

Ключевые слова: мошенничество, хищение, киберпреступность, банковская карта, информационные технологии, технологический прогресс.

Kristina Sergeevna KASHCHEEVA

student

Tamбов State University named after G.R. Derzhavin

CYBER FRAUD: CHARACTERISTICS AND METHODS OF ITS COMMITMENT

Abstract. The article is devoted to the study of this type of crime as fraud committed using information technology. In particular, the author examines and analyzes the most popular ways of performing cyber fraud. According to the author, cyber fraud is a threat to both an individual and the entire society and the state as a whole, because the number of frauds committed using information technologies increases in proportion to the number of users of information and computer networks. At the same time, it becomes more and more difficult to calculate such criminals every year. This conclusion is based on the fact that the development of computer and information technologies has an impact on the criminal environment, including providing fraudsters with new forms and means of displaying their criminal activities.

Keywords: fraud, theft, cybercrime, Bank card, information technology, technological progress.

XXI в. – это век информационных технологий, которые проникли и охватили практически все сферы жизнедеятельности людей,

организаций, государства. Действительно, сегодня мы не можем представить свою жизнь без компьютера, смартфона и других видов гаджетов. Не стала исключением и преступная, криминальная сфера, именно мошенники все чаще используют компьютерные и иные информационные технологии в своих преступных целях. «Мошеннические схемы постоянно меняются, поскольку меняются способы взаимодействия людей друг с другом. Мошенничество сильно эволюционировало, двумя самыми значительными факторами стали рост глобальных коммуникаций и огромные достижения, которые мы наблюдаем в области технологий и использования данных»¹.

Мошенничество представляет собой наиболее распространенный вид преступлений, совершаемых в экономической сфере. Данное преступление выступает одним из сложных видов не только хищения, но и преступлений в целом. Это проявляется в сложном уголовно-правовом составе, в наличии хорошо обдуманного замысла и плана реализации преступного деяния, а также в способах его совершения. В большей степени именно способы и позволяют выделить мошенничество в отдельный вид хищения. К способам мошенничества относят применение обмана, то есть введение потенциальной жертвы, потерпевшего, в заблуждение относительно реального события путем сообщения ей ложных сведений, а также злоупотребление доверием, характеризующееся добровольной передачей потерпевшим, то есть обманутой жертвой, имущества либо права на него мошеннику, будучи уверенным в законности и правомерности намерений последнего. Отсюда следует, что отличительной чертой деятельности мошенников выступает отсутствие применения с их стороны угроз, насилия, оружия против жертвы, преступный замысел реализуется лишь путем обмана или злоупотребления доверием. Исходя из этого, данный вид преступности, а точнее, данный вид мошенников, можно охарактеризовать через такой признак, как гуманность, ведь мошенники совершают преступление лишь путем своей находчивости, хитрости и хорошей конспирации, не применяя при этом насилия, психического воздействия и иных жестоких приемов в отношении жертвы.

Следует обратить внимание на то, что значительно возрос в последнее время вид преступности, совершаемый в киберпространстве,

¹ Маркеева К.А., Лошкарев А.В. Мошенничество в современном обществе журнал // Международный гуманитарных и естественных наук. 2020. № 5–4 (44). С. 83.

посредством использования сети Интернет в частности. Данная сеть, являющаяся, с одной стороны, средством получения различной необходимой информации в неограниченном объеме и обмена ею, с другой же стороны, таит в себе опасность стать жертвой мошенников, ведь вычислить последнего в таком случае становится практически невыполнимой задачей. Остановимся на способах совершения мошенничеств с использованием информационных технологий.

Сейчас в современном мире проходит процесс цифровизации, набирает темпы технологический прогресс, приводящий к изменению экономики. Данные изменения касаются увеличения информационного объема различной продукции, меньшей площадью, занимаемой электронными носителями, виртуальным характером хозяйственных связей, перемещением товаров и услуг через сеть Интернет, появлением цифровых валют и повсеместного безналичного денежного обращения. Действительно, безналичный денежный расчет, банковские платежные карты активно внедряются в повседневную жизнь каждого человека.

Как было отмечено ранее, вместе с развитием информационных технологий развиваются способы совершения мошеннических действий. Именно владельцы банковских карт нередко становятся жертвами злоумышленников. Рассмотрим наиболее популярные виды мошенничества с использованием банковских карт. Так, одни ученые относят к таким видам мошенничества скимминг, шимминг, фишинг, кардинг, ливанскую петлю, снифферинг, социальную инженерию². Другими учеными выделяются такие способы обмана как скимминг, фишинг, вишинг, траппинг³. Третьи к способам совершения мошенничеств с использованием банковских карт относят вишинг, фишинг, скишинг, фарминг, скимминг, траппинг, шимминг, снифферинг, ливанскую петлю⁴.

² Гришина Е.А. Виды мошенничеств с банковскими картами // Факторы успеха. 2018. № 1 (10). С. 20–23.

³ Урсаева Ю.А., Сорокашвили И.Ю., Зиница О.С. Мошенничество с банковскими картами в современном мире // Научные исследования XXI века. 2020. № 2 (4). С. 106.

⁴ Козодаева О.Н., Обьденнова А.С. Способы совершения мошенничества с использованием банковских карт // Ученые записки Тамбовского отделения РоСМУ. 2019. № 13. С. 52–58.

Как мы видим, такое мошенничество может быть совершенно различными способами, дадим краткую характеристику лишь наиболее распространенным. Скимминг – снимать деньги с банковских карт – способ мошенничества с использованием специального сканирующего устройства, позволяющего злоумышленникам считывать с карты персональные данные ее владельца и номер счета, которые в дальнейшем будут использованы для изготовления поддельной банковской карты. Траппинг – разновидность скимминга, при котором данные с банковской карты не считываются, а лишь используется устройство, позволяющее задержать банковскую карту в банкомате. Мошенники в данном случае осуществляют хищение в то время, пока владелец карты будет разбираться с образовавшейся проблемой в банке. Фишинг и смишинг схожи между собой и проявляются в том, что хищение в данном случае осуществляется посредством поддельных сайтов, во втором случае ссылка на такой поддельный сайт отправляется через SMS. Вишинг – мошенничество с использованием телефонных звонков, в ходе которых жертве сообщается о попытке взлома карты с целью списать имеющиеся на ней денежные средства. После чего мошенники просят позвонить на определенный, заранее подготовленный, продиктованный номер, позвонив по которому впоследствии необходимо будет сообщить, например, пароль от карты. Ливанская петля – вид мошенничества, при котором мошенник, заранее вставив специальное приспособление, удерживающее карту в банкомате, встает в очередь позади жертвы. Пока владелец карты вводит ПИН-код, мошенник, стоя позади, запоминает его. Как только потенциальной жертве не удастся осуществить нужную операцию и извлечь карту, она обращается в банк за помощью. В это время мошенник, пользуясь моментом, вытаскивает банковскую карту и снимает с нее нужную сумму. Снифферинг – способ мошенничества, выражающийся в перехвате персональных данных в людных местах, как правило, через незащищенные wi-fi сети. В качестве таких людных мест мошенники выбирают вокзалы, кафе и другие места. Как мы видим, способов мошенничества с использованием банковских карт большое количество, ведь мошенники легко и достаточно быстро подстраиваются под технологический прогресс, придумывая все новые и новые формы хищений.

На практике не меньший интерес представляет мошенничество, совершенное в сети Интернет. Помимо явных преимуществ,

развитие данной всемирной сети таит в себе и глобальные угрозы, в том числе подрывающие экономическую безопасность государства. Так, мгновенный доступ к необходимой искомой информации, беспрепятственная дистанционная коммуникация, возможность осуществлять онлайн различные денежные переводы и оплату товаров и услуг являются неоспоримыми преимуществами сети Интернет. Но вместе с развитием глобальной сети стремительно развивается и кибермошенничество, представляющее собой одну из экономических угроз XXI в. Помимо указанного фишинга, существуют другие способы обмана и совершения мошенничеств в киберпространстве, например, существование фиктивных Интернет-магазинов, черный инфобизнес, казино и нелегальные букмекеры, кликфрод.

Фиктивные Интернет-магазины отличает то, что они, как правило, работают по стопроцентной предоплате. Нетрудно догадаться, что оплатив полностью товар, произведя денежный перевод, жертва не получит ожидаемый товар. Данный вид мошенничества может касаться не только продажи товаров, но и предложений об оказании различных услуг дистанционно – предложение несуществующих услуг (написание контрольных, других письменных работ, помощь в составлении проектов, гадание, снятие порчи и др.). Впоследствии владелец сайта его либо блокирует, либо меняет доменное имя. Черный бизнес характеризуется продажей жертве информации в различной форме (книги, фото-, видео-файлы) под видом эксклюзивной и редкой, но по факту содержащейся в открытом доступе на различных сайтах. Кликфрод также является разновидностью мошенничества в сети Интернет. Во время поиска необходимой информации пользователь случайно или в результате заинтересованности нажимает на всплывшее рекламное окно, попадая затем на вредоносный сайт. Для выхода с такого сайта и его закрытия злоумышленник просит перевести определенную денежную сумму.

Также в настоящее время в сети Интернет распространен такой вид мошенничества как лже-благотворительность. Суть данного мошенничества состоит в том, что злоумышленники, используя фотографии и информацию, например, о детях, нуждающихся в помощи, голодающих животных, с официальных сайтов благотворительных фондов, действительно стремящихся помочь, рассылают чаще всего в форме спама такие объявления с криком о помощи. Конечно,

деньги, полученные таким путем, ни на какую помощь направлены не будут. В таких случаях пользователям следует помнить о том, что благотворительные фонды никогда не будут распространять действительно важную информацию в форме спама или вывешивания объявлений на сомнительных сайтах. Кроме того, существует отдельный вид мошенничества, наиболее безопасный для таких преступников. Безопасность и благоприятность для мошенников состоит в том, что в результате раскрытия обмана, факта мошенничества, такая жертва никогда не обратится за помощью в правоохранительные органы с целью наказать виновных. К такому виду мошенничества относят предложения о поставке запрещенных наркотических средств, оружия, вплоть до предложений оказать такую услугу как заказное убийство.

Подводя итог, еще раз обратим внимание на то, что владельцам банковских карт и пользователям сети Интернет необходимо проявлять осторожность при пользовании банкоматом в людных местах, мобильной связью, услугами в сомнительных интернет – магазинах, с настороженностью переходить на незнакомые сайты. Безболезненному для населения переходу на массовые безналичные платежи будет способствовать повсеместное повышение финансовой грамотности, кроме того, это поможет ликвидировать недобросовестных онлайн-игроков.

В заключении хотелось бы отметить, что в XXI в. мошенничество не стоит на месте, а идет в ногу со временем, с развитием технического прогресса. В ходе совершенствования и появления новых форм и средств информационных технологий, изобретаются все новые методы и способы мошенничества, хищения чужого имущества. Таким образом, информационные технологии представляют собой не только способы поиска новой информации и развития человека в различных областях науки и техники, но и являются средством совершения более новых и изобретательных видов преступления, мошенничеств в частности. Отсюда следует, что методы борьбы с такими видами преступлений должны соответствовать их уровню развития, в идеале даже быть гораздо более профессиональными.

Кристина Петровна КОЧЕТКОВА

студент

*Санкт-Петербургский юридический институт (филиал)
Университета прокуратуры Российской Федерации*

НЕКОТОРЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В РОССИИ

Аннотация. В данной статье автор затрагивает вопросы противодействия киберпреступлениям. На пороге XXI в. современное общество стало именоваться «информационным», что привело как к положительным, так и к отрицательным факторам – возникновению киберпреступности. Автор раскрывает определение понятия киберпреступления, ссылаясь на международные разъяснения и терминологию российских ученых и правоведов. В УК РФ зафиксированы статьи, связанные с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий. Также установлено, что количество кибератак в России значительно возросло – это подтверждается в представленной статье статистическими показателями. Автор приводит несколько существенных проблем противодействия киберпреступлений, которые значительно тормозят их раскрываемость, и предлагает способы решения данных актуальных вопросов.

Ключевые слова: киберпреступление, информационная безопасность, следователь, противодействие киберпреступлениям.

Kristina Petrovna KOCHETKOVA

student

*St. Petersburg Law Institute (branch)
University of the Prosecutor's Office of the Russian Federation*

SOME PROBLEMS OF COUNTERACTION CYBERCRIME IN RUSSIA

Abstract. In this article, the author addresses the issues of countering cybercrime. At the threshold of the XXI century, modern society became known as «information», which led to both positive and negative factors – the emergence of cybercrime. The author reveals the definition of «cybercrime», referring to international explanations and terminology of Russian scientists and legal experts. The current Criminal code of the Russian Federation contains articles related to attacks on security in the use of information and communication technologies. It is also established that the number of cyber-attacks in Russia has increased significantly – this is confirmed in the article presented by statistical indicators. The author cites several significant problems of countering cybercrime, which significantly inhibit their detection, and suggests ways to solve these topical issues.

Keywords: cybercrime, information security, the investigator, combating cybercrime.

История развития общества претерпела несколько этапов, переход из которых сопровождался значительными изменениями

общественных отношений, сложившихся устоев, экономических связей и в целом всего мира. Эволюция привела к социально-экономическому развитию мира, к возникновению в середине прошлого столетия новых высоких технологий и к необходимости обработки, хранения, распространения огромного потока информации.

На современном этапе общество именуется «информационным», что говорит о прогрессе, о высоких достижениях в информационно-телекоммуникационной сфере. По мнению американского профессора У. Мартина, информационное общество – это развитое постиндустриальное общество, возникшее в 60-70 гг. XX в., в котором ключевым фактором являются информационные технологии, применяемые в производстве, учреждениях, системе образования и быту¹. За столь короткий промежуток времени информационные технологии стали частью жизни каждого человека. Они служат эффективному развитию экономики, политики, медицины, культуры и искусства, играют неотъемлемую роль в повседневной жизни граждан.

Тем не менее, несмотря на такую положительную характеристику информационных технологий, на удобство нахождения информации, обработки и использования, появилась огромная проблема, возникшая перед всем мировым сообществом – киберпреступления. Также проблематика возникновения киберпреступлений характерна и для России.

В российском законодательстве не закреплено официального определения понятия киберпреступления. Кроме того, в современной научной литературе нет единого подхода к тому, как называть данную группу преступлений: компьютерные, информационные, киберпреступления и т.д. Считаем, что наиболее правильно именовать посягательства на безопасность в сфере использования информационно-коммуникационных технологий именно киберпреступлениями, что подтверждается международными разъяснениями и некоторыми российскими учеными. Например, можно обратиться к Докладу X Конгресса ООН по предупреждению преступности и обращению с правонарушителями, в котором кибер-

¹ Теория постиндустриального и информационного общества и его основные представители. URL: <http://wiki1.pskovedu.ru> (дата обращения: 27.10.2020).

преступление выделяется как любое преступление, совершаемое с помощью системы или сети, в рамках компьютерной системы или сети или против компьютерной системы и сети². М.Е. Батухтин пишет, что киберпреступление – это любое преступление в электронной сфере, совершенное при помощи компьютерных средств или виртуальной сети, или против них³. Д.Н. Карпова говорит об общественном явлении так: «киберпреступление – это акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет»⁴. Говоря о киберпреступлениях, стоит дать определение понятию киберпространство. Вокруг данного понятия множество лет ведутся активные дискуссии, но однозначной трактовки до сих пор нет, а в большинстве социологических справочников этот термин вовсе отсутствует⁵. А.Е. Войскунский определяет киберпространство как «наличие некоего мира, обладающего протяженностью и метрикой и представленного в сознании разных людей по-разному. Также в качестве особенности киберпространства он называет хранение неограниченных объемов информации и развлечений, а также предоставление индивидам возможностей для бесчисленных способов самовыражения⁶. Резюмируя, можно сделать вывод, что киберпреступлением является любое преступное деяние,

² Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Сборник документов / сост. А.Г. Волеводз. М., 2001.

³ Батухтин М.Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе: материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов. М., 2018. С. 28.

⁴ Карпова Д.Н. Киберпреступность: глобальная проблема и ее решения. // Власть. 2014. № 8. С. 47.

⁵ Добринская Д.Е. Киберпространство: территория современной жизни // Вестник Московского университета. Сер. 18. Социология и политология. 2018. № 1. URL: <https://cyberleninka.ru/article/n/kiberprostranstvo-territoriya-sovremennoy-zhizni> (дата обращения: 30.10.2020).

⁶ Войскунский А.Е. Метафоры интернета // Вопросы философии. 2001. № 11. С. 64–79. URL: <http://www.relarn.ru/human/cyberspace.html> (дата обращения: 30.10.2020).

совершенное в киберпространстве с помощью компьютерных и информационных технологий.

В настоящей статье будем использовать понятия киберпреступления, кибератаки, IT-преступления как тождественные, поскольку признаки и значения данных понятий схожи.

Действующее уголовное законодательство России не содержит понятия киберпреступление. По нашему мнению, данное понятие объединяет в одну группу различные преступления, так или иначе связанные с использованием информационных технологий. Прежде всего, речь идет о компьютерных преступлениях, ответственность за совершение которых установлена гл. 28 УК РФ:

- неправомерный доступ к компьютерной информации (ст. 272 УК РФ);
- создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

Также в данную группу могут быть включены такие преступления как:

- мошенничество с использованием электронных средств платежа (ст. 159³ УК РФ);
- мошенничество в сфере компьютерной информации (ст. 159⁶ УК РФ);
- неправомерный оборот средств платежей (ст. 187 УК РФ);
- незаконные изготовление и оборот порнографических материалов или предметов (ст. 242 УК РФ) и др.

Анализ судебной и следственной практики показывает, что к самым распространенным преступлениям относятся мошеннические действия в сети Интернет с помощью мобильных телефонов и мобильного банка; тайное хищение денежных средств у банковских организаций или с банковских карт физических лиц с помощью вредоносных программ; неправомерный доступ к компьютерной информации и распространение вредоносных программ.

На сегодняшний день киберпреступность – масштабная проблема всего мира, которой должно уделяться особое внимание.

Для подробного изучения данного явления и четкого понимания актуальности проблемы в настоящий момент следует проанализировать статистику последних трех лет. Россия входит в тройку стран с наибольшим количеством информационных атак. По данным МВД России в 2018 г. зафиксировано около 170 тыс. киберпреступлений, раскрыто всего 43 тыс.⁷. В 2019 г. отмечается значительное увеличение – более 290 тыс. кибератак, что составляет седьмую часть от общего числа преступлений, с потерями в более 10 млрд руб., 142 тыс. из них тяжкие и особо тяжкие, раскрыто всего 65 тыс.⁸. Количество зарегистрированных кибератак на октябрь 2020 г. составляет 363 тыс., или на 77 % больше аналогичного периода прошлого года. Из них 184 тыс. – тяжкие и особо тяжкие, всего 69 тыс. раскрыто⁹. Анализ статистических данных показывает, что в каждом пятом регионе страны число киберпреступлений увеличилось в два и более раз. Регионы с наибольшими темпами прироста зарегистрированных преступлений: Санкт-Петербург, Республика Ингушетия, Новосибирская область. Статистические данные четко показывают стремительно развивающуюся киберпреступность в России за последние годы.

Говоря об актуальности данного вопроса, необходимо отметить, что в июле 2020 г. состоялось заседание Координационного совещания руководителей правоохранительных органов РФ по вопросу «О состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации», на котором Генеральный прокурор РФ И.В. Краснов

⁷ Состояние преступности в России за январь – декабрь 2018 года. М., 2018. С. 7. URL: file:///C:/Users/user/Downloads/Sostoyanie_prestupnosti_2018.pdf (дата обращения: 28.10.2020).

⁸ Состояние преступности в России за январь – декабрь 2019 года. М., 2019. С. 30–36. URL: file:///C:/Users/user/Downloads/Sostoyanie_prestupnosti_yanvary-dekabry_2019.pdf (дата обращения: 28.10.2020).

⁹ Состояние преступности в России за январь – октябрь 2020 года. М., 2020. С. 30–36. URL: file:///C:/Users/user/Downloads/Sb_20_09.pdf (дата обращения: 28.10.2020).

отметил значительные проблемы борьбы с киберпреступлениями. «За последние 5 лет число киберпреступлений возросло в 25 раз»¹⁰, – заметил И.В. Краснов. Генеральный прокурор РФ отметил особо низкую раскрываемость компьютерных преступлений – 25 % из всего количества. Бесконтактный и быстрый способ совершения кибератак делает общество более уязвимым, а органы следствия – не готовыми к нововведениям в киберпреступности. Вследствие низкой раскрываемости преступники чувствуют безнаказанность, вседозволенность, и продолжают криминальную деятельность в компьютерной среде. В завершении заседания Генеральный прокурор РФ И.В. Краснов указал на необходимость эффективно отвечать на вызовы в киберпространстве, использовать инновационные технологии для раскрытия преступлений, предупреждать и прогнозировать их, своевременно устранять правовые пробелы¹¹.

Говоря о киберпреступлениях, следует отметить существование множества вопросов их выявления. Для того чтобы выявить и начать расследование киберпреступления, необходимо зафиксировать факт произошедшего деяния. Одним из поводов для возбуждения уголовного дела, согласно ст. 140 УПК РФ, является заявление о преступлении. Однако проблематичность в установлении преступления создают сами потерпевшие, поскольку часть из них не заявляют о киберпреступлении в соответствующие органы. Причиной этому является страх ухудшения репутации коммерческой организации, если факт киберпреступления будет предан огласке. Организации, предприятия, Интернет-магазины боятся утратить доверие потребителей, став жертвой криминальных киберинцидентов, поэтому тщательно скрывают преступления и не обращаются в полицию. Порой физическое лицо даже не осознает факт того, что оно стало жертвой преступления. Примером незамеченных киберпреступлений может стать незаконное завладение личными данными по-

¹⁰ Генпрокурор России Игорь Краснов провел совещание по теме борьбы с преступлениями, связанными с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий // Генеральная прокуратура Российской Федерации. 17 июля 2020 г. URL: <https://genproc.gov.ru/smi/news/genproc/news-1880616/> (дата обращения: 25.10.2020).

¹¹ Там же.

терпевшего, незаконное копирование информации. Поэтому очень часто потерпевшими от IT-преступлений становятся юридические и физические лица, а в качестве предмета выступают базы данных, информационные сети, серверы. В качестве решения данной проблемы можно предложить активное взаимодействие сотрудников правоохранительных органов со средствами массовой информации, ведение профилактической работы посредством информирования населения через СМИ. Средства массовой информации имеют возможность убедительно и наглядно освещать актуальные вопросы, четко разъяснять существующие проблемы, привлекать общественность к решению задач, стоящих перед органами следствия. Необходимо своевременно объявлять о возможных фактах мошенничества и иных противоправных действиях в информационной сфере. Также необходимо сообщать гражданам о существовании горячих линий, веб-сайтов, которые способны помочь с возникшей проблемой и ответить на актуальные вопросы.

Серьезной проблемой противодействия киберпреступлениям считается несвоевременное принятие решения о возбуждении уголовного дела. Даже если потерпевшие сообщают в правоохранительные органы о совершенном киберпреступлении или информация о нем поступает из иных источников, зачастую, следователи достаточно долго ее исследуют и обрабатывают, проводят длительные проверки. Вопрос о возбуждении дела не решается в течение трех суток, как предусмотрено УПК РФ, вследствие чего утрачивается значительное количество доказательств, что значительно тормозит раскрытие IT-преступлений.

Сотрудники правоохранительных органов нередко сталкиваются с техническими проблемами на этапе выявления преступления. Например, во многих подразделениях на компьютерах и иных устройствах используются устаревшие операционные системы и программное обеспечение. Имеются также определенные проблемы, связанные с подготовкой, назначением и проведением судебных экспертиз. В научной литературе судебная экспертиза в области киберпреступности именуется по-разному. С нашей точки зрения наиболее корректно назвать ее судебной компьютерно-технической экспертизой, в рамках которой существует несколько видов, отличающиеся между собой предметом и объектом исследования. Качественное противодействие

киберпреступности требует высокотехнического оснащения, которое необходимо именно для выявления преступлений, для проведения экспертных исследований. Эффективное применение большого количества специализированных инструментов для идентификации, сбора, сохранения цифровых доказательств приведет к качественной работе экспертных лабораторий в сфере киберпространства. Тем самым необходимо значительно расширять количество современной техники и оборудования.

Наблюдая существенный рост киберпреступлений, отметим возросшее количество кибератак в условиях перевода многих сервисов в онлайн на фоне распространения коронавирусной инфекции, а сотрудников банков, организаций и компаний – на удаленную работу. С каждым днем число киберпреступлений возрастает в десятки раз, появляются новые неизвестные способы шифрования и сокрытия данных преступника, методы и действия мошенников. Пандемия научила IT-преступников работать в совершенно новых условиях. Все неизученные правоохрнительными органами нововведения также значительно тормозят процесс противодействия киберпреступлениям. Зачастую, сотрудники правоохрнительных органов и следователи сталкиваются с большими трудностями, обусловленными ограниченными возможностями. Из-за того что множество сотрудников органов внутренних дел не имеют специального образования в сфере информационных технологий, они не всегда понимают тонкости способа и метода IT-преступления, возможность существования виртуальных следов. Часть следователей подходят к раскрытию киберпреступлений с определенным стереотипом и не осознают, что нужно искать необходимую для раскрытия преступления информацию не только на компьютере, но и на других платформах или облачных серверах, где информация хранится довольно долго. Важно, чтобы следователи понимали то, что следы киберпреступления можно найти в памяти устройств, если приложить к этому особые усилия.

Кроме того, глава Ассоциации защиты бизнеса, сопредседатель Партии роста Александр Хуруджи высказался по этому поводу так: «Для полицейских, работающих с IT-преступлениями, важно обеспечить постоянную экспертную поддержку и непрерывную систему получения новых знаний. Обучать нужно не только полицейских, но

и надзорные органы. Иначе мы получим ситуацию, при которой полицейские удачно ловят киберпреступников, а прокуратура не может обеспечить объективный контроль без новых компетенций¹². Для качественного противодействия киберпреступлениям следователям необходимо прибегать к помощи программистов, IT-специалистов. Решением данной проблемы мы хотели бы привести необходимость получения обязательного дополнительного образования для следователей, расследующих киберпреступления, или своевременную регулярную переподготовку сотрудников правоохранительных органов. Сотрудники будут иметь углубленные знания в компьютерной среде, разбираться в программах безопасности и использовать качественные способы борьбы с кибератаками. Необходимо внедрять специализацию сотрудников, осуществлять их профессиональный отбор. IT-навыки следователей позволят облегчить процесс выявления информационных преступлений на ранних стадиях и значительно увеличат раскрываемость. Примером такого пути решения проблемы является новость, опубликованная официальном сайте МВД России о том, что департамент государственной службы и кадров МВД России совместно с Центральным банком РФ и АНО «Цифровая экономика» подготовила учебный курс в области кибербезопасности. Более 600 полицейских из всех регионов России пройдут подготовку в форме лекций и тренингов, направленных на рассмотрение вопросов технологического обеспечения информационной безопасности. Также акцент будет сделан на практических аспектах расследования киберинцидентов, способах установления личностей мошенников, что позволит снизить рост преступности в сфере IT-технологий¹³.

Кроме того, обратим внимание на иных лиц, участвующих в уголовном процессе, таких как прокуроры и судьи, которые, по нашему мнению, также должны владеть специальными знаниями о киберпреступности и разбираться в информационно-компьютерной среде. Для них необходимо создать учебные курсы для повышения квалификации в области киберпреступности и информационной безопасности.

¹² Полицейских натаскают против онлайн-мошенников. URL: <https://www.kommer-sant.ru/doc/4537640> (дата обращения: 10.11.2020).

¹³ URL: <https://мвд.рф/news/item/21494389/> (дата обращения: 10.11.2020).

Таким образом, понятно, насколько актуальна в настоящее время проблематика преступлений, посягающих на безопасность в сфере использования информационно-коммуникационных технологий. Органы власти упорно следят за киберпреступностью и активно способствуют противодействию данному виду преступлений. Однако значительные проблемы и недочеты остаются. Правоохранительным органам следует регулярно разрабатывать механизмы и методики предотвращения киберпреступности, исследовать программы защиты населения от кибератак и в целом углубленно изучать киберсреду. Необходимо чаще сообщать общественности из средств массовой информации о существовании данной группы преступлений, о возможных атаках и преступных компьютерных нападениях, о том, что делать в такой ситуации, куда обращаться и как гражданам смогут помочь. Кроме того, чтобы избежать нехватки высокопрофессиональных сотрудников в системе следствия, следует увеличить численность IT-специалистов в правоохранительных органах, которые будут качественно отслеживать любое опасное действие в компьютерной сфере. Создать на постоянной основе курсы повышения квалификации для полицейских и следователей (дознателей) по расследованию преступлений данной группы. К тому же, следует организовать полноценный регулярный факультет повышения квалификации для прокурорских работников в области противодействия киберпреступлений и использования информационно-коммуникационных технологий в надзорном производстве. Регулярно обновляемые комплексные знания правоохранительных и надзорных органов будут способствовать эффективному противодействию киберпреступлений, что приведет к снижению числа совершаемых IT-преступлений. Необходимо увеличить и своевременно обновлять материально-техническое оборудование экспертов, повысить технические возможности криминалистических лабораторий, специализирующихся в области киберпреступлений. Общественная безопасность страны – важнейшая задача любого государства, поэтому необходимо тщательно искать и разрабатывать эффективные подходы к противодействию киберпреступлений, которые так мешают развитию современного информационного общества.

Юлия Олеговна КРУЧИНОВА

магистрант

*Среднерусский институт управления –
филиал Российской академии народного хозяйства
и государственной службы при Президенте
Российской Федерации (г. Орел)*

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Аннотация. В статье рассматривается международное сотрудничество в борьбе с киберпреступлениями. Рассматривается сам термин киберпреступления и основной документ в Европе, который регулирует данную сферу.

Ключевые слова: интернет, информация, киберпреступления, преступления, международное сотрудничество.

Yulia Olegovna KRUCHINOVA

graduate student

*Central Russian Institute of Management –
branch of the Russian Presidential Academy
of National Economy and Public Administration (Orel)*

INTERNATIONAL COOPERATION IN FIGHT AGAINST CYBERCRIME

Abstract. This article discusses the international cooperation in the fight against cybercrime. The term cybercrime itself and the main document in Europe that regulates this area are considered.

Keywords: internet, information, cybercrimes, crimes, international cooperation.

Постоянно растущее использование компьютеров и информационно-коммуникационных технологий в мире «электронного всего» открыло ряд новых видов деятельности для совершения преступлений с помощью электронных средств в глобальном масштабе, независимо от национальных и транснациональных границ. Эффективная борьба с такими преступлениями, их расследование и судебное преследование требует международного сотрудничества между странами, правоохрнительными органами и учреждениями, поддерживаемого законами, международными отношениями, конвенциями, директивами и рекомендациями, кульминацией которых является набор международных руководящих принципов по борьбе с киберпреступностью.

Киберпреступность – это транснациональная преступность¹. Безотлагательные меры, необходимые для сохранения данных на национальном уровне, также необходимы в рамках международного сотрудничества.

23 ноября 2001 г. в Будапеште подписана Конвенция о преступности в сфере компьютерной информации² (далее – Конвенция). В настоящее время Конвенция открыта для подписания как государствами – членами Совета Европы, так и не являющимися его членами странами, которые участвовали в ее разработке. В частности, Конвенцию подписали США, Япония и многие другие страны. Россия на данный момент Конвенцию не подписала. Глава III Конвенции о киберпреступности обеспечивает правовую основу для международного сотрудничества с общими и конкретными мерами, включая обязательство стран сотрудничать в максимально возможной степени, безотлагательные меры для сохранения данных и эффективной взаимной правовой помощи.

Преступления в киберпространстве в Конвенции разделены на четыре группы.

В первую группу преступлений, направленных против конфиденциальности, целостности и доступности компьютерных данных и систем, входят: незаконный доступ (ст. 2), незаконный перехват (ст. 3), воздействие на компьютерные данные (противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных) (ст. 4) или системы (ст. 5).

Во вторую группу входят преступления, связанные с использованием компьютерных средств. К ним относятся подлог и мошенничество с использованием компьютерных технологий (ст. 7–8). Подлог с использованием компьютерных технологий включает в себя злонамеренные и противоправные ввод, изменение, удаление или блокирование компьютерных данных, влекущие за собой нарушение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных.

¹ Овчинский В.С. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия. М., 2020. С. 28.

² Конвенция о преступности в сфере компьютерной информации (ETS № 185) (заключена в г. Будапеште 23 ноября 2001). URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#006727637110355822> (дата обращения: 05.11.2020).

Третью группу составляет производство (с целью распространения через компьютерную систему), предложение и (или) предоставление в пользование, распространение и приобретение порнографии, эротики и детской порнографии, а также владение детской порнографией, находящейся в памяти компьютера (ст. 9).

В четвертую группу входят преступления, связанные с нарушением авторского права и смежных прав.

Конвенция дополняется широким спектром других договоров Совета Европы о международном сотрудничестве в уголовных делах.

Важные каналы сотрудничества включают глобальную систему связи Интерпола I-24/7, а также национальные центральные контрольные точки, созданные Интерполом, то есть сеть назначенных следователей, работающих в национальных подразделениях по компьютерным преступлениям в более чем 120 странах.

Кибернетическая деятельность национальных государств, как правило, привлекает к себе наибольшее международное внимание, но на самом деле киберпреступники несут ответственность за большую часть злонамеренной киберактивности – по некоторым оценкам, около 80 % . Помимо прямого ущерба, который, по прогнозам, к 2021 г. будет обходиться мировой экономике в 6 трлн долларов (или 6,3 %) ежегодно, киберпреступность является колоссальным препятствием для цифрового доверия³. Это резко подрывает преимущества киберпространства и препятствует международным усилиям по обеспечению кибербезопасности.

В ответ международное сообщество приняло поощряющие меры по укреплению национального потенциала правоохранительных органов и содействию международному сотрудничеству в борьбе с киберпреступностью – Глобальная программа Интерпола по борьбе с киберпреступностью и Центр инноваций в Сингапуре. Европейский центр по киберпреступности Европола и Совместная целевая группа по борьбе с киберпреступностью являются ведущими результатами этих усилий, равно как и международные политические диалоги, такие как Межправительственная группа экспертов открытого со-

³ Глобальный Ущерб от Киберпреступности, по прогнозам, к 2021 году достигнет 6 триллионов долларов в год. URL: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> (дата обращения: 05.11.2020).

става Организации Объединенных Наций по киберпреступности и Будапештская конвенция Совета Европы⁴.

Однако обычные межправительственные усилия по уголовному правосудию оказываются слишком ограниченными, чтобы справиться с этой задачей. В недавних отчетах подчеркивается «потрясающий пробел в правоприменении» в отношении киберпреступности, и отмечается, что даже в США вероятность успешного судебного преследования киберпреступлений оценивается в 0,05 %, что намного ниже уровня преследования за насильственные преступления⁵.

Систематическое пресечение киберпреступности невозможно без противодействия источнику киберпреступной деятельности и повышения риска преследования правонарушителей. Поскольку одних усилий правительства недостаточно, успешные подходы требуют объединения усилий и ресурсов различных стран.

Таким образом, можно сделать вывод, что киберпреступления – это сложные и опасные действия, положительный результат в борьбе с которыми возможен только при совместных усилиях международного сообщества.

⁴ Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 48.

⁵ To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors. URL: <https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors> (дата обращения: 05.11.2020).

Ирина Сергеевна КУЗНЕЦОВА

студент

Тамбовский государственный университет им. Г.Р. Державина

КИБЕРБУЛЛИНГ КАК СЕРЬЕЗНАЯ ОПАСНОСТЬ В ПРОСТРАНСТВЕ СОВРЕМЕННЫХ СРЕДСТВ КОММУНИКАЦИЙ

Аннотация. В статье рассматривается одна из актуальных, социальных проблем современного цифрового общества – кибербуллинг. Кибербуллинг – новая, быстро распространяющаяся как в России, так и за рубежом форма травли, которая использует средства коммуникации для агрессивного преследования, угнетения человека. Исследуется явление кибербуллинга, его понятие, причины, особенности, способы реализации в киберпространстве, а также рассказываются реальные истории жертв Интернет-травли. В статье подчеркивается чудовищность последствий кибертравли, которая заключается в том, что об этом никто не говорит и, как правило, просят помощи уже слишком поздно.

Ключевые слова: виртуальный мир, травля, киберпространство, кибербуллинг, Интернет, средства коммуникации.

Irina Sergeevna KUZNETSOVA

student

Tambov State University named after G.R. Derzhavin

CYBERBULLYING AS A SERIOUS DANGER IN THE SPACE OF MODERN MEANS OF COMMUNICATION

Abstract. The article deals with one of the most urgent social problems of modern digital society – cyberbullying. Cyberbullying is a new form of bullying that is rapidly spreading both in Russia and abroad, using the means of communication to aggressively harass and oppress people. The article explores the phenomenon of cyberbullying, its concept, causes, features, and methods of implementation in cyberspace, as well as tells the real stories of victims of Internet bullying. The article highlights the enormity of the consequences of cybertravel, which is that no one talks about it and, as a rule, they ask for help too late.

Keywords: virtual world, bullying, cyberspace, cyberbullying, Internet, means of communication.

Стремительное развитие общественных отношений, институтов, их информатизация и цифровизация, научно-технический прогресс влекут за собой не только преимущества, но и недостатки. Высокие результаты в области науки и техники, создание всемирной

компьютерной сети Интернет дали большие возможности преступникам выйти на новый, наиболее сложный и профессиональный уровень и овладеть киберпространством. Теперь преступник стал латентным, незаметным, скрытым, невидимым и особо опасным для каждого, кто является пользователем всемирной сети Интернет, для крупнейших организаций и даже целых государств.

Сегодня пространство ежедневного общения образует новую яркую особенность – распространение в виртуальном мире. Для взрослого поколения навыки общения в так называемых мессенджерах – надстройка над приобретенными навыками общения вживую, то для современных детей, подростков это нормальный, привычный стиль общения, который осваивается одновременно и с другими навыками.

«Онлайновая виктимизация может проявляться в разных формах»¹. Часто обсуждаемыми являются мошенничество, кража личных данных. Также дети и молодежь, которые имеют легкий доступ в киберпространство и совсем не подготовлены к рискам, могут стать жертвами страшных преступлений в сети Интернет, к примеру, торговли людьми и т.д. На данный момент молодое поколение сталкивается с кибербуллингом, а именно проблемой преследования, запугивания со стороны, чаще всего, своих ровесников.

Кибербуллинг как социальная проблема, безусловно, нуждается в обсуждении и поиске методов и способов решения. Кибербуллинг – новая современная и быстро распространяющаяся как в России, так и за рубежом форма травли, которая использует современные средства коммуникации для агрессивного преследования, угнетения человека. «Джудит Донат трактует троллинг как игру в подделку личности, при этом никто, кроме играющего, о ней не знает»².

«Как отмечала в 2010 г. Всемирная организация здравоохранения, кибербуллинг является серьезной проблемой общественного здравоохранения, влияя на психическое и физическое здоровье детей

¹ *Коданева С.И.* Кибербуллинг: причины явления и методы предупреждения // Социальные новации и социальные науки. 2020. С. 150.

² *Бобровникова Н.С.* Опасность интернета – кибербуллинг // Восточно-Европейский научный вестник. 2015. № 1 (1). С. 7.

и подростков во всем мире. По данным Всемирной организации здравоохранения 2017 г, депрессия является третьей ведущей причиной болезней и инвалидности среди подростков, а самоубийство – третьей причиной преждевременной смерти в этой возрастной группе»³. Особо сильно эти тягостные формы поведения протекают в возрасте 12–18 лет, когда происходит становление личности – процесс социализации.

На данный момент приблизительно 30 % детей в какой-либо степени подвергались кибертравле. Так, уполномоченный при Президенте РФ по правам ребенка Анна Кузнецова считает, что ужесточение ответственности за распространение различных материалов, содержащих сцены насилия над детьми, является одним из способов решения рассматриваемой проблемы.

Для полного понимания негативных последствий и опасности кибербуллинга следует отметить причины его наступления: демонстрация силы либо стремление к превосходству; комплекс неполноценности – наличие чувства самоущербности; зависть – скрытое соперничество, когда человек жаждет победить; скука; «месть – действия, произведенные из побуждения адекватно ответить на реальную или мнимую несправедливость, причиненную ранее; развлечение»⁴.

Травля – это систематическое, регулярное преследование, терроризирование, унижение, оскорбление, к примеру, в школе, на работе, через Всемирную сеть и т.д. При травле классическими являются следующие действия: распространение заведомо ложной информации, то есть сообщение каких-либо сплетней, слухов о человеке, провокации, издевки, насмешки, колкости, прямые угрозы, запугивание, социальная изоляция, например, игнорирование, нападки, которые ущемляют честь и достоинство человека, причинение физического либо материального вреда.

Интернет-травля происходит непосредственно в информационном пространстве через конкретные информационно-коммуникационные средства и каналы: с помощью электронной почты,

³ Коданева С.И. Указ. соч. С. 150.

⁴ Ефимов Ю.А. Причины кибербуллинга и способы борьбы с данным явлением // Новые вопросы в современной науке. 2017. С. 360–361.

программ для общения в социальных сетях (ICQ); посредством размещения на видеопорталах (YouTube) спорных материалов либо мобильного телефона (назойливые звонки).

Лица, совершающие рассматриваемые противоправные действия, как правило, действуют анонимно, поэтому жертва не может знать и предположить, кто по отношению к ней проявляет агрессию. Отметим, что согласно новым исследованиям, «почти половина подростков (49 %) совершали агрессивные действия в Интернете, и более половины (61 %) подвергались киберагрессии»⁵.

Подчеркнем особенности кибербуллинга: анонимность, неизвестность, постоянность, невидимые свидетели, завуалированность, неимение обратной связи, «феномен растормаживания»⁶.

«Известный американский программист Алан Купер, «отец Visual Basic», выделил три аспекта Интернет-коммуникации и назвал их принципом Triple A – anonymous, accessible, affordable (анонимность, доступность и «дешевизна» компьютерно-посредованной коммуникации)»⁷.

Как уже отмечено выше, в типичной травле, агрессор известен и его можно миновать, в киберпространстве же преследователь чаще всего анонимен. Жертва не знает о нем ничего: ни количество, ни пол, ни возраст и т.д. Данная неясность, неконкретность только увеличивает тревогу, жертва начинает воображать образ преследователя, фантазировать о его силе, мощи, власти и на основании этого – «о собственной незащитности и уязвимости, опираясь на свой личный прошлый опыт, персональные переживания»⁸. Следовательно, кибертравля очень опасна, в первую очередь, для детей и подростков, которые уже имеют психологические травмы, душевные потрясения либо переживают из-за недопонимания, разногласий в семье.

Интересно выделить особенности жертв Интернет-травли. Обычно такие жертвы – дети, имеющие в реальной жизни про-

⁵ Коданева С.И. Указ. соч. С. 150.

⁶ Бочавер А.А., Хломов К.Д. Кибербуллинг: травля в пространстве современных технологий // Психология. Журнал Высшей школы экономики. 2014. Т. 11. № 3. С. 185.

⁷ Шевко Н.Р., Исхаков И.И. Особенности проявления кибербуллинга в социальных сетях // Ученые записки Казанского юридического института МВД России. 2017. Т. 2. № 3. С. 20.

⁸ Бочавер А.А., Хломов К.Д. Указ. соч. С. 185.

блемы похожего характера. В основном, преследователь обращает внимание на внешний вид, к примеру, очень толстый или худой. Большое число жертв и их неприятелей приходится на возраст между 11 и 16 годами – период полового созревания или пубертатный период, в процессе которого отмечается эмоциональность, чувствительность к различным неудачам, оскорблениям, острое восприятие реальности. Например, Джуди Румб – обычная пятнадцатилетняя девочка, которая отличалась от своих сверстников наличием лишнего веса. Одноклассники посчитали ее не такой как все и начали третировать. Кульминация истории – создание сайта, который был посвящен избыточному весу этой бедной девочки, где был установлен счетчик дней, оставшихся жить Джуди.

«Жертва кибербуллинга переживает особое состояние расстройства нервной системы: сильный стресс, вызванный осознанием полной беспомощности, который влияет на общие показатели здоровья, снижение самооценки»⁹. Кроме того, многие пользователи современных средств коммуникации зачастую не распространяются, что стали жертвами кибертравли, так как боятся осуждения, непонимания, полной социальной изоляции, тем самым совершая огромную ошибку решить сложившуюся ситуацию самостоятельно, ведь по данным статистики это приводит, нередко, к таким чудовищным последствиям, как самоубийство.

В доказательство названного положения отметим истории Реты Парсонс и Одри Потт, получившие известность по всему миру. Во Всемирную сеть были загружены фотографии изнасилования канадки Рета Парсонс. Затем в Интернете появилась отдельная страница, на которой четверо парней подробно, не стесняясь деталей, описывали произошедшее и различно унижали, оскорбляли девушку. Семнадцатилетняя Рета не выдержала позора и повесилась.

Одри Потт – калифорнийская школьница. После бурной вечеринки пятнадцатилетняя девочка проснулась вся исписанная черным маркером. В дальнейшем в Интернет выложили фотографии, видеозаписи, где она подверглась сексуальному насилию и издевательствам со стороны пьяных ребят. Ситуация обострилась, когда пользователи

⁹ Кувшинова А.А. Конфликты в социальных сетях: кибербуллинг // Актуальные проблемы современной психологии и педагогики: сборник научных статей. Нефтекамск, 2017. С. 55.

Сети поддержали данную выходку и заявили, что Одри в произошедшем виновата сама. Такого мнения были и ее подруги, с которыми в тот роковой вечер девушка пришла на вечеринку. Через несколько дней после вечеринки Одри Потт, не выдержав травли со стороны одноклассников, пользователей социальных сетей повесилась.

Одри Потт, Рета Парсонс – одни из многих подростков, чьи жизни оборвались в результате кибербуллинга или Интернет-травли. Сегодня аналогичных примеров достаточно много, что, безусловно, приводит в ужас и должно быть предано широкой огласке, ведь последствия кибертравли дикие, жестокие, их чудовищность заключается, прежде всего, в том, что об этом никто не говорит и обычно просят помощи только когда становится очень поздно. Кибербуллинг не случайно называют «чумой двадцать первого века» из-за повсеместного характера его распространения, не зависящего от временных или географических рамок»¹⁰.

Истории, которые произошли с названными девушками, легли в основу сюжета современного фильма ужасов «Убрать из друзей».

Важно подчеркнуть, что в настоящее время в России законодательно не регламентировано такое общественно опасное деяние как кибербуллинг, но есть действующий Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», регулирующий отношения, которые возникают непосредственно в условиях пользования Интернетом. Кроме того, обратим внимание на распространение телефонов горячих линий, конкретные группы в социальных сетях, где люди могут получить консультацию по интересующему их вопросу. Однако этого недостаточно, чтобы эффективно бороться с кибертравлей. Государственным органам следует широко освещать и решать проблемы кибербуллинга.

Решить проблему травли в киберпространстве может создание проектов, преследующих агрессоров и защищающих их жертв. «В России уже созданы «Дети онлайн» и «Дружественный рунет», деятельность которых связана с борьбой против кибербуллинга»¹¹.

¹⁰ Кувшинова А.А. Указ. соч. С. 57.

¹¹ Парфеленко А.А., Шарытова Т.Н. Кибербуллинг – травля в сети // Наука сегодня: вызовы и решения: материалы международной научно-практической конференции. Вологда, 2018. С. 160.

Угрозы, которые сегодня исходят из социальных сетей потенциально, реально и очевидно, обладают высокой степенью общественной опасности. Для устранения данных угроз безопасности общества в целом, логично внести доработки в УК РФ, а именно вновь криминализировать ст. 130 УК РФ в части закрепления понятия оскорбления несовершеннолетнего, особенно путем использования сети Интернет, и внести некоторые поправки, пресекающие возможные попытки некомпетентности сотрудников государственных организаций. В свою очередь, на основании примеров других развитых стран (например, Японии) запретить выход в Интернет детям без установки особого программного обеспечения и фильтров, то есть разработать «свой» закон о поддержке здоровой Интернет-среды для молодежи.

Таким образом, кибербуллинг – одна из серьезных опасностей в пространстве современных средств коммуникации, которая, безусловно, нуждается в обязательном разрешении. Сегодня по всему миру миллионы детей и подростков продолжают страдать от Интернет-травли, держа все в себе и пытаясь решить проблемы самостоятельно, не прося у взрослых помощи или, что очень печально и грустно, обращаясь и не находя ее. Но известно, что игнорирование проблемы – не есть ее решение, она все равно остается, лишь только нарастает, как снежный ком, до того времени, пока не уничтожит всех со своего пути, обновив новыми, очередными некрологами страницы газет. На данный момент важно построить максимально, предельно продуктивную, эффективную превентивную программу борьбы с кибербуллингом или кибертравлей. Также обществу следует научиться сочувствовать, сопереживать, сострадать и помогать жертвам травли, а именно жертвам унижения и преследования в киберпространстве.

Мария Сергеевна КУРБАТОВА

курсант

*Московский университет Министерства внутренних дел
Российской Федерации им. В.Я. Кикотя*

ОБЛАЧНЫЕ СЕРВИСЫ ХРАНЕНИЯ ДАННЫХ КАК ОБЪЕКТ ПРЕСТУПНОГО ПОСЯГАТЕЛЬСТВА В СОВРЕМЕННОМ МИРЕ

Аннотация. Рассматриваются облачные сервисы хранения данных, механизмы работы облачных хранилищ данных, анализируются способы хищения данных из «облака» у организаций и частных лиц, приводятся способы защиты данных хранящихся на облачных сервисах.

Ключевые слова: облачные сервисы, облачные технологии, «облако», хранилища данных, Mega, Google Диск, Яндекс Диск.

Maria Sergeevna KURBATOVA

*Moscow University of the Ministry of Internal Affairs
of the Russian Federation of the V.Ya. Kikot*

CLOUD DATA STORAGE SERVICES AS AN OBJECT OF CRIMINAL ENCROACHMENT IN THE MODERN WORLD

Abstract. The main approaches of cloud data storage services, how cloud data storage works, analysis ways to steal data from the «cloud» from organizations and individuals, ways to protect data stored on cloud services are given.

Keywords: cloud services, cloud technologies, «cloud», data store, Mega, Google Drive, Yandex Disk.

Облачные сервисы хранения данных достаточно быстро набирают популярность среди пользователей во всем мире. Это обуславливается удобством использования данного вида хранилища, а именно его доступностью, масштабируемостью и возможностью сохранения большого объема данных. Под технологией облачного хранения понимается возможность сохранять необходимую информацию пользователя в онлайн хранилище удаленного сервера, причем доступ к такой информации можно получить из любой точки мира, достаточно иметь лишь возможность подключения к сети Интернет¹. По мнению аналитиков компании Falcongaze, специ-

¹ Клементьев И.П., Устинов В.А. Введение в Облачные вычисления, М., 2016. С. 310.

ализирующей в области информационной безопасности, наиболее безопасными облачными сервисами хранения данных на 2020 г. являются следующие².

1. **Мега** – используется сквозное шифрование данных непосредственно на устройстве пользователя до момента выгрузки их на сервер. Ключи шифрования имеются лишь у владельца данных, также владелец самостоятельно определяет право доступа к данным иных лиц. Расшифровать хранящиеся на сервере данные хакеры не имеют возможности. Также доступ к паролю имеет лишь владелец аккаунта, в случае его утраты или если владелец его забыл, то с помощью стандартной процедуры проверки почты или номера телефона сделать это будет невозможно. Единственным вариантом восстановления доступа к сервису является использование предварительно созданного ключа восстановления. Его необходимо хранить на секретном флэш-носителе, в случае утраты которого доступ к данным будет потерян навсегда. Компания делает ставку на сохранность пароля самим пользователем лично. Уязвимостью может являться заражение устройства вирусом или кейлогером. Кейлогер – это программное обеспечение, перехватывающее нажатие клавиш устройства, в итоге, он сохраняет данные логина и пароля. Также присутствует двухфакторная аутентификация.
2. **Google Диск** – используется криптографический протокол шифрования SSL, обеспечивающий безопасную связь между сервисом и клиентом, имеет режимы разграничения доступа, двухфакторную аутентификацию, а также возможность использования физического электронного ключа для дополнительной защиты данных. Однако такое средство защиты доступно лишь бизнесменам, политикам, писателям, но не обычным гражданам.
3. **Яндекс Диск** – используется передача данных через защищенное соединение SSL. Данные, загруженные на сервер, автоматически проверяются на наличие вирусов. В случае утери устройства, на котором выполнен вход в аккаунт, имеется возможность от-

² Самые безопасные облачные хранилища 2020 URL: <http://www.itcsme.ru/PressReleaseitcsme/PressReleaseShow.asp?ID=718777/> (дата обращения: 07.11.2020).

ключить доступ к облачному хранилищу всех программ и приложений. Возможности очистить историю действий нет, что позволяет отследить, кто получал доступ к данным. Сотрудники правоохранительных органов имеют возможность получить доступ к дешифрованным сообщениям пользователей в рамках, установленных законодательством РФ.

Для более полного представления данной технологии необходимо рассмотреть механизм работы облачных хранилищ³. С помощью специализированного программного обеспечения пользователь выбирает файл, который необходимо сохранить в «облаке». Далее нужный файл копируется на удаленный сервер. Получить доступ к нужным данным пользователь может через Web-сайт сервиса, предоставившего возможность хранения данных. Стоит отметить, что данные хранятся не на одном сервере, а на множестве таких серверов, расположенных в различных точках планеты. Получить доступ к своим данным с другого устройства, к примеру, телефона, компьютера, планшета, можно с помощью входа в учетную запись пользователя, этим и обуславливается высокая масштабируемость данного хранилища данных. Однако у данной модели хранения данных имеется ряд недостатков, которые не позволяют использовать ее повсеместно. Сбои в подключении к Интернету могут привести к невозможности работы с данными, нередко имеет место быть и халатность Интернет-провайдера. По этой причине в организациях использование облачных сервисов в качестве резервного хранилища данных является достаточно полезным, что предотвращает возможность полного уничтожения данных. В качестве эталонной модели целесообразнее всего использовать «гибридное облако», представляющее собой совместное хранение данных на облачных серверах и в локальной сети организации. Это позволяет предотвратить полную утрату данных при критических сбоях в локальной инфраструктуре.

Облачные сервисы хранения данных могут являться объектом преступного посягательства. Опасность использования таких

³ Облачные системы хранения. URL: <https://itelon.ru/blog/oblachnye-sistemy-khraneniya/> (дата обращения: 08.11.2020).

сервисов обуславливается в утечке информации. В случае неправомерного доступа к каким-либо данным организации имеется риск утери конфиденциальной информации. В любой компании имеются персональные данные сотрудников, а также клиентов. Предоставляя паспортные данные, любую другую личную информацию, клиент дает право использовать эти данные организации. Любая утечка хранящихся данных в облачных хранилищах вызывает негативную реакцию со стороны клиента, а также подрывает и репутацию самой компании⁴. В случае доступа хакера к данным компании, хранящимся в «облаке», может быть разглашена и другая тайна (коммерческая; профессиональная: врачебная, адвокатская; банковская) в зависимости от специфики работы организации. Имеют место также DDoS-атаки со стороны злоумышленников. В результате нее конечный пользователь не имеет возможности получить доступ к необходимым ему данным в нужное время. DDoS-атака или распределенный отказ в обслуживании представляет собой вектор атаки при котором сервис, в нашем случае облачное хранилище, перезагружается огромным количеством запросов, причем такие запросы поступают с большого числа устройств, имеющих различные IP-адреса и местоположение.

В случае реализации атаки на частных лиц злоумышленники имеют иные цели. Чаще всего преступники используют шантаж, желая получить от лица денежные средства за нераспространение каких-либо личных данных, фото/видеоматериалов, документов лица. Причем лицо, возможно, незаметно разместило информацию в облачном хранилище или же даже не подозревает о хранении таковой в «облаке». К примеру, популярный среди владельцев техники Apple сервис iCloud может автоматически выгружать данные в облако.

Согласно Конституции РФ права и свободы человека, являются высшей ценностью. Личные права человека гарантированы ст. 20–29 Конституции РФ. Данный перечень статей является главенствующим и лежит в основе правового статуса человека и гражданина. В ст. 23 основного закона страны закреплено право на тайну переписки, телефонных переговоров и иных сообщений. Ограничение

⁴ ThreatZone Иллюзия безопасности, М., 2019. С. 77.

данной правовой нормы допускается лишь по решению суда. В ст. 24 Конституции РФ закрепляется охрана частной жизни лица от сбора информации, лицо должно знать, что предоставленные данные будут использоваться в открытых источниках и дать свое согласие на данное использование. Таким образом, распространение любой информации, содержащей сведения о личности, не являющиеся общедоступными (если гражданин не сам предоставил их широкому кругу лиц), является вторжением в личную жизнь и нарушением права человека.

В данном случае любому гражданину предоставляется возможность самому контролировать объем информации, содержащейся в открытых источниках, а также данные о своей личности и какие-либо подробности частной жизни. Нарушение таких прав преследуется в соответствии с УК РФ.

Рассмотрим, каким образом злоумышленник может получить доступ к личным данным «облачных» сервисов. Для доступа к облачному хранилищу пользователю необходимо пройти процедуру авторизации⁵. Злоумышленнику достаточно знать такие данные пользователя, как логин и пароль. Киберпреступники для достижения своей цели часто используют методы социальной инженерии. В этом случае нет необходимости в использовании сложных программно-аппаратных комплексов для реализации атаки и подбора пароля. Достаточно лишь ввести в заблуждение владельца аккаунта облачного хранилища таким образом, чтобы он самостоятельно передал нужную информацию злоумышленнику. В связи с этим создание надежного пароля является необходимым. Использование какой-либо личной информации при создании пароля является нежелательным, хранение паролей на бумажных и электронных носителях информации также может привести к возможности быть доступными третьим лицам. В то же время имеет место и уязвимость в интерфейсах самих программ, позволяющих реализовать возможность облачного хранения данных.

Количество пользователей облачных хранилищ данных увеличивается ежегодно. Такими пользователями являются как организации, так и частные лица. В связи с этим преступники стремятся

⁵ SecureNews. URL: https://securenews.ru/cloud_data/ (дата обращения: 06.11.2020).

получить какие-либо личные данные, преследуя материальную выгоду или желая нанести ущерб репутации компании. Преступники могут использовать различные способы осуществления атак: методы социальной инженерии, уязвимости в программном обеспечении, использование вредоносных программ, а также халатность сотрудника или лица. Необходимо реализовывать комплексный подход к обеспечению безопасности, заключающийся в повышении уровня информационной, правовой грамотности населения, а также комплексной проверки безопасности отдельной системы.

Александр Олегович ЛУКАШОВ

аспирант

Московский финансово-юридический университет МФЮА

О ПРАКТИКЕ СУДЕБНОЙ ЗАЩИТЫ ДЕЛОВОЙ РЕПУТАЦИИ В СЕТИ ИНТЕРНЕТ

Аннотация. В статье исследуется гражданское законодательство, а также современная судебная практика по делам о защите деловой репутации, опороченной в сети Интернет. Дается характеристика правовым позициям судов первой, апелляционной и кассационной инстанций по данной теме.

Ключевые слова: деловая репутация, интернет, судебная практика, права человека, информация.

Aleksandr Olegovich LUKASHOV

graduate student

Moscow Finance and Law University MFUA

ABOUT THE PRACTICE OF JUDICIAL PROTECTION OF BUSINESS REPUTATION ON THE INTERNET

Abstract. The article examines the civil legislation, and modern judicial practice about the protection of business reputation defamed on the Internet. The characteristic is given to the legal positions of the courts of the first, appeal and cassation instances on this topic.

Keywords: Business reputation, Internet, judicial practice, human rights, information.

С повышением доступности и популярности сети Интернет, и, как следствие, количества информации, доступной к просмотру неограниченному кругу лиц, вопрос защиты такого нематериального блага как деловая репутация, встает как никогда остро. В связи с тем, что в настоящее время пользователи Интернет-ресурсов активно используют функции оставления отзывов на многочисленных тематических каналах и сайтах, сложно спрогнозировать, какое именно сообщение получит особое распространение или общественный резонанс.

Так как деловая репутация компании находится в прямой связи с мнениями конечных пользователей, логичным является, что организации крайне заинтересованы в применении положений гл. 8 ГК РФ, содержащей описание понятия «нематериальное благо» и порядка его защиты.

При рассмотрении данной категории дел суду приходится балансировать между следующими правами, требующими защиты: правом на защиту частной жизни, чести, достоинства и деловой репутации и правом на свободу мысли и слова, распространение информации законным способом, правом на обращение в государственные органы и органы местного самоуправления (ст. 23, 29, 33 Конституции РФ), а также на свободу массовой информации (Обзор судебной практики Верховного Суда РФ № 3 (2019))¹.

Судебный способ защиты деловой репутации является следствием отказа участника гражданско-правовых отношений от добровольной реализации своей ответственности. Как пишет по данному поводу Ж.Ю. Юзефович, «Добровольная форма реализации ответственности предусматривается во многих законодательных актах, в том числе и в Конституции РФ. Более того, хотя принудительная реализация функций ответственности сопряжена с государственным принуждением, и в ней также имеются элементы добровольности исполнения обязанностей, то есть реализации собственной воли лица по отношению к тому, чтобы следовать нормам ответственности, ограничивающим его поведение, и возможностью собственными усилиями привести нарушенное правоотношение в нормальное состояние. Государство, устанавливая обязанности, рассчитывает на их добровольное исполнение, так как видит в субъектах права не правонарушителей, а законопослушных граждан, предполагая тем самым возможность добровольной формы реализации ответственности, то есть добровольная форма реализации функций юридической ответственности может занимать значительное место в системе этой реализации»².

Анализ материалов судебной практики в целом свидетельствует о сложившемся единообразии в рассмотрении дел данной категории, однако возникающие у суда вопросы подтверждают необходимость обратить внимание на следующее.

¹ Обзор судебной практики Верховного Суда Российской Федерации № 3 (2019) (утв. Президиумом Верховного Суда РФ 27 ноября 2019 г.). URL: <https://www.vsrfg.ru/documents/practice/28477/> (дата обращения: 23.09.2020).

² Юзефович Ж.Ю. Функции юридической ответственности и формы их реализации по российскому законодательству. автореферат дис. ... канд. юрид. наук. М., 2004.

При рассмотрении спора по делу истец указал, что неустановленными лицами на странице сайта <https://otzovik.com> в сети Интернет по указанным Интернет-ссылкам опубликованы сведения об обществе, которые содержат сведения, не соответствующие действительности и порочащие деловую репутацию заявителя³.

Мотивируя свои требования, истец ссылаясь на размещение спорной информации на сайте otzovik.com. Судом отмечено, что указанный сайт является информационным, созданным с целью предоставлять возможность общения и обмена информацией, размещать мнения пользователей относительно качества товара, выполнения работ, оказания услуг. Также судом указано, что любой гражданин вправе высказать свое мнение относительно восприятия им того или иного понятия.

В Определении Верховного Суда РФ от 22 июля 2014 г. № 60-КП4-4 говорится что согласно п. 1 ст. 10 Конвенции о защите прав человека и основных свобод⁴ каждый имеет право свободно выражать свое мнение. Это право включает свободу придерживаться своего мнения и свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ.

Европейский Суд по правам человека также указал, что свобода выражать свое мнение, как она определена п. 1 ст. 10 Конвенции, является одной из ключевых основ демократического общества, принципиальным условием его прогресса и самореализации каждого члена общества. Свободой слова охватываются как информация и идеи, воспринимаемые в обществе благоприятно или же по крайней мере, как безобидные либо нейтральные, но кроме того и те, которые могут оскорбить, шокировать или внушить беспокойство. Этого требуют плюрализм, толерантность и либерализм, без которых невозможно нормальное функционирование демократического общества.

³ Решение Арбитражного суда г. Москвы от 27 декабря 2019 г. по делу № А40-271306/19-5-2158. URL: <https://sudact.ru/arbitral/court/reshenya-as-goroda-moskvy/> (дата обращения: 23.09.2020).

⁴ Конвенция о защите прав человека и основных свобод (Заключена в г. Риме 4 ноября 1950 г.) (с изм. от 13 мая 2004 г.) (вместе с Протоколом № 1. Подписан в г. Париже 20 марта 1952 г.) // СПС «КонсультантПлюс». URL: <http://www.consultant.ru> (дата обращения: 24.09.2020).

Таким образом, суд указал, что оценочные суждения, а также суждения негативного, критического или иного отрицательного характера, сами по себе не образуют возникновения безусловной обязанности по их опровержению в порядке ст. 152 АПК РФ.

Касательно лиц, распространивших оспариваемые сведения, в Постановлении Девятого арбитражного апелляционного суда от 19 марта 2020 г. № 09АП-6092/2020⁵ по делу № А40-271306/2019 указано, что при отсутствии доказательств, что лица, распространившие оспариваемые сведения, обладают достаточными специальными познаниями в вопросах технического устройства фильтров для воды, спорная информация является лишь оценочными суждениями потребителей о фильтрах для воды, а не утверждениями а фактах, которые можно было бы проверить в судебном порядке.

В постановление Арбитражного суда Московского округа от 7 июля 2020 г. № Ф05-9778/2020⁶ по данному делу указывается, что категоричность изложенного частным лицом мнения о товаре либо продавце не является основанием для признания такого мнения не соответствующим действительности и/или порочащим утверждением о фактах или событиях.

Также суд округа отклонил ссылку заявителя на возмездный характер размещения отзывов, поскольку вывод о целенаправленной публикации негативных отзывов при прочих равных условиях является предположительным, вследствие чего не опровергает правильность и обоснованность изложенных в обжалуемых судебных актах выводов судов.

Таким образом, судами был сделан вывод о том, что высказывания, которые привел заявитель в качестве основания своих требований, являются по своей сути частным мнением, суждением авторов отзывов, а не утверждением о фактах.

⁵ Постановление Девятого арбитражного апелляционного суда от 19 марта 2020 г. № 09АП-6092/2020 по делу № А40-271306/2019 // СПС «Консультант-Плюс». URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=MARB&n=1843526#019801961295807957> (дата обращения: 24.09.2020).

⁶ Постановление Арбитражного суда Московского округа от 7 июля 2020 г. № Ф05-9778/2020 по делу № А40-271306/2019 // СПС «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/41986807/> (дата обращения: 23.09.2020).

При разрешении спора по делу № А41-63477/2019⁷ истец обратился в арбитражный суд Московской области с требованием признать сведения, опубликованные на Интернет-сайте, в разделе «наша оценка» – 1 бал, носящими порочащий характер и не соответствующими действительности. Как указано истцом, размещение ответчиком на своем сайте оценочной информации о качестве деятельности ООО УК «МИКО» может сформировать неблагоприятное общественное отношение к деловой деятельности истца и нанести ему репутационный вред.

При рассмотрении данного спора, суд пришел к выводу, что оспариваемые сведения в виде оценки (цифры) «1» сами по себе не содержат информации о каких-либо фактах и событиях, касающихся деловой репутации истца, а также информации о деловых качествах или негативных утверждений, которые могли бы вызвать определенную оценку в общественном мнении.

Кроме того, суд отметил, что истцом не представлено доказательств, подтверждающих факт нанесения репутационного ущерба, который вызван спорным заявлением ответчика

В постановлении Десятого арбитражного апелляционного суда от 10 декабря 2019 г. № 10АП-21958/2019⁸ по данному делу также указано, что оценочные суждения об истце, даже в том случае, если они носят обидный характер, тем не менее являются выражением субъективного мнения ответчика, и таким образом, не могут быть проверены на предмет соответствия их действительности. Исходя из вышеизложенного, факт распространения спорных сведений в сети интернет не может стать причиной удовлетворения иска о защите деловой репутации.

При рассмотрении спора по делу № А40-181225/2019⁹ публичное акционерное общество «Транснефть» обратилось с иском

⁷ Решение Арбитражного суда Московской области от 7 октября 2019 г. по делу № А41-63477/2019. URL: <https://sudact.ru/arbitral/court/reshenya-as-moskovskoi-oblasti/> (дата обращения: 23.09.2020).

⁸ Постановление Десятого арбитражного апелляционного суда от 10 декабря 2019 г. № 10АП-21958/2019 по делу № А41-63477/2019. URL: <https://10aas.arbitr.ru/> (дата обращения: 23.09.2020).

⁹ Решение Арбитражного суда г. Москвы от 11 ноября 2019 г. по делу № А40-181225/19-110-1589. URL: <https://sudact.ru/arbitral/court/reshenya-as-goroda-moskvy/> (дата обращения: 23.09.2020).

о защите деловой репутации к закрытому акционерному обществу «Редакция “Независимой газеты”», Истец требовал признать не соответствующими действительности и порочащими деловую репутацию сведения, которые содержались в статье «Будем компандировать» Правда о “грязной” нефти», размещенной ответчиком в сети Интернет.

При разрешении данного спора судом установлен факт о том, что ПАО «Транснефть» имеет устойчивую положительную деловую репутацию. Истцом представлены достаточные доказательства, которые подтверждают данный факт. А именно: показатели рейтингов, составленных международными агентствами, а также положительные оценки деятельности истца в отзывах профессионального общества и контрагентов.

Также суд отметил, что спорная статья касается сферы предпринимательской деятельности и репутации истца как транспортировщика нефти и нефтепродуктов, в связи с чем, ответчики не могут апеллировать к ст. 10 ЕКПЧ¹⁰. Данной статьей журналистам предоставлены гарантии касающиеся распространения сведений по вопросам всеобщего интереса только в случаях, когда они действуют добросовестно и с целью предоставления точной и достоверной информации, руководствуясь журналистской этикой. Так журналист, описывая ситуацию, вызвавшую общественный интерес, обязан проверять публикуемые им сведения на соответствие действительности, его высказывания не должны содержать утверждений, которые не соответствуют действительности. Осуществляя журналистскую деятельность необходимо проявлять уважение, и к деловой репутации физических и юридических лиц в том числе.

В Постановлении Девятого арбитражного апелляционного суда № 09АП-78848/2019, 09АП-78850/2019¹¹ по данному делу дана оценка результатам лингвистических экспертиз, представленных сторонами. Суд указал, что поскольку в обоснование своих доводов стороны представили лингвистические заключения специалистов,

¹⁰ Конвенция о защите прав человека и основных свобод.

¹¹ Постановление Девятого арбитражного апелляционного суда от 28 января 2020 г. № 09АП-78848/2019, 09АП-78850/2019 по делу № А40-181225/2019 URL: <https://9aas.arbitr.ru/?from=xiaodiaomao.com> (дата обращения: 23.09.2020).

выводы которых противоположны и учитывая отсутствие необходимости для разрешения настоящего спора специальных знаний, исходя из предмета доказывания, руководствуясь ст. 71 АПК РФ¹², суд провел анализ каждой спорной фразы, оценил как оспариваемые сведения, так и статью в целом по своему внутреннему убеждению, основанному на всестороннем, полном, объективном и непосредственном исследовании имеющихся в деле доказательств.

При установлении судом факта наступления неблагоприятных последствий в виде нематериального вреда деловой репутации истца, суд исходил из того, что необходимо установить факт сформированной деловой репутации истца, а также факт утраты доверия к его репутации. Также при выявлении причинно-следственной связи между действиями ответчика и возникновением неблагоприятных последствий на стороне истца необходимо установить наличие реальной возможности влияния действий ответчика на формирование мнения об истце у третьих лиц.

При определении размера компенсации суд оценивал в совокупности заключение специалиста о рыночной стоимости компенсации, экономический отчет, учитывая представленные доказательства в подтверждение деловой репутации истца, нанесенного ей урона, как участнику международной экономической деятельности, размер необходимых затрат на проведение достаточных мероприятий для нейтрализации репутационного вреда, причиненного Компанией спорной публикацией.

Кроме того, суд указал, что охват читательской аудитории Независимой Газеты значителен, что подтверждено материалами дела. Данный факт также был учтен при установлении размера компенсации.

Давая оценку доводам ответчика о наличии в распространенных сведениях метафоры, которая не может быть проверена на соответствие действительности («затаиться», «молчать», «рисует картинку»), судом установлено что, несмотря на наличие метафоры, указания на конкретные действия истца, что является утверждением, могут быть проверены на предмет соответствия действительности

¹² Арбитражный процессуальный кодекс Российской Федерации от 24 июля 2002 г. № 95-ФЗ (ред. от 08 июня 2020 г.) // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/> (дата обращения: 23.09.2020).

Размер взыскиваемого вреда рассчитан исходя из затрат на проведение PR-кампании для нейтрализации репутационного вреда, причиненного истцу статьей. Для компенсации необходимо опубликовать сопоставимое количество материалов в СМИ, так как восстановление деловой репутации происходит с помощью вытеснения (замещения) порочащих сведений о деятельности компании положительными.

Довод жалоб о том, что истец не воспользовался правом на ответ, реплику, не имеет отношения к вопросу об оценке репутационного вреда, так как истец на основании консультаций специалистов посчитал, что для восстановления его нарушенной репутации недостаточно реализации права на ответ, реплику. Для нейтрализации негативных сведений, истцу необходимо осуществить организационные и материальные затраты.

При рассмотрении дела № А40-96736/2019¹³ судом установлено, что истец, обосновывая исковые требования, указал, что на портале «Сердитый Гражданин», расположенном в сети интернет было опубликовано обращение ответчика под названием «Задымление в районах города», которое содержало утверждения, которые порочили деловую репутацию истца.

Как отметил суд – указанный портал, что непосредственно указано на его главной странице, осуществляет помощь гражданам в формулировании и подаче жалоб на некачественные товары, услуги, проблемы в жилищно-коммунальном хозяйстве, состояние дорог и т.д. Указанным порталом пользуется более тысячи государственных органов и иных организаций.

В ходе рассмотрения спорного обращения, размещенного ответчиком на портале, были получены ответы из Управления Роспотребнадзора по Московской области, Гостехнадзора Московской области, Администрации губернатора Московской области, Министерства экологии и природопользования Московской области. Ответы содержали ссылки на Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

¹³ Решение Арбитражного суда г. Москвы от 4 декабря 2019 г. по делу № А40-96736/19-51-794. URL: <https://sudact.ru/arbitral/court/reshenya-as-goroda-moskvy/> (дата обращения: 23.09.2020).

Как указано в ст. 10 Конвенции о защите прав и основных свобод человека¹⁴ – каждый имеет право на свободное выражение своего мнения. В это право входит, кроме того и свобода получать и распространять информацию и идеи, не опасаясь вмешательства публичных властей и безотносительно государственных границ. Осуществляя эти свободы, тем не менее, налагаются обязанности и ответственность, их реализации может быть сопряжена с некоторыми формальностями, условиями, ограничениями или санкциями, установленными законом и которые необходимы в любом демократическом обществе для защиты интересов или прав других лиц, в частности защиты деловой репутации. Свобода выражения мнения составляет одну из существенных основ демократического общества и одно из основных условий его развития.

Согласно п. 9 «Обзора практики рассмотрения судами дел по спорам о защите чести, достоинства и деловой репутации»¹⁵, требования истца о защите чести и достоинства не могут быть удовлетворены, в случае, когда он оспаривает сведения, которые изложены в официальном обращении ответчика в государственный орган или к должностному лицу, при этом само обращение не содержит оскорбительных выражений и вызвано желанием ответчика осуществить свое конституционное право на обращение в государственные органы и органы местного самоуправления. Все граждане имеют право беспрепятственно обращаться в государственные органы, органы местного самоуправления и к должностным лицам с целью защиты своих прав и законных интересов или прав и законных интересов иных лиц. Также граждане могут указывать в обращениях на известные ему факты и события, по их мнению, имеющие отношение к сути поднятого в обращении вопроса и могущие оказать влияние

¹⁴ Конвенция о защите прав человека и основных свобод (Заключена в г. Риме 4 ноября 1950 г.) (с изм. от 13 мая 2004 г.) (вместе с Протоколом № 1. Подписан в г. Париже 20 марта 1952 г.) // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/> (дата обращения: 23.09.2020).

¹⁵ Обзор практики рассмотрения судами дел по спорам о защите чести, достоинства и деловой репутации (утв. Президиумом Верховного Суда РФ 16 марта 2016 г.). // СПС «КонсультантПлюс». URL http://www.consultant.ru/document/cons_doc_LAW_195322/ (дата обращения: 23.09.2020).

на его разрешение. Тот факт, что содержащиеся в обращении сведения могут не подтвердиться, не может стать основанием для привлечения заявителя к гражданско-правовой ответственности, которая предусмотрена ст. 152 ГК РФ¹⁶, в случае если это обращение вызвано попыткой осуществить свои конституционные права, которые имеют явно публичную направленность, цель привлечь внимание к важной общественной проблеме. Другая позиция означала бы привлечение лица к гражданско-правовой ответственности за действия, которые совершены им в рамках предоставленных ему конституционных прав, или же при исполнении им своего гражданского долга.

Вместе с тем, в силу ст. 6 Федерального закона от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»¹⁷ запрещено преследование граждан по поводу обращений в государственные органы, органы местного самоуправления или к должностным лицам с заявлениями, содержащими критику деятельности указанных органов или должностных лиц, или с целью восстановления или защиты своих прав, свобод и законных интересов или прав, свобод и законных интересов иных лиц. Рассматривая такие обращения, не допускается разглашение сведений, которые в нем содержатся, а также сведений, которые касаются частной жизни гражданина, без его согласия. Не будет являться разглашением сведений, содержащихся в обращении, факт направления письменного обращения в государственный орган, орган местного самоуправления или должностному лицу, в компетенцию которых входит решение поставленных в обращении вопросов.

При разрешении данного спора суд пришел к выводу о том, что направление ответчиком спорного обращения на портал «Сердитый Гражданин» было продиктовано необходимостью привлечения внимания компетентных органов на ситуацию, требующую, по мнению заявителя, проверки.

¹⁶ Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ (ред. от 31 июля 2020 г.) // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/> (дата обращения: 23.09.2020).

¹⁷ Федеральный закон от 2 мая 2006 г. № 59-ФЗ (ред. от 27 декабря 2018 г.) «О порядке рассмотрения обращений граждан Российской Федерации» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/> (дата обращения: 23.09.2020).

Доказательств, свидетельствующих о том, что при направлении спорного обращения, ответчиком были совершены умышленные действия, направленные исключительно на причинение вреда истцу, его деловой репутации, в нарушение положений ст. 65 АПК РФ¹⁸ не представлено. Учитывая изложенное, суд пришел к выводу об отсутствии оснований для защиты деловой репутации истца.

Также, по мнению суда, ссылка истца в обоснование своих требований на то, что портал «Сердитый Гражданин» не является государственным органом, не может свидетельствовать о правомерности заявленных требований. В судебном заседании суд апелляционной инстанции исследовал портал «Сердитый Гражданин», и пришел к выводу, что размещенная ответчиком статья передана порталом государственным органам, то есть фактически данный портал выступал как посредник между гражданином и государственным органом, в связи с чем данное обращение следует квалифицировать как обращение в госорган.

¹⁸ Арбитражный процессуальный кодекс Российской Федерации от 24 июля 2002 г. № 95-ФЗ.

Эдуард Геннадьевич МАРТЫНЮК
*обучающийся факультета подготовки следователей
юридического института
Московская академия Следственного комитета
Российской Федерации*

ДЕЯТЕЛЬНОСТЬ ФСБ РОССИИ, СК РОССИИ И МВД РОССИИ ПО ПРЕДУПРЕЖДЕНИЮ, РАСКРЫТИЮ И РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. Правоохранительные органы на протяжении многовековой российской истории играли огромную роль в выявлении, предупреждении, пресечении, раскрытии и расследовании преступлений и по сей день только наращивают свой потенциал в этой области. Несмотря на их глобальное значение, на данный момент преступность тоже набирает обороты – начинает использовать достижения науки и техники, что очевидно, при этом возрастая в мировых масштабах. Информационные технологии – одно из главных орудий современности. С помощью них криминальные группы наносят вред обществу в целом. Задача следственных подразделений ФСБ России, СК России и МВД России на современном этапе развития – пресечь возможные правонарушения и уничтожить мировую угрозу.

Ключевые слова: ФСБ России, СК России, МВД России, информационные технологии, преступления, общество, закон, право.

Eduard Gennadevic MARTYNIUK
*student of the faculty of training investigators
Moscow Academy of the Investigative
Committee of the Russian Federation*

ACTIVITIES OF THE FEDERAL SECURITY SERVICE OF RUSSIA, THE INVESTIGATIVE COMMITTEE OF RUSSIA AND THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA ABOUT PREVENT, SOLVE AND INVESTIGATION CRIMES RELATED TO THE USE OF INFORMATION TECHNOLOGY

Abstract. Law enforcement agencies have played a huge role in identifying, preventing, suppressing, solving and investigating crimes over the centuries of Russian history, and are still developing their potential in this area. Despite their global significance at this point in time, crime is also gaining momentum-it is beginning to use the achievements of science and technology, which is obvious, while increasing on a global scale. Information technologies are one of the main tools of our time. They are used by criminal groups to harm society as a whole. The task of the investigative units of the FSB of Russia, the IC of Russia and the

Ministry of internal Affairs of Russia at the present stage of development is to stop possible offenses and destroy the world threat.

Keywords: FSS of Russia, IC of Russia, MIA of Russia, information technology, crimes, society, law, right.

Задачи следственных подразделений ФСБ России, Следственного комитета России (далее – СК России) и МВД России – пресечь возможные правонарушения и уничтожить мировую угрозу, в той или иной степени связаны с органами, осуществляющими оперативно-розыскную деятельность (далее – ОРД). Среди задач ОРД, обозначенных в Федеральном законе от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – закон об ОРД), выделяются такие как выявление, предупреждение, пресечение, раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших.

Органами, осуществляющими ОРД, являются ФСБ России и органы внутренних дел России. СК России не относится к органам, полномочным осуществлять ОРД, однако в соответствии с Федеральным законом от 28 декабря 2010 г. № 403-ФЗ «О Следственном комитете Российской Федерации» (далее – закон о Следственном комитете) этот орган играет другую ключевую роль – выявление, предупреждение, пресечение, раскрытие и расследование преступлений.

Таким образом, полномочия указанных правоохранительных органов в определенной степени дополняют друг друга для достижения общей цели – искоренения преступности.

Говоря о деятельности правоохранительных органов в области выявления, предупреждения, пресечения, раскрытия и расследования преступлений, необходимо определить значение вышеперечисленных категорий и обозначить компетенцию трех упомянутых органов, а также дать комплексное определение понятию «информационные технологии».

В науке нет единых определений перечисленных понятий, но, опираясь на Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности» (далее – закон о федеральной службе безопасности), закон о Следственном комитете, Федеральный закон от 30 ноября 2011 г. № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации», можно сформулировать следующее:

- выявление преступлений – задача, указанная в законе об ОРД, состоящая в обнаружении общественно опасных деяний, запрещенных уголовным законом под угрозой наказания, а также лиц, их совершающих;
- предупреждение преступлений – особая система мер, принимаемых правоохранительными органами, направленных на противодействие процессам роста преступности, на предотвращение совершения новых преступлений и криминализации общества;
- пресечение преступлений – своевременное вмешательство в действие/ бездействие преступника, прекращение его/их, задержание виновного;
- раскрытие преступлений – установление прокурором, следователем, органом дознания или дознавателем события преступления и изобличение лица или лиц, виновных в совершении преступления¹;
- расследование преступлений – одна из стадий следственной деятельности по расследованию (получению сведений) возбужденного уголовного дела.

Таким образом, названные категории создают цепочку последовательных задач, которые осуществляют ФСБ России, СК России и МВД России.

В соответствии с законом о федеральной службе безопасности в компетенцию (направления деятельности в данной области) органов федеральной службы безопасности входит контрразведывательная деятельность, борьба с терроризмом, борьба с преступностью, разведывательная деятельность, пограничная деятельность, обеспечение информационной безопасности и др.

СК России осуществляет расследование преступлений, обеспечение законности в разных проявлениях; процессуальный контроль деятельности следственных органов СК России и их должностных лиц; выявление обстоятельств, способствующих совершению престу-

¹ Низамов В.Ю. К вопросу о понятии «раскрытие преступления» в криминалистике и уголовном процессе. URL: <https://cyberleninka.ru/article/n/k-voprosu-o-ponyatii-raskrytie-prestupleniya-v-kriminalistike-i-ugolovnom-protssesse> (дата обращения: 08.11.2020).

плений, принятие мер по устранению таких обстоятельств; международное сотрудничество в сфере уголовного судопроизводства и др.

В полномочия Министерства внутренних дел РФ входит ОРД, противодействие коррупции и иным преступлениям, предупреждение, выявление и пресечение правонарушений, профилактика в пределах компетенции правонарушений, ведомственный контроль и др.²

Понятие «информационные технологии» указано в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Преступная среда не упускает возможности использования информационных технологий. Все-таки информация – главное оружие. Еще в XVIII–XIX вв. Натаном Майером Ротшильдом сказано, что тот, кто владеет информацией, владеет миром. Именно поэтому преступность неотъемлема сейчас от достижений науки и техники.

Что касается расследования преступлений, связанных с использованием информационных технологий, указанные правоохранительные органы по сей день вносят свой вклад в их качественное и оперативное разрешение.

Так, среди громких дел, раскрытых ФСБ России, отметим следующие.

1. Д. осужден по ст. 275 («Государственная измена») УК РФ. По информации ЦОС ФСБ, с 2004 г. он искал возможности приобрести за денежное вознаграждение сведения, составляющие государственную тайну, для их последующей передачи спецслужбам ФРГ. Сотрудникам ФСБ России удалось подтвердить связь Д. с германской спецслужбой и конкретные факты сбора им информации по перспективным образцам ракетного вооружения. ФСБ сообщает: «В целях предотвращения ущерба обороноспособности России было принято решение о его задержании при

² Указ Президента Российской Федерации от 21 декабря 2016 г. № 699 (ред. от 25 декабря 2019 г.) «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации».

попытке вывоза им секретных материалов по военной тематике за рубеж»³.

2. За государственную измену в форме шпионажа (передавал данные посредством использования информационных технологий) в пользу спецслужб Великобритании в 2006 г. осужден С.⁴
3. Бывший кадровый разведчик ВМС США П. при содействии заведующего кафедрой МГТУ имени Н.Э. Баумана Б. (позднее помилован Президентом Российской Федерации) собирал в интересах американского военно-промышленного комплекса техническую документацию по созданию не имеющего аналога не только в США, но и в мире, противолодочного ракетного комплекса «Шквал», состоящего на вооружении ВМФ России⁵.

СК России расследованы следующие резонансные уголовные дела:

- подрыв самодельного взрывного устройства в 2017 г. в метрополитене г. Санкт-Петербурга. Это и есть информационные технологии. Уголовное дело возбуждено по ст. 205 («Террористический акт») УК РФ и расследовалось Главным управлением по расследованию особо важных уголовных дел СК России⁶;
- в Республике Коми по ст. 159 и 210 УК РФ (мошенничество, организация и участие в преступной деятельности) привлечены 19 чел., в том числе глава Республики Коми и его заместитель, председатель Государственного Совета Республики, заместитель Председателя Правительства Республики, экс-сенатор от Республики и др. лица (преступные операции совершены посредством использования информационных технологий)⁷;
- множество преступлений, совершенных М., в том числе 3 – по ст. 282 («Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства») УК РФ, по фактам выкладывания в Интернет видеороликов, разжигающих ненависть или вражду⁸.

³ Электронная газета «Коммерсантъ». 2006. URL: <https://www.kommersant.ru/doc/993756> (дата обращения: 09.11.2020).

⁴ Свободная энциклопедия Википедия. URL: https://ru.wikipedia.org/wiki/Скрипаль,_Сергей_Викторович (дата обращения: 09.11.2020).

⁵ Электронная газета «Коммерсантъ». 2006. URL: <https://www.kommersant.ru/doc/993756> (дата обращения: 09.11.2020).

⁶ URL: <http://sledcom.ru/news/item/1331193/> (дата обращения: 09.11.2020).

⁷ URL: <http://sledcom.ru/news/item/968949/> (дата обращения: 09.11.2020).

Органами МВД России раскрыты следующие преступления, совершенные с использованием достижений науки и техники:

1. Директору Департамента контроля расходов на науку, образование, культуру, спорт и СМИ Счетной палаты РФ М. предъявили обвинение в совершении преступления, предусмотренного ч. 6 ст. 290 («Получение взятки в особо крупном размере»). По версии следствия, за получение 3 млн руб. он согласился включить ФГУП «Спорт-инжиниринг», которое занимается строительством и реконструкцией стадионов, в список организаций, подлежащих проверке Счетной палатой РФ в 2014 г.⁹
2. По факту хищения более 350 млн руб. кредитных средств, выделенных государственной корпорацией Внешэкономбанк на строительство элитного жилого комплекса, возбуждено уголовное дело по ч. 4 ст. 159 («Мошенничество в особо крупном размере») УК РФ. В результате следственных действий по подозрению в совершении преступления задержан бывший председатель Высшей аттестационной комиссии при Министерстве образования и науки РФ Ш.¹⁰
3. По итогам проверки банкротства банка «Московский капитал» в 2009 г. в отношении бывшего руководителя московского Управления Росимущества Ш. возбуждено уголовное дело по ст. 30, ч. 3 ст. 159 (покушение на мошенничество в особо крупном размере) УК РФ. Он подозревается в махинациях с объектами недвижимости стоимостью более 10 млрд руб.¹¹

Многие преступления, совершенные в недалеком прошлом, совершаемые сейчас и, к сожалению, которые будут совершены в будущем, в той или иной степени связаны с информационными технологиями. Правоохранительные органы – ФСБ России, СК России и МВД России, обязаны своевременно, качественно и оперативно осуществлять их выявление, предупреждение, пресечение, раскрытие и расследование.

⁸ Резонансные дела Следственного комитета Российской Федерации. URL: <https://sledcom.ru/cases/item/1114713> (дата обращения: 09.11.2020).

⁹ URL: <http://moscow.sledcom.ru/news/item/745099/> (дата обращения: 09.11.2020).

¹⁰ URL: https://www.forbes.ru/news/233913-v-zdanii-vysshei-attestatsionnoi-komissii-idut-obyski?_ga=2.133800332.388148900.1613572044-541999486.1613572044 (дата обращения: 09.11.2020).

¹¹ Пресс-конференция на тему «Резонансные уголовные дела, расследуемые ГСУ ГУ МВД России по г. Москве». URL: https://77.xn--b1aew.xn--p1ai/SMI/Press_konferencija_na_temu_Rezonansnie_u (дата обращения: 09.11.2020).

Анна Сергеевна МЕДВЕДЕВА
*старший государственный судебный эксперт
ФБУ «Северо-Западный региональный центр
судебной экспертизы Минюста России»*

ОСОБЕННОСТИ ДОСУДЕБНОГО ПРОИЗВОДСТВА ПО УГОЛОВНЫМ ДЕЛАМ, СВЯЗАННЫМ С СЕКСУАЛЬНЫМИ ДОМОГАТЕЛЬСТВАМИ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ ИНТЕРНЕТ

Аннотация. В статье рассматривается ряд особенностей такого вида преступлений, как сексуальное домогательство несовершеннолетних в сети Интернет. Раскрыта специфика его осуществления, приемы, которые используют злоумышленники. Отдельное внимание уделяется процессу выявления и расследования данных преступлений, в частности, сбору доказательств, поиску человека, назначению судебных экспертиз, производству следственных действий. Сделан вывод о необходимости психологического сопровождения следственных действий с несовершеннолетними потерпевшими, а также о необходимости профилактики данного вида преступности путем соответствующей адаптации информационно-телекоммуникационных технологий.

Ключевые слова: Интернет, несовершеннолетние, киберпреступность, сексуальное домогательство, экспертиза.

Anna Sergeyevna MEDVEDEVA
*senior forensic expert FSI North-West RCFE
of the Ministry of Justice of Russian Federation*

PECULIARITIES OF PRE-TRIAL PROCEEDINGS IN CRIMINAL CASES RELATED TO SEXUAL HARASSMENT OF MINORS IN THE INTERNET

Abstract. The article examines a number of features of this type of crime as sexual harassment of minors on the Internet. The specifics of their implementation, the techniques used by criminals are revealed. Special attention is paid to the process of identifying and investigating these crimes, in particular, the collection of evidence, the search for the offender, the appointment of forensic examinations, the production of investigative actions. The conclusion is made about the need for psychological support of investigative actions with underage victims, as well as the need to prevent this type of crime by appropriate adaptation of information and telecommunication technologies.

Keywords: cybercrime, expertise, Internet, minors, sexual harassment.

С учетом большого количества случаев сексуального домогательства несовершеннолетних в сети Интернет и их дальнейшей

эксплуатации особенности досудебного производства по таким уголовным делам требуют внимательного рассмотрения.

В настоящее время выявляется ряд способов использования Интернета лицами с девиантным сексуальным отношением к детям: обмен детской порнографией, поиск потенциальных жертв сексуального насилия, вовлечение детей в непристойное сексуальное общение, общение с другими лицами с девиантным сексуальным отношением к детям.

Интернет предоставляет пользователям возможность устанавливать контакты прямо из дома, участвовать в разнообразных видах сексуальных действий и совершать связанные с этим поступки. Благодаря доступности, приемлемым ценам и анонимности огромное количество материалов сексуального характера становится доступным любому человеку, выступающему под собственным именем или онлайн-псевдонимом. Интернет помогает более простому и быстрому распространению подобной информации и взаимодействию педофилических сообществ, объединяя как разные территории внутри страны, так и разные страны. Он также может быть использован для реализации потребности в порнографии, текстах эротического содержания и поддержания сообществ с общими взглядами. Эти сообщества также могут давать советы о том, как получить доступ к потенциальным жертвам и избежать обнаружения.

Одним из наиболее опасных для несовершеннолетних преступных действий является вступление правонарушителей в онлайн-коммуникацию с детьми, последствия которой могут быть чрезвычайно деструктивными, например, приводить к дальнейшей встрече в реальном мире. В настоящее время число подобных случаев велико и их количество продолжает расти¹.

Зарубежные исследования показывают, что, помимо анонимности, для злоумышленников важное значение имеют следующие факторы, побудившие их к сексуальному домогательству: ощущение собственной значимости (авторитетности) и желанности для ребенка, пусть и в краткосрочной перспективе; ощущение подлинной связи с ним, аналогичной той, которая возникает при реальных

¹ Дозорцева Е.Г., Медведева А.С. Сексуальный онлайн груминг как объект психологического исследования // Психология и право. 2019(9). № 2. С. 250–263.

отношениях; возможность реализовать потребность в сексуальном удовлетворении «безопасным» способом². Для преступников, чьи нормальные способы сексуальной разрядки оказываются заблокированы, интернет может служить средством сексуального удовлетворения благодаря его атмосфере анонимности и свободному доступу к широкому спектру материалов откровенного содержания. Куэйл и Тэйлор считают, что анонимная и полушутливая природа интернета может оказывать мощное активизирующее воздействие на поведение людей, в сочетании с возможностью свободно выражать свои сексуальные интересы и фантазии³.

При выявлении и расследовании преступлений, связанных с сексуальным домогательством несовершеннолетних в сети Интернет, следует учитывать ряд особенностей, а именно: скрытность и анонимность коммуникантов, сложности в формировании доказательств, трудности в поиске злоумышленника и его жертвы ввиду отсутствия территориальной привязки.

Во многих случаях факту обнаружения преступления способствует простая случайность, когда родители несовершеннолетнего замечают его повышенную активность в Интернете, признаки скрытности и другие изменения в поведении. Специфика онлайн-атак сексуальных преступников заключается в том, что в процессе коммуникации происходит завоевание доверия ребенка, преодоление его возможного сопротивления и последующее злоупотребление полученным доверием. Взрослые правонарушители при коммуникации с несовершеннолетним часто используют стратегии, направленные на создание доброжелательной атмосферы (лесть, обещание безопасности, демонстрация наличия общих интересов, положительных чувств, внимания к ребенку, одобрение его, обещание подарков⁴), поскольку данные условия минимизируют вероятность возникновения у ребенка жалоб и возможность обнаружения и разоблачения⁵. Хотя

² *Kloess J.A., Larkin M., Beech A.R., Hamilton-Giachritsis C.E.* Case Studies of Men's Perceptions of Their Online Sexual Interactions With Young People: An Interpretative Phenomenological Analysis // *Sexual Abuse*. 2018. Т. 00. № 0. С. 1–19.

³ *Quayle E., Taylor M.* Child seduction and selfrepresentation on the Internet // *Cyber-Psychology and Behavior*. 2001. Т. 4. С. 597–608. doi:10.1089/109493101753235197.

⁴ *Shannon D.* Online sexual grooming in Sweden – online and offline sex offenses against children as described in Swedish police data // *Journal of Scandinavian Studies in Criminology and Crime Prevention*. 2008. Т. 9. С. 160–180. doi:10.1080/14043850802450120.

преступники могут взаимодействовать одновременно с несколькими потенциальными жертвами, с помощью специальных стратегий они создают ложное впечатление особой связи и уникальных отношений с конкретным ребенком, а также их секретность⁶. Также злоумышленники могут использовать принуждение, выражающееся в угрозах, жестокости, подкупе, шантаже, запугивании, чтобы добиться послушности ребенка и предотвратить разоблачение⁷. Дети часто могут испытывать чувство вины и ответственности, особенно когда их вынуждают совершать сексуальные акты. Этот эффект может быть усилен преступниками с помощью психологических стратегий обвинения несовершеннолетнего и создания ощущения соучастия⁸.

Вместе с тем коммуникации преступников нередко скрыты паролями или намеренно удаляются пользователями. В случае если переписки лиц остаются сохраненными в памяти устройств, необходимо применение специфических средств формирования доказательств (обработки компьютерной информации). Сложность заключается в том, что преступнику достаточно одной минуты для того, чтобы

⁵ *McAlinden A.M.* «Setting ‘em up»: Personal, familial and institutional grooming in the sexual abuse of children // *Social and Legal Studies*. 2006. Т. 15. С. 339–362. doi:10.1177/09646639060666613.

⁶ *Craven S., Brown S., Gilchrist E.* Sexual grooming of children: Review of literature and theoretical considerations // *Journal of Sexual Aggression*. 2006. Т. 12. С. 287–299; *Shannon D.* Online sexual grooming in Sweden – online and offline sex offenses against children as described in Swedish police data // *Journal of Scandinavian Studies in Criminology and Crime Prevention*. 2008. Т. 9. С. 160–180. doi:10.1080/14043850802450120.

⁷ *Cossins A.* The hearsay rule and delayed complaints of child sexual abuse: The law and the evidence // *Psychiatry, Psychology and Law*. 2002. Т. 9. С. 163–176. doi:10.1375/13218710260612055; *Craven S., Brown S., Gilchrist E.* Sexual grooming of children: Review of literature and theoretical considerations // *Journal of Sexual Aggression*. 2006. Т. 12. С. 287–299; *Raja A.* Online Child Sex Exploitation: Sexting and Grooming // *Computer Forensics and Investigation*. 2014. С. 1–67. URL: <http://dx.doi.org/10.1111/j.1468-2958.2007.00299> (дата обращения: 14.10.2020); *Bryce J.* Online sexual exploitation of children and young people // *Handbook of Internet crime*. 2010. С. 320–342. URL: https://research.birmingham.ac.uk/portal/files/18272411/Literature_Review_Manuscript_Revision_2_complete_pdf (дата обращения: 14.10.2020).

⁸ *Cossins A.* The hearsay rule and delayed complaints of child sexual abuse: The law and the evidence // *Psychiatry, Psychology and Law*. 2002. Т. 9. С. 163–176. doi:10.1375/13218710260612055; *Craven S., Brown S., Gilchrist E.* Sexual grooming of children: Review of literature and theoretical considerations // *Journal of Sexual Aggression*. 2006. Т. 12. С. 287–299.

удалить ее как со своего личного устройства, так и с какого-либо другого (например, если переписка с ребенком происходила в социальной сети).

Другая сложность заключается в том, чтобы выявить злоумышленника и соотнести его с полученными доказательствами, что особенно затруднительно в случае использования человеком псевдонимов. Кроме того, распространена практика, когда злоумышленники при коммуникации с несовершеннолетними сами выдают себя за детей. Это способствует тому, что ребенок может длительное время не знать (или так и не узнать) о том, что он вступил в нежелательное общение с взрослым человеком.

Вместе с тем сфера информационных технологий подразумевает взаимодействие пользователей независимо от их физического местонахождения, что влечет за собой увеличение сроков поиска преступника. Как указывает Д.В. Милютин, при получении правоохранительными органами одного из регионов России информации о нахождении на территории обслуживания потерпевшего лица может возникнуть необходимость проведения на территории нескольких других регионов комплекса оперативно-розыскных мероприятий и следственных действий для установления злоумышленника. Это вызывает затруднения в связи с необходимостью осуществления выезда в данные регионы и наличием проблем с предоставлением информации гражданскими организациями, в частности, проблемы сроков предоставления запрошенной информации и ее полноты. Также данная особенность вызывает некоторые проблемы при определении места совершения преступления и соответственно места осуществления предварительного расследования⁹.

В определенный момент времени у правоприменителей также возникает необходимость в установлении обстоятельств, подлежащих доказыванию, и разрешении вопросов, требующих специальных знаний. Здесь наиболее востребованным является назначение ком-

⁹ Милютин Д.В. Специфика выявления и расследования преступлений в сфере высоких технологий, совершенных с использованием сети интернет и социальных сетей // Общественная безопасность, законность и правопорядок в III тысячелетии. Воронежский институт Министерства внутренних дел Российской Федерации (Воронеж). 2017. Т. 3–3. С. 295–303.

пьютерно-технической и комплексной судебной психолого-лингвистической экспертиз.

Компьютерно-техническая экспертиза позволяет установить факт, период времени и частоту использования лицами конкретного оборудования. В рамках комплексной судебной психолого-лингвистической экспертизы текстов коммуникации между взрослым и ребенком становится возможным определить смысловое содержание переписки, ее инициаторов, наличие в ней информации о действиях сексуального характера, коммуникативную цель участников переписки, признаки побуждения несовершеннолетнего к действиям сексуального характера и приемы речевого и психологического воздействия на него со стороны преступника.

Отдельного рассмотрения требует вопрос о специфике производства следственных действий с участием несовершеннолетнего потерпевшего от сексуального домогательства в сети Интернет. Представляется необходимым обязательное привлечение психолога к допросу ребенка с целью предотвращения его повторной травматизации, снижения уровня страха и тревоги, помощи в присвоении номинаций при обсуждении сексуально ориентированных тем.

Таким образом, активное развитие информационно-телекоммуникационных технологий и их использование оказывают влияние на все сферы жизни общества. Оно побуждает несовершеннолетних взаимодействовать с другими людьми в виртуальном пространстве, что облегчает доступ преступникам к своим потенциальным жертвам. Представляется важным эффективно ограничивать адаптацию новых технологий с негативной целью при одновременном расширении положительного влияния данных технологий с точки зрения профилактики сексуального домогательства.

Мария Сергеевна НОВИКОВА

студент

*Крымский юридический институт (филиал)
Университета прокуратуры Российской Федерации*

ИСПОЛЬЗОВАНИЕ МАССОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. В статье анализируются распространенные способы использования информационных технологий в экстремистской деятельности. На основании их анализа делается вывод об основных тенденциях распространения экстремизма в информационно-телекоммуникационных сетях. Исследуются основные проблемы противодействия экстремизму в сети Интернет.

Ключевые слова: экстремизм, информационные технологии, Интернет, противодействие экстремизму.

Maria Sergeevna NOVIKOVA

student

*Crimean Institute of Law (branch)
of the University of Prosecutor's Office
of the Russian Federation*

USE OF MASS INFORMATION TECHNOLOGIES IN EXTREMIST ACTIVITIES

Abstract. The article analyzes common ways of using information technologies in extremist activities. Based on this analysis, it is concluded about the main trends in the spread of extremism in the Internet networks. The article examines the main problems of countering extremism on the Internet.

Keywords: extremism, information technology, Internet, counteracting extremism.

Деятельность экстремистских организаций на сегодняшний день официально признана одной из угроз государственной и общественной безопасности. Как отмечено в Стратегии национальной безопасности РФ, появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий¹. Это применимо и к такому виду противоправной деятельности как экстремизм. Реалии

¹ Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. 4 января. № 1 (ч. II). Ст. 212.

современного информационного общества создают условия для беспрепятственного использования массовых информационных технологий в экстремистской деятельности.

Необходимо отметить, что значительная часть преступлений экстремистской направленности совершается в Интернете: по данным МВД России они составляют порядка 80 % от общего числа подобных преступлений². При этом в целом число экстремистских преступлений неуклонно растет с каждым годом. Так в 2020 г. в России зафиксировано преступлений на 40,9 % больше, чем в 2019 г.

Экстремизм – категория многоплановая и включает в себя множество видов деятельности, прямо или косвенно направленной на насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности РФ или возбуждение социальной, расовой, национальной или религиозной розни³. Стратегия противодействия экстремизму определяет в качестве наиболее опасных проявлений экстремизма возбуждение ненависти либо вражды, унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а также принадлежности к какой-либо социальной группе, в том числе путем распространения призывов к насильственным действиям, прежде всего с использованием информационно-телекоммуникационных сетей, включая сеть Интернет; вовлечение отдельных лиц в деятельность экстремистских организаций; организацию и проведение несогласованных публичных мероприятий (включая протестные акции), массовых беспорядков. Более того, на сегодняшний день информационно-телекоммуникационные сети, включая сеть Интернет, являются основным средством связи для экстремистских организаций, которое используется ими для вербовки новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии⁴.

² *Ильиных О.* Не допустить ненависти и вражды // Полиция России. 2019. № 9. URL: <http://ormvd.ru/pubs/101/to-prevent-hatred-and-enmity/> (дата обращения: 01.11.2020).

³ Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // СЗ РФ. 2002. 29 июля. № 30. Ст. 3031.

⁴ Указ Президента РФ от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // СЗ РФ. 2020. 1 июня. № 22. Ст. 3475.

Использование массовых коммуникационных технологий продиктовано тем, что с помощью них можно воздействовать на общественное сознание. В первую очередь, информационные технологии, преимущественно Интернет, используются как средство массовой информации распространения пропагандистских материалов. Веб-сайты с экстремистским контентом в последнее время широко распространены. Использование Интернета дает правонарушителям ряд преимуществ, включая небольшую стоимость распространения, отсутствие специального оборудования и глобальную аудиторию⁵. Кроме того, такие сайты довольно быстро создаются, а вот процедура их закрытия куда более длительна и затратна.

Следует отметить, что создатели таких веб-сайтов с особой тщательностью подходят к их созданию и ведению. Веб-сайты с экстремистским контентом, как правило, выделяются из массы других оригинальным дизайном, ярким оформлением, доступной системой навигации и поиска интересующей информации. В качестве основных форм предоставления информации выступают новостные ленты, различные аналитические материалы, содержание которых преподносится пользователю с выгодной для экстремистов позиции. При этом сами идеологические установки скрыты в контексте сообщений. Модераторы сайта применяют те же способы подачи информации, что и официальные средства массовой информации: заголовки имеют сенсационный характер, наиболее важная информация содержится в первом абзаце и не повторяет информацию заголовка, а только поясняет ее, новостная лента располагается на главной странице и подкрепляется соответствующими фотографиями. На многих сайтах есть форумы, где участники могут общаться в режиме реального времени⁶.

Другой способ применения информационных технологий в экстремистской деятельности это использование социальных сетей для создания тематических групп и сообществ, которые ис-

⁵ Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. М., 2020. С. 70.

⁶ Жаворонкова Т.В. использование сети интернет террористическими и экстремистскими организациями // Вестник Оренбургского государственного университета 2015 № 3. С.30.

пользуется злоумышленниками для вовлечения людей в дискуссию, навязывания экстремистской идеологии⁷. Наиболее ярким примером такой деятельности является распространение тематических сайтов в сети Интернет, посвященных деструктивной идеологии связанной с событиями 20 апреля 1999 г. в школе Колумбайн в США. Подростков приглашают в закрытые группы в социальных сетях под любым предлогом (приглашение в «братство», «сообщество», возможное вознаграждение, бонусы, лайки и т.п.), а далее подросткам, находящимся в таком сообществе, постепенно навязываются радикальные взгляды⁸. Поскольку подростки значительную часть своего времени проводят в социальных сетях, и в целом в Интернет-пространстве, то в силу психологических особенностей дольше подвержены внушению, и как следствие более уязвимы для воздействия со стороны экстремистов. Однако удручающим в данной ситуации является не только само существование таких сообществ, а еще и то, что их массовое выявление и закрытие произошло уже после того как студент Керченского политехнического колледжа совершил вооруженное нападение на сверстников и преподавателей учебного заведения. До трагедии, подобные деструктивные Интернет-сообщества не привлекали столь пристальное внимание правоохранительных органов и органов прокуратуры.

Кроме вышеуказанного, возможности Интернета используется экстремистами для отправки электронных писем и новостных рассылок, а также для распространения видеоклипов и телевизионных программ с использованием популярных Интернет-площадок для хранения соответствующих файлов, например YouTube.

Отдельное применение информационные технологии нашли в продаже товаров, сбыт которых запрещен. Благодаря Интернету нацистские предметы, такие как флаги с нацистской символикой, униформа и книги, свободно доступны на аукционных площадках и в специализированных веб-магазинах⁹.

⁷ Ганаева Е.Э, Муцалов Ш.Ш. Использование массовых информационных технологий экстремистскими организациями // Армия и общество. 2014. С. 4.

⁸ Ильиных О. Указ. соч.

⁹ Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. М., 2020. С. 70.

Указанные способы использования информационных технологий в экстремистской деятельности с каждым годом все более усиленно воздействуют на сознание граждан. И данной тенденции во многом способствует активное развитие Интернет-технологий и, как следствие, появление новых тактических приемов по использованию этих технологий экстремистскими организациями.

Среди технологических особенностей последних лет следует отметить такие как:

- существенное увеличение скорости обработки цифровой информации и объемов ее хранения;
- доступность Интернета в любой точке мира при использовании мобильных smart-устройств;
- преобладание аудиовизуальной информации по отношению к другим видам информации, размещаемой в Интернете¹⁰.

Эти и многие другие тенденции развития информационных технологий приводят к тому, что их использование становится популярным для осуществления экстремистской деятельности, которая, в свою очередь достигает цели, находя свое отражение в сознании пользователей.

Отдельно необходимо отметить несовершенство системы противодействия экстремизму, распространяемого в информационно-телекоммуникационной сети Интернет, что в свою очередь, только способствует ускоренному развитию распространения экстремистских материалов в сети.

В данном вопросе необходимо учесть, что экстремистская идеология представляет собой сложную категорию, которой требует системного подхода к борьбе с ней. Поскольку такая идеология находит свое отражение в массовом сознании то реализуется она в различных социальных группах. Массовые коммуникации способствуют формированию таких групп. Многоаспектность экстремистской деятельности приводит к тому, что борьба с ней исключительно методами правоохранительных органов не принесет существенных результатов. Потому требуется реализация комплексного подхода и осуществление организационных, правовых, профилактических,

¹⁰ Румянцев А.А. К вопросу о современных тенденциях использования информационного пространства в целях распространения идеологии экстремизма и терроризма // Международная конференция АТЦ СНГ «Информационное противодействие терроризму и экстремизму». М., 2015. С. 117.

воспитательных мероприятий, совершенствования взаимодействия государственных органов и общественных организаций¹¹. При этом, субъекты противодействия экстремизма, для эффективного осуществления своих полномочий нуждаются в обеспечении информационными ресурсами, включающими современные аппаратно-программные комплексы.

Борьба с экстремизмом также требует особо усиленной работы Роскомнадзора как органа, осуществляющего государственный контроль и надзор в сфере информационных технологий и обладающего полномочиями ограничения доступа к сайтам в сети Интернет содержащим информацию, распространение которой в РФ запрещено. План деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций на 2020 г. (утв. Минкомсвязью России 14 февраля 2020 г. № МШ-П12-067-3382) в качестве деятельности по выявлению нарушений, связанных с использованием средств массовой информации для осуществления экстремистской деятельности определяет анализ материалов, публикаций и сообщений, размещенных в средствах массовой информации на предмет соответствия требованиям ст. 4 Закона РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» с формой отчетности в виде докладных записок, справок, предупреждений. Однако учитывая значительный объем Интернет-ресурсов, содержащих экстремистские материалы, то возникает необходимость применения более конструктивных методов выявления экстремистского контента со стороны Роскомнадзора.

Таким образом, можно сделать вывод, что совершенствование информационных технологий создает благоприятные условия для массового распространения экстремистской идеологии и совершения преступлений экстремистской направленности. А указанные тенденции в свою очередь делают необходимыми разработку действенных методов пресечения противоправной деятельности на данном направлении, поскольку имеющаяся на данный момент система противодействия экстремизму мало приспособлена к реалиям развивающегося информационного общества.

¹¹ *Заливанский Б.В.* Технологии информационного противодействия экстремизму // Современные научные исследования и инновации. 2014. № 3. URL: <http://web.snauka.ru/issues/2014/03/32751> (дата обращения: 23.10.2020).

Валерий Владимирович ПЕТРЕНКО

аспирант

Университет прокуратуры Российской Федерации

**ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ,
ПРЕСЕЧЕНИЯ, РАСКРЫТИЯ
И ДОКАЗЫВАНИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ
С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-
ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ¹**

Аннотация. В публикации исследованы вопросы законодательной регламентации ответственности за незаконное получение сведений, составляющих банковскую тайну. Проведен анализ состояния преступности в сфере хищений с использованием информационно-телекоммуникационных технологий на примере уголовно-правовой статистики Краснодарского края. Рассмотрены типовые способы совершения таких преступлений и проблемные вопросы ведомственной регламентации противодействия преступности в указанной сфере, влекущие крайне низкую раскрываемость данного вида преступлений.

Ключевые слова: мобильные хищения, банковская тайна, противодействие преступности.

Valery Vladimirovich PETRENKO

postgraduate student

*University of the Prosecutor's Office
of the Russian Federation*

**PROBLEMS OF LEGISLATIVE REGULATION,
SUPPRESSION, DISCLOSURE AND PROVING
OF THEFT COMMITTED USING INFORMATION
AND TELECOMMUNICATIONS TECHNOLOGIES**

Abstract. The publication examines the issues of legal regulation of liability for illegal receipt of information constituting a bank secret. The analysis of the state of crime in the field of theft using information and telecommunication technologies is carried out on the example of criminal law statistics of the Krasnodar territory. Typical ways of committing such crimes and problematic issues of departmental

¹ По материалам обобщения прокуратуры Краснодарского края к координационному совещанию руководителей правоохранительных органов Краснодарского края «Об анализе эффективности работы правоохранительных органов в сфере противодействия преступлениям, совершенным дистанционно, в том числе с использованием IT-технологий». Не публиковались.

regulation of combating crimes in this area, which entail extremely low detection of this type of crime, are considered.

Keywords: mobile theft, bank secrecy, crime prevention.

Современный уровень развития электронных средств платежа, увеличение доли безналичного оборота привели к широкому распространению преступлений, направленных на хищение денежных средств с банковских счетов граждан, а также в отношении электронных средств платежа.

В последние годы отмечается рост случаев мошенничества, совершаемых с использованием информационных технологий (*таблица 1*)².

При этом значительный рост преступлений исследуемых категорий отмечен за истекший период 2020 г., что связано, в первую очередь, с ростом хищений с использованием информационно-коммуникационных технологий в период пандемии. Складывающаяся криминогенная ситуация осознается как гражданами, так и владельцами информационных бизнесов, принимающими попытки противодействия преступлениям, даже без соответствующей помощи правоохранительных органов³. При этом из числа совершенных мошенничеств с использованием средств мобильной связи к категории тяжких преступлений относится в 2019 г. – 219 преступлений, что составляет 6,24 % от общего числа таких преступлений, за 9 месяцев 2020 г. – 422 (8,83 %), за 9 месяцев 2019 г. – 148 (6,04 %).

Рассмотрим одну из наиболее распространенных типовых ситуаций совершения преступления. Потерпевшему, разместившему объявление имущественного характера на сайте объявлений, звонят под видом покупателя и сообщают о согласии совершить покупку, при этом предлагая перевести деньги в качестве задатка. Под видом получения данных, необходимых для совершения перевода, у по-

² Показатели приведены по данным Информационного центра ГУ МВД России по Краснодарскому краю. Документ опубликован не был. Доступ из автоматизированной информационной системы «Статистика» ИЦ ГУ МВД России по Краснодарскому краю.

³ Как Авито выявляет мошенников и борется с фродом. URL: <https://habr.com/ru/company/avito/blog/505916> (дата обращения: 27.10.2020).

Таблица 1

**Случаи мошенничества,
совершаемые с использованием информационных технологий**

	<i>Период</i>	2014 г.	2015 г.	2016 г.	2017 г.	2018 г.	2019 г.	9 мес. 2019 г.	9 мес. 2020 г.
	Всего зарегистрировано мошенничеств	8060	8252	9668	9818	11353	8620	6308	9133
	Мошенничества с использованием средств мобильной связи	2371	3020	3700	3362	3809	3507	2451	4777
2.1	Из п. 2 осталось нераскрытыми	2224/ 93,8 %	2272/ 75,23 %	3493/ 94,41 %	3046/ 90,6 %	3596/ 94,41 %	3372/ 96,15 %	2322/ 94,74 %	4644/ 97,22 %
	Хищения с использованием сети Интернет	484	1033	1867	2212	2253	1888	2202	3348

терпевшего выясняют конфиденциальную информацию держателя платежной карты, либо временный пароль на доступ в личный кабинет, после чего похищают денежные средства с банковского счета.

Отметим несколько элементов преступной деятельности, при анализе которых можно зафиксировать следы преступления: предварительный сбор виновным информации о вероятных жертвах преступления с электронных ресурсов, голосовой контакт с ним, попытка доступа к банковскому счету с использованием CVV/CVC кода либо временного пароля на доступ в личный кабинет.

Звонки с целью совершения указанных преступлений часто производятся на значительное количество номеров. При этом большое количество граждан, не поддавшись обману, отказывают в предоставлении конфиденциальной информации. Эти граждане при надлежащей информационной работе правоохранительных органов могут оказать помощь в пресечении обычно серийной преступной деятельности, жертвами которой следом становятся иные граждане, часто входящие в уязвимые группы населения. Однако, рассмотрев сложившееся нормативно-правовое регулирование в сфере раскрытия и расследования указанных преступлений, можно отметить, что лица, пресекшие совершение в отношении них преступления, фактически лишены возможности оказания помощи правоохранительным органам. При звонке преступников их действия можно зафиксировать, записав телефонный разговор на диктофон мобильного телефона, а также сообщив недействительную собираемую конфиденциальную информацию. Так сообщение, например, недействительного CVV/CVC кода повлечет попытку списания денежных средств, что можно квалифицировать как покушение на кражу с банковского счета, то есть тяжкое преступление, предусмотренное п. «г» ч. 3 ст. 158 УК РФ.

При незначительно отличающемся способе хищения путем получения временного пароля на доступ к личному кабинету ответственность при неудавшейся попытке доступа за совершение общественно опасного деяния российским уголовным законодательством не предусмотрена, так как действия, непосредственно направленные на совершение кражи, не совершены. К уголовной ответственности, установленной ст. 183 УК РФ, за незаконное получение сведений, составляющих банковскую тайну, виновное лицо не может быть

привлечено, так как в диспозиции статьи закреплена обязательность получения данных сведений путем похищения документов, подкупа или угроз, а равно иным незаконным способом. Согласно ч. 2 ст. 857 ГК РФ сведения, составляющие банковскую тайну, самим клиентом банка могут быть предоставлены. Отдельными авторами поддержано включение обмана как способа собирания сведений в диспозицию ст. 183 УК РФ, составляющих налоговую, коммерческую, либо банковскую тайну⁴, либо рассматривается возможность отнесения конкретных видов обмана к иным незаконным способам⁵. Представляется, что с учетом увеличивающейся распространенности и социальной значимости анализируемых хищений, в которых получение сведений, составляющих банковскую тайну, является одним из элементов преступной деятельности, внесение изменения и указание обмана как одного из способов совершения преступления, предусмотренного ст. 183 УК РФ, является более предпочтительным.

Телефонный разговор может быть записан потерпевшим и передан правоохранительным органам. При этом для раскрытия преступления необходима постановка записи на учет в фонотеку.

Согласно разделу X Инструкции по организации формирования, ведения и использования экспертно-криминалистических учетов органов внутренних дел РФ, утвержденной Приказом МВД России от 10 февраля 2006 г. № 70⁶, посвященному учету фонограмм речи (голоса) неустановленных лиц, органами внутренних дел для установления неизвестных лиц, подозреваемых в совершении преступлений, и фактов совершения нескольких преступлений одним лицом по особенностям речи ведется фонотека. Данный учет ведется

⁴ *Карташов С.В.* Современные проблемы квалификации незаконных получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну, связанные с толкованием отдельных признаков составов преступлений // Журн. Вестник Московского университета МВД России. 2017. № 5. С. 160.

⁵ *Клебанов Л.Р.* Незаконное получение сведений, составляющих коммерческую, налоговую или банковскую тайну: особенности квалификации // Вестник Омского университета. Серия «Право». 2014. № 2. С. 182.

⁶ Приказ МВД Российской Федерации от 10 февраля 2006 г. № 70 «Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации» // СПС «Гарант». URL: <http://www.garant.ru/> (дата обращения: 23.09.2020).

на региональном уровне, только по записям русской речи и только по ст. 207 («Угроза совершения акта терроризма») УК РФ, а также по тяжким и особо тяжким преступлениям. Так как более 90 % совершаемых преступлений анализируемой категории относятся к небольшой и средней тяжести, фонограммы лиц, совершивших данное преступление, на основании указанного приказа в экспертно-криминалистический учет органов внутренних дел введены быть не могут. Принимая во внимание, что подавляющее большинство преступлений анализируемой категории носят межрегиональный либо трансграничный характер, учет на региональном уровне фонограмм безрезультативен.

В указанных и многих других положениях приведенный раздел Инструкции по организации формирования, ведения и использования экспертно-криминалистических учетов органов внутренних дел РФ устарел и не отвечает складывающейся криминогенной ситуации, уровню технического прогресса, а также потребностям противодействия преступлениям анализируемой категории.

Преступления указанной категории часто совершаются группой лиц, с использованием большого количества сим-карт, телефонных аппаратов, различных платежных систем «Киви-кошелек», «Юнистрим» и т.д., услуг подмены абонентского номера, многочисленных счетов, открытых на третьих лиц в банках. При этом лица, на которых открыты счета, зачастую не осведомлены о совершении преступления.

При расследовании уголовных дел и проведении оперативно-розыскных мероприятий в банки, организации, владеющие сайтами размещения объявлений, социальных сетей, направляются запросы, которые исполняются адресатами запросов в срок более месяца. При этом общий срок получения ответа на запрос составляет 2–4 месяца. Получение ответа часто вызывает необходимость направления нового запроса. Для организации оперативного расследования преступлений необходимо создание системы электронного документооборота между оперативными подразделениями и банками, организациями-владельцами сайтов объявлений, социальных сетей со значительной посещаемостью, а также организациями, предоставляющими услуги подмены абонентского номера. Необходимо законодательное установление срока на исполнение указанных запросов

правоохранительных органов и ответственности за его нарушение.

Использование преступниками в большом количестве транзитных счетов вызывает необходимость получения судебного разрешения на получение информации о движении денежных средств по каждому счету после получения ответа. Те финансовые операции, которые занимают у лиц, совершивших преступление, десятки минут, в ходе раскрытия преступления для фиксации преступной деятельности требуют многомесячной работы органов расследования, оперативных подразделений⁷. Отсутствие оперативно действующего процессуального механизма влечет неоправданное использование сил и средств правоохранительных органов.

С учетом потребностей правоприменительной деятельности необходима выработка процессуального механизма по даче единого судебного разрешения органам расследования, оперативным подразделениям на получение сведений о движении похищенных денежных средств по всей цепочке межбанковских операций. При законодательном регламентировании необходимо учесть возможность обезличивания денежных средств в случае зачисления на расчетный счет, используемый и для других операций.

Также необходимо рассмотреть возможность возложения на банки обязанностей по уведомлению под роспись лиц, открывающих счет, о перечне необходимых и достаточных реквизитов для зачисления денежных средств на счет, осуществления платежа, а также по фиксации ошибочных попыток введения пароля на доступ к личному кабинету владельца счета, CVV/CVC кода при списании денежных средств с указанием данных обращения за доступом и перечня использованных кодов. Получение правонарушителем недействительного кода и использование его для совершения операции явится доказательством покушения на совершение преступления. Необходимо законодательно обязать банки предоставлять клиентам возможность запрещения совершения операций по счету из-за пределов РФ.

⁷ Гончар В.В. Отдельные особенности этапа возбуждения уголовного дела по дистанционным хищениям денежных средств // Актуальные вопросы производства предварительного следствия: теория и практика: сборник научных трудов Всероссийской научно-практической конференции. 11 апреля 2019 г. М., 2019. С. 106.

Таким образом, для пресечения роста анализируемых преступлений необходима комплексная работа, направленная на совершенствование уголовного, уголовно-процессуального, иного федерального законодательства, ведомственных нормативных актов правоохранительных органов, на организацию системы взаимодействия органов внутренних дел с банками, участниками рынка информационно-телекоммуникационных услуг.

Антонина Васильевна ПЕТРЯКОВА
старший преподаватель
Московский международный университет

МЕЖДУНАРОДНАЯ ИНТЕГРАЦИЯ В БОРЬБЕ С ПРОЯВЛЕНИЯМИ ТЕРРОРИЗМА В ИНТЕРНЕТЕ

Аннотация. Вступление в силу Директивы 2017/541 криминализировало на европейском правовом пространстве преступление публичной провокации к совершению террористического преступления: теперь преступным признан не только террористический акт, но и любые формы пропаганды терроризма, включая прославление, оправдание терроризма, проявления неуважения к жертвам террористических проявлений в Интернете. Поскольку имплементация положений указанной Директивы в законодательство Государств-участников является обязательной, подход к выявлению, предупреждению, пресечению, раскрытию и расследованию этой категории преступлений, а также подход к назначению наказания за их совершение на территории Европейского Союза будет унифицирован; отношения в сфере апологии терроризма переходят из информационно-правового регулирования в уголовно-правовую сферу уже не на уровне отдельного государства, но на наднациональном уровне.

Ключевые слова: Интернет, терроризм, прославление терроризма, пропаганда терроризма, призывы к терроризму, Директива 2017/541, борьба с терроризмом, провокация, подстрекательство, восхваление, апология терроризма, блокирование, удаление контента, наднациональное регулирование, международное право, кибертерроризм.

Antonina Vasilievna PETRYAKOVA
senior lecturer
Moscow International University

INTERNATIONAL INTEGRATION IN THE COUNTERING TERRORISM ON THE INTERNET

Abstract. The enforcement of Directive 2017/541 criminalizes the crime of public provocation to commit a terrorist crime in the European legal space: now not only a terrorist act is criminalized, but also any form of propaganda of terrorism on the Internet, including glorifying, justifying terrorism, showing disrespect for the victims of terrorist manifestations. The implementation of the provisions of the Directive into the legislation of the EU States is required. So the approach to the identification, prevention, suppression, disclosure and investigation of the category of crimes, as well as the approach to sentencing for committing them in the territory of the European Union will be unified. The relations in the sphere of apology for terrorism are transferring from the

information-legal regulation into the criminal law sphere not in one only country but at the supranational level.

Keywords: Internet, terrorism, glorification, propaganda, calls for terrorism, Directive 2017/541, provocation, incitement, praise, apology, blocking, removal of content, supranational regulation, international law, cyberterrorism.

Призывы к совершению террористических актов и восхваление терроризма в Интернете, а также дополнительные возможности, которые предоставляет Интернет как средство информационного обмена и коммуникации, в том числе в преступных целях, позволяют в настоящее время рассматривать его как источник террористической угрозы и требуют использования различных правовых инструментов для ограничения/блокирования распространения соответствующего вредоносного контента и наказания преступников.

Безусловный интерес в этой связи вызывают исследования российских ученых на тему борьбы с преступлениями террористической направленности, совершаемыми с использованием сети Интернет. Этой теме посвящены некоторые работы В.В. Войникова¹, А.Г. Волеводза², В.П. Кашепова³. Проблемы, связанные с кибертерроризмом, исследуются в работах О.А. Степанова⁴. Криминализация и декриминализация как способы трансформации уголовного права рассматриваются в трудах коллектива ученых Института законодательства и сравнительного правоведения при Правительстве РФ⁵. Вопросам взаимодействия правоохранительных органов на международном правовом пространстве и имплементации зарубежного правоохра-

¹ *Войников В.В.* Правовое регулирование борьбы с терроризмом в рамках ЕС // *Lex Russica*. 2019. № 2. С. 121–131.

² *Волеводз А.Г.* Международно-правовые основы противодействия боевикам-террористам и внутригосударственное право // *Московский журнал международного права*. 2017. № 1. С. 98–109.

³ *Кашепов В.П.* Уголовно-правовое регулирование противодействия терроризму // *Уголовное право*. 2006. № 3. С. 31–36.

⁴ *Степанов О.А.* Противодействие кибертерроризму в цифровую эпоху. М., 2020; *Он же.* О правовом регулировании отношений в сфере безопасного функционирования и развития систем искусственного интеллекта // *Уголь*. 2020. № 6. С. 21–22.

⁵ *Криминализация и декриминализация как формы преобразования уголовного законодательства / под ред. В.П. Кашепова.* М., 2018.

нительного опыта посвятил свои работы доктор юридических наук, профессор О.А. Зайцев⁶.

Из зарубежных исследователей в рассматриваемой области следует особо отметить Кристиана Каунерта (Christian Kaunert)⁷, Габриэля Вайман (Gabriel Weimann)⁸, занимающихся исследованием разнообразных проявлений терроризма, включая кибертерроризм в сети Интернет.

Директива 2017/541, принятая Европейским Парламентом и Советом Европейского Союза 15 марта 2017 г.⁹ (далее по тексту – Директива), направлена на гармонизацию уголовно-правовых норм Европейского Союза о борьбе с терроризмом и адаптацию законодательства Европейского Союза к новым вызовам и угрозам террористического характера путем, в числе прочего, криминализации некоторых новых видов преступлений. Европейский законодатель ввел новый состав уголовного преступления – преступление публичной провокации к совершению террористического преступления (the offence of public provocation to commit a terrorist offence), которое включает в себя прославление, оправдание терроризма, распространение сообщений, изображений в Интернете и в автономном режиме, связанных с жертвами терроризма, в качестве способа получения одобрения террористических целей.

⁶ *Зайцев О.А.* Основные направления развития уголовнопроцессуального законодательства в условиях цифровизации // Вестник Московского университета МВД России. 2020. № 3. С. 18–20; *Зайцев О.А., Смирнов П.А., Тлехуч З.А.* Новые правовые возможности участия России в международном сотрудничестве по уголовным делам на европейском континенте и перспективы их применения // Международное уголовное право и международная юстиция. 2020. № 4. С. 7–10; *Зайцев О.А., Епихин А.Ю., Мишин А.В.* Проблемы имплементации международного опыта безопасности участников российского уголовного процесса // Международное уголовное право и международная юстиция. 2018. № 2. С. 3–7.

⁷ *Kaunert C.* Supranational governance in EU counter-terrorism. *Central European Journal of International and Security Studies*. 2010. Vol. 4. № 1. P. 1–32.

⁸ *Weimann G.* 2016. Going Dark: Terrorism on the Dark Web // *Studies in Conflict & Terrorism*. 2016. № 39 (3). P. 195–206.

⁹ См. подробнее: Директива Европейского Парламента и Совета ЕС 2017/541 от 15 марта 2017 г. о противодействии терроризму, о замене Рамочного Решения 2002/475/ПВД Совета ЕС и об изменении Решения 2005/671/ПВД Совета ЕС. URL: <https://eur-lex.europa.eu/eli/dir/2017/541/oj> (дата обращения: 12.09.2020).

Директива устанавливает минимальные меры уголовной ответственности для физических лиц за террористические преступления. В частности, она предписывает Государствам-участникам принимать надлежащие меры для того, чтобы преступления, перечисленные в ст. 4 Директивы (включая преступления публичной провокации к совершению террористического преступления), наказывались лишением свободы с максимальным сроком наказания не менее 15 лет за преступление, упомянутое в пункте (а) ст. 4 (руководство террористической группой – А.П.), а за преступления, перечисленные в пункте (б) ст. 4 (участие в деятельности террористической группы – А.П.), максимальным сроком наказания не менее 8 лет¹⁰. Для сравнения скажем, что положения ст. 205² УК РФ за совершение публичных призывов к осуществлению террористической деятельности, публичное оправдание терроризма, пропаганду терроризма, в том числе в сети Интернет, предусматривают иное, менее строгое максимальное наказание. Интересно также, что Директива не разделяет по виду и размеру максимального наказания ответственность за совершение террористического акта и, например, ответственность за совершение публичных призывов к совершению актов терроризма, фактически уравнивая ответственность за эти преступления и признавая их равновеликую тяжесть и опасность.

Согласно ст. 28 Директивы Государствам-участникам следует к 8 сентября 2018 г. ввести в действие законы и процедуры, необходимые для соответствия Директиве. Директива обязательна для всех Государств-участников. Тем не менее статистика имплементации Директивы¹¹ в национальное законодательство Государств-участников показывает, что некоторые государства (например, Дания, Ирландия) не принимали нормативные правовые акты для целей гармонизации национального права и Директивы (статистика имплементации содержит сведения «0 мер принято»), тогда как иные государства (например, Финляндия) включили текст Директивы

¹⁰ Петрякова А.В. Противодействие апологии терроризма в глобальной сети Интернет на европейском правовом пространстве // Союз криминалистов и криминологов. 2020. № 3. С. 165.

¹¹ URL: <https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32017L0541> (дата обращения: 06.11.2020).

в свое законодательство дословно или почти дословно¹². Причины полного отказа от преобразования национального законодательства или частичного следования нормам Директивы, на наш взгляд, необходимо изучить дополнительно.

Факт принятия Директивы указывает на признание необходимым гармонизации законодательства в рассматриваемой сфере и, в частности, в сфере борьбы с публичной провокацией к совершению актов терроризма, на европейском правовом пространстве. Думается, что трагические события недавнего времени, произошедшие в некоторых европейских странах, ускорят интеграционные процессы для достижения общей цели борьбы с терроризмом, в том числе с его проявлениями в сети Интернет. В дальнейшем, полагаем, возможна и необходима международная унификация уголовно-правовых механизмов борьбы с терроризмом, поскольку «архитектура глобальной информационно-коммуникационной сети предполагает международный характер взаимодействия»¹³ и очевидно, что взаимодействия на национальном и даже наднациональном уровне недостаточно; необходимо международное, глобальное объединение усилий государств.

¹² *Петрякова А.В.* Борьба с пропагандой терроризма в Интернете: опыт ЕС // Национальные проекты в системе приоритетов развития российской экономики: социальные, правовые и духовные аспекты: материалы XIV международной научно-практической конференции // под ред. А.Д. Моисеева, В.В. Черняева. Елец, 2020. С. 116.

¹³ *Степанов О.А.* О проблеме конкретизации права в условиях цифровизации общественной практики // Право. Журнал Высшей школы экономики. 2018. № 3. С. 9.

Екатерина Анатольевна РОДИНА
помощник Урюпинского межрайонного прокурора
Волгоградской области;
аспирант
Саратовская государственная юридическая академия

О НЕКОТОРЫХ ПРОБЛЕМАХ МЕХАНИЗМА ДЕТЕРМИНАЦИИ ПРЕСТУПНОСТИ И ВИКТИМНОГО ПОВЕДЕНИЯ

Аннотация. В статье рассмотрены теории детерминации преступности. В теории криминологии часть детерминационного комплекса, влияющего на формирование личности преступника, выносится за пределы рассмотрения причин отдельных видов преступления и рассматривается в разделе «Личность преступника». Те же обстоятельства, которые именуются причинами преступлений, фактически являются лишь условиями, оказывающими наиболее сильное воздействие на мотивацию преступника. Качественной разницы между причинами единичного преступления и причинами всей преступности не имеется. Они соотносятся между собой как часть и целое. Неопределенность криминологических прогнозов свидетельствует не о своеобразии причинных связей, действующих на уровне всей преступности, и их вероятностном характере, а лишь о недостаточном количестве криминологической информации и несовершенстве способов ее описания.

Ключевые слова: преступность, причины преступности, виктимность, предупреждение преступности, общее, частное.

Ekaterina Anatolevna RODINA
assistant to the Uryupinsk inter-district Prosecutor
Volgograd region;
postgraduate student
Saratov State Law Academy

SOME PROBLEMS OF THE MECHANISM OF DETERMINATION OF CRIME AND VICTIM BEHAVIOR

Abstract. The article deals with problematic theories of crime determination. In the theory of criminology, part of the determinative complex that affects the formation of the criminal's personality is removed from the scope of consideration of the causes of certain types of crime and is considered in the section "the criminal's Personality". The same circumstances that are called the causes of crimes, in fact, are only the conditions that have the strongest impact on the motivation of the criminal. There is no qualitative difference between the causes of a single crime and the causes of all crime. They relate to each other as part and whole. The uncertainty of criminological forecasts does not indicate the uniqueness of causal relationships that operate at the level of all crime, and their probabilistic

nature, but only an insufficient number of criminological information and imperfect ways to describe it.

Keyword: crime, causes of crime, victimization, crime prevention, general, private.

В криминологической теории проблема детерминации преступности является одной из самых сложных. Несмотря на то, что теории причинности развиваются уже длительное время, до настоящего времени имеется ряд неясных вопросов. Еще более слабо развита теория виктимологической детерминации, которая начала развиваться значительно позже и в которой до настоящего времени, как указывает К.В. Вишневецкий, вопрос о механизме виктимного поступка и системе его детерминации до настоящего времени остается открытым, поскольку преступник и жертва – индивидуально и типологически разные люди¹.

Не стоит говорить о том, что проблематика виктимологической детерминации преступлений, совершаемых в сети Интернет, и виктимологического предупреждения таких преступлений разработаны в еще меньшей степени.

Поэтому прежде чем строить научно-обоснованную систему виктимологического предупреждения преступлений в сети Интернет, необходимо прояснить некоторые неразрешенные общие вопросы причинности.

Необходимость такого подхода, на наш взгляд, обусловлена тем, что предупреждение преступности, как и любая целенаправленная деятельность, нуждается в точном определении желаемых результатов воздействия. В связи с этим необходимо разграничить виктимологическую профилактику от специально-криминологической, с тем, чтобы определить объекты воздействия в обоих случаях. И, если они не совпадают, ставить вопрос о нормативном определении виктимологической профилактики. Для этого нужно уяснить, какое место в детерминации преступлений занимают обстоятельства, относящиеся к его жертве, являются ли они лишь условиями, или могут выступать и в качестве причин совершаемого преступления.

¹ Вишневецкий К.В. Механизм виктимологической детерминации // Теория и практика общественного развития. № 2014. № 10. С. 154–157.

В отдельных работах по криминологии встречаются пессимистические взгляды относительно возможностей корректно определить причины преступлений. Так, Е.Г. Самовичев, характеризуя современную концепцию причин преступности, отметил, что она не выдерживает никакой критики, поскольку никаких причин в строгом смысле слова установить не удастся².

В.Н. Фадеев в ходе глубокого анализа современной концепции причинности приходит даже к более радикальному выводу о необходимости в объяснении причин преступности отказаться от материализма и сформулировать новую концепцию³.

В качестве основной проблемы он указывает то, что разработанный в криминологической теории комплекс представлений о причинах, условиях, факторах и детерминации преступности с точки зрения диалектической логики функционален лишь на уровне частного, но не общего⁴.

Разделяем мнение, что в объяснении причин преступности все «хорошо работает» на уровне единичных преступлений, однако попытка перенести эти объяснения на уровень всей преступности упирается в необходимость возвращать к жизни отвергнутые ранее положения позитивистской школы и поэтому криминологи, как отметил Е.Г. Самовичев, уводят проблематику «в сферу системности, сложности», уклоняясь от предметного объяснения.

Проиллюстрируем сказанное на примере. Если говорить о сущности причинной связи, то в соответствии с определением, она состоит в производстве причиной следствия. Причина – это внутренняя связь между тем, что уже есть и тем, что им порождается, им только становится⁵.

В приложении к преступному поведению это означает, что причина – это то, что со всей необходимостью, закономерно побуждает

² Здесь приводится выдержка из стенограммы научно-практического межвузовского семинара «Какая криминология сегодня нужна стране? (Проблемы преподавания и практического применения)», прошедшего 19 апреля 2011 г. Цит. по: Фадеев В.Н. Причинность в криминологии и детерминация преступности // Криминология: вчера, сегодня, завтра. 2017. № 3 (46). С. 21–27.

³ Философский энциклопедический словарь. М., 1983. С. 532.

⁴ Стручков Н.А. Преступность как социальное явление: лекции. Л., 1979.

⁵ Философский энциклопедический словарь. С. 532.

лицо совершить общественно опасное деяние. В этой связи уместно вспомнить, что фундаментальной предпосылкой юридической ответственности является свобода воли индивида. Таким образом, в юриспруденции и, наиболее детально, в уголовном праве в настоящее время определено, что уголовная ответственность устанавливается лишь в отношении вменяемых лиц, то есть лиц, осознающих фактический характер своих действий и способных руководить ими, или, иными словами, обладающими свободой воли. Неспособность хоть в малейшей степени осознавать фактический характер своих действий или руководить ими является, в соответствии со ст. 21 УК РФ, признаком невменяемости, исключающей уголовную ответственность.

Сказанное означает, что причина любого преступления лежит не в сфере общественной жизни, как указывается во многих учебниках криминологии⁶, не в особенностях экономических отношений, имущественном неравенстве, несправедливости и т.п., а в личности преступника. Как писал в этой связи Н.А. Стручков, непосредственные причины преступления находятся в сфере сознания, поскольку все побудительные силы, вызывающие действия человека, должны обязательно пройти через его голову и превратиться в побуждения его воли»⁷.

По поводу того, как формируются эти побуждения воли, есть несколько объяснений. Например, А.И. Долгова указывала, что традиционно-диалектический подход предусматривает одностороннее влияние объективных факторов преступности на субъективные: «материальные условия жизни людей определяют общественное сознание, а уже оно – преступность. Отсюда оценка общественной психологии (ранее упоминалось в связи с этим об «отставании сознания от бытия») как непосредственной, ближайшей причины преступности»⁸.

⁶ Как, к примеру, писал М.Д. Шаргородский, причины конкретного преступления – это ... те активные силы, которые вызывают у субъектов интересы и мотивы для его совершения». См.: *Шаргородский М.Д.* Преступность, ее причины и условия в социалистическом обществе // Преступность и ее предупреждение. Л., 1966. С. 30.

⁷ *Стручков Н.А.* Указ. соч.

⁸ *Долгова А.И.* Криминология: учебник для вузов. М., 2005. С. 258–259.

Э.А. Поздняков в своей работе «Философия преступления» красной нитью проводит мысль о том, что причина совершения преступлений состоит, прежде всего, в том, что человек от природы склонен к отклоняющемуся поведению. Такое поведение – не патология, а норма⁹.

Этому мнению вторит В.Н. Фадеев, по мнению которого «корни преступности кроются в самой дуально-диалектической природе человека, как социально-биологического существа, а плохие условия жизни людей являются лишь катализатором, ускоряющим проявление правонарушающего, «криминального начала» в сознании и жизни индивидуума»¹⁰.

Таким образом, имеются две точки зрения на непосредственную причину преступности, плохо совместимые между собой для того, чтобы уместить их в единой теории. Нетрудно заменить, что абсолютизация каждой из них возвратит нас на те же теоретические позиции, которые сложились в криминологии более ста лет назад (речь идет о социологическом и антропологическом направлении в криминологии). При этом, обе эти позиции слабо совместимы и с представлениями о свободе воли, лежащей в основе уголовной ответственности. Вместе с тем у этих взглядов есть и нечто общее – причинами единичного преступления можно называть некоторые особенности личности, делающие для соответствующего индивида позволительным совершение преступления для реализации своих потребностей (иногда в таких случаях говорят о деформациях личности). В криминологии эта часть причинного комплекса сконцентрирована в представлениях о формировании личности преступника и обычно «выносятся за скобки» в рассуждениях о причинах конкретного преступления, ограничивая их изучение относительно небольшим интервалом времени, связанным с негативными изменениями в личности отдельного человека.

Зафиксировав это, перейдем к следующему проблемному вопросу теории детерминации. Оставив за кадром рассуждения о том, как формируются побудительные мотивы, обратимся к тому, как

⁹ Поздняков Э.А. Философия преступления. М., 2001.

¹⁰ Фадеев В.Н. Причинность в криминологии и детерминация преступности // Криминология: вчера, сегодня, завтра. 2017. № 3 (46). С. 21–27.

в теории происходит переход от рассмотрения причин единичного преступления к причинам всей преступности.

Приняв за отправную точку то, что в обществе есть определенная группа лиц, склонных в силу имеющихся деформаций, полагаем возможным ожидать, что при возникновении неблагоприятных внешних условиях или в случае возникновения удобной ситуации они будут интенсивно совершать преступления.

Однако имея возможность заранее определить количество совершаемых преступлений, нельзя точно указать, кто именно их совершит. Так, изучая статистические данные МВД России, Генеральной прокуратуры РФ, Судебного департамента при Верховном Суде РФ за ряд лет, можно прогнозировать, что в 2021 г. будет зарегистрировано около 7 тыс. убийств и покушений на убийство. Уверенность таким ожиданиям придает то, что в течение ряда лет количество таких преступлений постоянно снижалось и, несмотря на то что в стране в связи с неблагополучной эпидемиологической обстановкой наблюдаются и негативные процессы в экономике, каких-либо катастрофических сценариев изменения преступности не наблюдается.

Также можно очертить и примерный круг лиц, совершивших такие преступления: как правило, это граждане, не имеющие постоянного места работы, недавно освободившиеся из мест лишения свободы и злоупотребляющие алкоголем¹¹.

Казалось бы: вот точно очерченный объект для специально-криминологического воздействия и нужно всего лишь подвергнуть профилактическому воздействию силами правоохранительных органов 3,6 млн. безработных (по данным Росстата), чтобы радикально снизить не только количество убийств, но и целый ряд других посягательств на личность и собственность. Однако, по всей видимости, даже такое количество потенциальных подозреваемых

¹¹ По данным С.Ю. Бытко, более 70 % убийств совершается в состоянии алкогольного опьянения и доля таких лиц постоянно растет, более 70 % убийц не имели места работы, примерно треть из них имеют неснятую или непогашенную судимость. См.: Бытко С.Ю. Эффективность предупредительного воздействия уголовного наказания на преступность: теоретический и прикладной аспекты: дис. ... докт. юрид. наук. Саратов, 2018. С. 56, 65 и др.

составляет чрезмерную нагрузку на правоохранительную систему. Сузить же их круг, вычленив из этой массы всего 5–6 тыс. наиболее вероятных убийц, к огромному разочарованию, невозможно. И здесь возникает один из самых сложных вопросов – как сочетать представления о причинности как проявлении закономерных процессов, хорошо работающих на уровне конкретного преступления, с вероятностными результатами, возникающими при рассмотрении массовых проявлений преступности и попытках прогноза индивидуального поведения? Проблема в том, что включение в процесс детерминации стохастического элемента полностью обесценивает все предшествующие рассуждения о механизме детерминации, поскольку, согласно теории вероятности, вероятность совершения преступления будет определяться уже не строго детерминированными закономерностями в поведении человека, а именно той, не поддающейся полноценному исследованию, случайностью. Так, для рассмотренных выше убийств, вероятность успешного поиска возможного убийцы на основе приведенных данных о его личности во всей массе безработных, составляет, по нашим оценкам 0,15 %. Для организации целенаправленной государственной деятельности очевидно, что такой прогноз бесполезен и равносителен отсутствию всякого прогноза.

Возможно, именно такой низкой результативностью прогнозов и обусловлена потеря государством интереса к результатам криминологических исследований. Интересно, что сходная ситуация сложилась с исследованиями склонности к преступному поведению на основе анализа дерматоглифической картины рук. Так, изучение дерматоглифики серийных маньяков показало, что все они обладают редким типом ассиметрии в распределении узоров. Для А. Чикатило, как указывают авторы работы, была характерна локализация узора более высокой сложности на большом пальце левой руки – самый редкий тип левшества, составляющий всего 2,5 % в популяции¹². Заметим, что 2,5 % носителей такого типа ассиметрии во всей массе

¹² *Богданов Н.Н.* Дерматоглифика пишущих левой // *Вопр. психол.* 1997. № 2. С. 76–87; *Богданов Н.Н., Самищенко С.С., Хвьяля-Олинтер А.И.* Дерматоглифика серийных убийц // *Вопросы психологии.* 1998. № 4. С. 64.

населения РФ составляет 3,6 млн чел. Так что «угадать» серийного убийцу только по дерматоглифическим признакам не удастся.

В.Е. Эминов, задаваясь вопросами о том, возможен ли переход от объяснения единичного преступления к общему (всей преступности), подчиняется ли движение преступности тем же причинным законам, что и поведение отдельного лица, или речь должна идти о совершенно иных типах детерминации, пришел к выводу, что причинные связи применительно к преступности вообще несколько иные, чем в каждом индивидуальном акте преступного поведения, поскольку массовые явления имеют специфические свойства (например, количественную устойчивость), которых у индивидуального события нет¹³.

При этом автор указывает, что механистическое понимание причинности как «жесткой», однозначной связи между явлениями приводит к выводу о неприменимости этого понятия для объяснения массовых вероятностных процессов¹⁴.

Не совсем понятен термин «механистическое понимание причинности». Полагаем, что причинная связь, если она есть, предполагает именно такую, «жесткую», как характеризует ее В.Е. Эминов, связь между явлениями и процессами. Другое дело, что исследуя поведение человека, невозможно в полной мере исследовать всю сложность психических процессов, нюансов его реакции на изменения в окружающей обстановке, природных факторов и т.п. Отсюда возникает неточность прогнозов преступного поведения. Предположения основываются на мизерном количестве факторов преступности, доступных для количественной и качественной оценки, поэтому несоответствие теоретических оценок реальным показателям преступности воспринимается как отсутствие жесткой связи.

Однако, на наш взгляд, это никак не свидетельствует о принципиально иной природе детерминации всей преступности. Скорее речь идет о степени неполноты наших знаний о поведении человека. Возвращаясь к примеру с убийствами, сказанное можно сформулировать так: знания о поведении обеспечивают точность прогноза индивидуального преступного поведения на уровне 0,15 %. Не-

¹³ Эминов В.Е. Причины преступности в России: криминологический и социально-психологический анализ. М., 2011. С. 11, 12.

¹⁴ Там же.

сомненно, наращивая объем данных о преступниках, в настоящее время можно резко повысить точность прогноза. Например, включая в анализ пол, возраст, образование, состояние здоровья, круг общения, продолжительность пребывания в статусе безработного, наличие семьи, детей, родственников и т.п., можно довести точность прогноза до приемлемых для практического применения показателей.

Подводя итог рассуждениям, сделаем некоторые промежуточные выводы:

- непосредственные причины преступления кроются в личности;
- наиболее общие причины всей преступности, влияющие на деформацию системы нравственных ценностей личности, ее потребности и проч. относятся к вопросам личности преступника и поэтому, являясь, по сути, элементами причинного комплекса, в качестве таковых не рассматриваются;
- причины конкретного преступления и причины всей преступности сходны и относятся между собой как часть и целое (где часть – причины конкретных преступлений, целое – причины всей преступности);
- внешние по отношению к личности факторы, именуемые в криминологии причинами преступлений, таковыми фактически не являются. Имеет место своеобразная терминологическая маскировка, при которой наиболее важные и близкие по времени к преступлению условия именуются причинами;
- изучение причин конкретных преступлений необходимо переводить на современные рельсы, накапливая максимальное количество информации о личности преступника, обстоятельствах совершения преступления для дальнейшей ее автоматизированной обработки (речь идет о таком направлении исследования огромных массивов данных, которые вручную обработать невозможно, и именуемом «BigData», большие данные).

В той части, которая характеризуется причинами индивидуального поведения, приведенные рассуждения применимы и к причинам виктимизации. Личность жертвы как совокупность специфических особенностей психики, мировоззрения, физиологических качеств формируется под влиянием общественных отношений, особенности которых, по всей видимости, и следует рассматривать в качестве общей причины виктимизации.

В то же время детерминация виктимного поведения имеет и свои особенности. В ряде случаев нельзя говорить о включении виктимности в механизм детерминации.

Например, гражданин П., имея в силу служебных полномочий доступ к служебным базам данных оператора сотовой связи «Вымпел-Коммуникации», намереваясь использовать доступ в Интернет для преступных целей и в целях маскировки своей деятельности, получил доступ к управлению абонентским номером и сопряженными с ним мобильными приложениями клиента компании, телефонный номер которого он выбрал произвольно, что привело к блокированию доступа к компьютерной информации для потерпевшего.

В других случаях характерным свойством отдельных видов преступлений в сети Интернет является то, что вред может причиняться неопределенному числу лиц. Например, мошенники организывают call-центр и обзванивают граждан, обращаясь к ним под видом сотрудников социальных служб и обещая компенсацию. В таких ситуациях личные качества потерпевшего выступают необходимым условием совершения в отношении него преступления.

Мошенники, организуя определенный вид обмана, учитывают потенциальный круг потерпевших с тем, чтобы оценить прибыль от совершения преступлений. Например, получая доступ к базе данных лиц, ранее пострадавших от каких-либо незаконных действий, они рассчитывают, что значительная часть из них может быть обманута ими. Если эта часть меньше определенного значения, то потенциальная прибыль не возместит расходов на организацию преступления. В таких ситуациях распространенность определенных качеств личности потенциальных жертв может выступать в качестве причины вида преступлений. Например, в нашем случае – значительное число лиц в пожилом возрасте, имеющих сходные проблемы и обладающих в силу возраста слабыми знаниями о функционировании сети Интернет, особенностях государственного социального обеспечения, позволявших им бы определить мошенника и т.п.

Галина Сергеевна САБЕЛЬНИКОВА

студент

Московская академия Следственного комитета

Российской Федерации

КИБЕРПРЕСТУПНОСТЬ В БАНКОВСКОЙ СФЕРЕ. ТЕНДЕНЦИИ И ОСОБЕННОСТИ РАССЛЕДОВАНИЯ

Аннотация. Расследование преступлений, совершаемых посредством компьютерных технологий, – уже не новая задача для правоохранительных органов. С каждым днем количество таких общественно опасных деяний увеличивается, а способы их реализации совершенствуются. Вместе с тем отметим, что компьютерные технологии стали составной частью финансового механизма государства, в том числе и его банковского сектора. Личные данные клиентов банка, их денежные средства – потенциальные объекты для посягательства для так называемых киберпреступников. В связи с этим имеется необходимость рассмотрения отдельных аспектов расследования киберпреступлений в банковском секторе.

Ключевые слова: банки, банковская деятельность, киберпреступления, киберпреступность, расследование преступлений.

Galina Sergeevna SABELNIKOVA

student

Moscow Academy of the Investigative Committee of the Russian Federation

CYBERCRIME IN THE BANKING SECTOR. TRENDS AND FEATURES OF THE INVESTIGATION

Abstract. Investigation of the crimes committed with use of computer technologies is not new law enforcement agencies. Every day the number of crimes increases, and ways of their commission are improved. However, computer technologies – became an element of the financial mechanism of the state including its banking sector. Personal data of clients of bank, their money are potential objects for encroachment of cybercriminals. In this regard there is a need of consideration of the separate moments of investigation of cybercrimes for the banking sector.

Keywords: banks, bank activity, cybercrime, cybercrime, investigation of crimes.

Киберпреступность – реалии современного информационного мира. Как правило, совершение киберпреступлений направлено на получение материальной выгоды, поэтому объектами посягательства с точки зрения уголовного права является чужое имущество, в том числе денежные средства физических и юридических лиц, которые хранятся на банковских счетах. Вместе с тем крупные

транзакции, банковские счета с денежными накоплениями, персональные данные клиентов банка, а также недостаточно высокая степень защиты от кибератак, невнимательность клиентов стимулируют преступный контингент на совершение киберпреступлений в банковской сфере.

Составное понятие киберпреступности имеет «зарубежные корни»¹, а именно в футуристичном слове «cyber», которое современники используют с отсылкой на технические понятия, связанные с работой компьютеров, принадлежностью к виртуальному пространству сети Интернет. Существует несколько вариантов определения киберпреступности. Согласно установленным рекомендациям ООН, киберпреступность – это совершение любого преступления, направленного против конфиденциальности, целостности и доступности компьютерных данных или систем; преступления, предполагающие использование компьютера в целях извлечения личной или финансовой прибыли или причинения личного или финансового вреда; преступления, связанные с содержанием компьютерных данных². Тем не менее, следует отметить, что это преступления, которые могут совершаться не только с помощью компьютера, но и с помощью мобильного устройства.

В настоящее время практически любое преступление может быть реализовано при помощи компьютера, информационно-телекоммуникационных технологий и сетей. Так как сфера наших интересов находится в рамках финансового сектора экономики, рассмотрим киберпреступления в банковской сфере.

К киберпреступлениям в банковской сфере могут быть отнесены следующие составы преступлений, установленные УК РФ: п. «г» ч. 3 ст. 158 «Кража с банковского счета, а равно в отношении электронных средств», ст. 159³ «Мошенничество с использованием

¹ What is the Origin of the Word «Cyber»? //Alpine security. URL: <https://alpinesecurity.com/blog/what-is-the-origin-of-the-word-cyber/> (дата обращения: 05.11.2020); Варламова А.О. Английские заимствования в современном французском языке // Научный вестник Международного гуманитарного университета. Сер.: Филология. 2018. № 33 (2). С. 25.

² Comprehensive Study on Cybercrime/ United Nation Office on Drugs and Crime (UNDOC). 2013. P. 6–11.

электронных средств платежа», ст. 159⁶ «Мошенничество в сфере компьютерной информации», ст. 183 «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», ст. 187 «Неправомерный оборот средств платежей».

К рассматриваемой категории также следует отнести составы преступлений, включенных в гл. 28 «Преступления в сфере компьютерной информации» УК РФ (ст. 272–274¹).

Согласно данным отчета об инцидентах информационной безопасности при переводе денежных средств за I и II кварталы 2019–2020 гг. от 29 октября 2020 г., формируемого Банком России, на основании документов отчетности, подаваемых кредитными организациями, доля возмещенных средств клиентам от операций, проведенных без их согласия операций с использованием электронного средства платежа за 2019 г. составил в сумме за оба квартала 47,1 трлн руб., в 2020 г. – 41,9 трлн руб.; объем операций по переводу денежных средств, совершенных без согласия клиентов в первом квартале 2020 г. вырос на 38 %, по сравнению с первым кварталом 2019 г., а во втором квартале прирост составил 59 %³.

Осуществление таких транзакций представляет собой виновно совершенное уголовно наказуемое общественное опасное деяние, квалифицируемое в соответствии с УК РФ. Преступления, связанные с проведением операций без согласия клиентов, совершаются с применением компьютерных технологий, часто совместно с использованием методов социальной инженерии⁴.

Вопросы о киберпреступлениях в банковском секторе экономики стоят остро и в других государствах. Согласно исследованию, проведенному на международном уровне и опубликованному в 2019 г. компанией «IntSights»⁵, занимающейся разведкой и вы-

³ Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. I и II кварталы 2019–2020 годов. Банк России. URL: https://www.cbr.ru/analytics/ib/review_1q_2q_2020/ (дата обращения: 31.10.2020).

⁴ Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год. Банк России. URL: https://www.cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (дата обращения: 01.11.2020).

⁵ IntSights – платформа для анализа внешних угроз и защиты, созданная для нейтрализации киберугроз за пределами сети.

явлением киберугроз, более 25 % атак вредоносного программного обеспечения направлено на банки и финансовые организации. По сравнению с 2018 г. количество мошенничества с банковскими картами увеличилось и составляет 212 %⁶. Таким образом, вопрос, киберпреступности в банковской сфере представляет собой проблему не только национального, но и международного уровня.

В настоящее время имеется множество спорных вопросов при расследовании указанной категории преступлений.

Методика расследования преступлений, совершенных с помощью компьютерных технологий в банковской сфере имеет свои особенности, обусловленные спецификой банковской деятельности по обслуживанию клиентов, использованием специальных технологий, таких как система дистанционного банковского обслуживания, система искусственного интеллекта и др.

Например, в методику расследования входят способы совершения киберпреступлений в банковской сфере. Эти способы будут охватывать типичные способы совершения компьютерных преступлений и способы совершения хищения денежных средств с помощью специального оборудования. Заметим, что совершенствование системы защиты от киберугроз и кибератак в банковских организациях и наращивание опыта правоохранительных органов в расследовании подобных преступлений стимулируют на появление новых путей незаконного завладения преступниками денежными средствами.

Существуют следующие способы совершения киберпреступлений в банковской сфере: совершение преступлений в системе дистанционного банковского обслуживания (далее – ДБО), способ совершения преступления, связанный с подделкой платежных карт, совершение преступления, связанного с хищением денежных средств с банкомата⁷.

Система ДБО представляет собой технологию предоставления банковских услуг на основании распоряжений, передаваемых

⁶ Banking & Financial Services. Cyber Threat Landscape Report. Intsigths 2019. P. 4.

⁷ Головинов О.Н., Погорелов А.В. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. 2016. № 6 (1). С. 83.

клиентом без его визита в банк, как правило, используя при этом компьютерные или телефонные сети⁸.

На сегодняшний день используются следующие виды ДБО: технология «банк-клиент», Интернет-банкинг, мобильный банкинг, с использованием внешних сервисов – банкоматов и устройств банковского самообслуживания⁹. В свою очередь, используя систему ДБО, злоумышленники могут применять следующие способы для достижения преступной цели: использование вредоносных программ скрытого управления; использование программ считывания пароля; применение программ удаленного доступа; создание так называемого «зеркального» сайта или «сайта двойника»; перечисление денежных средств на так называемые «электронные кошельки» злоумышленникам, также используются такие схемы как отправка ложной информации «проблема у родственника» и получение звонков, SMS-сообщений «Ваша карта заблокирована»¹⁰.

Именно такими способами воспользовались участники хакерской группы во главе с братьями Д. и Е. В период с марта 2013 г. по май 2015 г. с помощью вредоносных программ «QHost», «Patched.IB», «grcss.dll» и др., обеспечивающих процесс хищения, группа осуществляла атаки на систему ДБО системообразующих российских банков, похитив таким образом более 12,5 млн руб.

Следствием установлено, что осужденные «заражали» компьютеры пользователей вирусом, который перенаправлял клиента на поддельную – «зеркальную страницу» банка, отличную от оригинала несколькими символами в адресной строке. Затем под предлогом смены политики безопасности, пользователи вводили данные банковской карты и код подтверждения со скретч-карты банка. Используя эти данные, преступники выводили деньги через настоящий сайт дистанционного банковского обслуживания (ДБО)¹¹.

⁸ Алексеров В.И., Колокольчикова О.Н., Василенко Л.В. Раскрытие преступлений в системе дистанционного банковского обслуживания: учебно-практическое пособие. Домодедово, 2020. С. 12; Лебедева А.А. Хищение денежных средств со счетов платежных карт // Безопасность бизнеса. Юрист. 2018. № 1. С. 59–64.

⁹ Системы дистанционного банковского обслуживания (рынок ДБО России) // TADVISER. Государство. Бизнес. ИТ. URL: <https://www.tadviser.ru/index.php> (дата обращения: 03.11.2020).

¹⁰ Алексеров В.И., Колокольчикова О.Н., Василенко Л.В. Указ. соч.

¹¹ Постановление об отказе в передаче кассационной жалобы для рассмотрения в судебном заседании суда кассационной инстанции № 4у/9-2730/19. Архив Московского городского суда.

В суд направлено уголовное дело по обвинению братьев Д. и Е. и их соучастников в совершении 813 преступлений, предусмотренных ч. 2 ст. 273 («Создание, использование и распространение вредоносных программ») УК РФ, ч. 3 ст. 272 («Неправомерный доступ к компьютерной информации») УК РФ, ч. 4 ст. 159 («Мошенничество в сфере компьютерной информации») УК РФ. В июле 2018 г. участникам группы вынесен обвинительный приговор.

Совершение киберпреступлений в банковской сфере с использованием поддельных, украденных пластиковых карт включает в себя использование личных данных владельцев карт при помощи установки специальных устройств на банкоматы (например, так называемые «cookie», «скиммеры»), которые позволяют считывать информацию с платежных карт.

Среди мировых тенденций киберугроз в банковском секторе, как отмечает в своем исследовании Banking & Financial Services Cyber Threat Landscape Report компания Intsigths, использование троянских программ (Adload, ATRAS, Emotet), использование уязвимостей протокола SS7.

Протокол SS7 (ОКС-7) разработан еще в 1970-х гг. и в настоящее время используется во всем мире для расчета биллинга сотовой связи и отправки текстовых сообщений. Несмотря на повсеместное использование, протокол обладает уязвимостями, которыми позволяют осуществить перехват SMS-сообщений и их перенаправление¹². Указанным способом воспользовались злоумышленники в 2017 г., перенаправив денежные средства клиентов немецких банков на их собственные счета¹³.

В феврале 2019 г. жертвами киберпреступников, которые также использовали недостатки протокола SS7, стали клиенты банка Metro Bank в Великобритании. В связи с тем, что недостатки протокола

¹² Кража денег с банковских счетов путем перехвата кодов в SMS. Kaspersky Daily. URL: <https://www.kaspersky.ru/blog/ss7-hacked/22218/> (дата обращения: 05.11.2020).

¹³ Schwachstelle im Mobilfunknetz: Kriminelle Hacker räumen Konten leer // Süddeutsche Zeitung. URL: <https://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504> (дата обращения: 05.11.2020).

не устранимы, специалисты рекомендовали банкам не использовать авторизацию клиентов через одноразовые SMS-пароли¹⁴.

Не остаются в стороне такие способы, как внедрение вредоносных приложений на коммутатор банкоматов АТМ, использование поддельных мобильных приложений, внедрение троянских программ в приложения банков на мобильных устройств (так называемые «банковские трояны»), DDoS-атаки, инсайдерские лазейки (когда посягательство осуществляет сотрудник банка, обналичивая в итоге денежные средства клиентов), фишинг и фишинговые наборы (пакет программного обеспечения, которое облегчает копирование дизайна сайта и загрузки его на другой веб-сервер в качестве фишинового сайта)¹⁵.

Таким образом, денежные средства физических и юридических лиц являются объектами посягательства со стороны преступных лиц и группировок, занимающихся киберпреступлениями. Наблюдается рост статистики: в частности, основываясь на собранных данных за 2018 г. и 2019 г., следует отметить, что увеличилась доля фишинговых атак на кредитные организации с 21,7 % почти до 30 %¹⁶, что связано с увеличением использования информационных технологий при совершении банковских операций, совершенствованием способов совершения киберпреступлений.

Необходимость в усилении борьбы с киберпреступлениями отметил Генеральный прокурор РФ И.В. Краснов, указав, что наблюдается ежегодный рост компьютерных атак, нацеленных на попытки взлома информационных систем государственных органов РФ, корпораций и банков¹⁷.

Рассмотренные способы совершения киберпреступлений в банковской сфере актуализируют необходимость совершенствования методики расследования киберпреступлений в банковской сфере.

¹⁴ Немецкие банки отказываются от поддержки авторизации по одноразовому SMS-коду // TADVISER. Государство. Бизнес. ИТ. URL: <https://www.tadviser.ru/index.php> (дата обращения: 05.11.2020).

¹⁵ Banking & Financial Services. Cyber Threat Landscape Report/ Intsigths 2019. p. 9.

¹⁶ Финансовые киберугрозы в 2019 году // Kaspersky Securelist. URL: <https://securelist.ru/financial-cyberthreats-in-2019/95792/> (дата обращения: 05.11.2020).

¹⁷ Генпрокурор РФ потребовал усилить борьбу с киберпреступлениями. URL: https://tvzvezda.ru/news/vstrane_i_mire/content/20207171518-tqoQj.html (дата обращения: 05.11.2020).

Илья Викторович СОРОКИН

аспирант

Московский финансово-юридический университет МФЮА

НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ПРОТИВОДЕЙСТВИЯ ПРАВОНАРУШЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. Постоянный рост числа пользователей, как физических, так юридических лиц (компаний), осуществляющих обмен информацией в электронной форме посредством информационно-телекоммуникационной сети Интернет, в том числе посредством электронных документов через операторов информационных системы, также с помощью средств электронной подписи, постоянный рост числа требований единой системы идентификации и аутентификации, операторов информационных систем, провайдеров хостинга, владельцев сайтов с необходимостью предоставления, обработки и распространения персональных данных физических лиц (субъектов персональных данных), а также рост числа способов мошенничества и их постоянная трансформация, ставят вопрос о направлении совершенствования противодействия правонарушениям, совершаемым с использованием информационных технологий. Таким образом, вопрос обеспечения безопасности информационной сферы, включающей информационные технологии, и информационной безопасности РФ становится все более актуальным, а совершенствование направлений противодействий правонарушениям и защиты прав пользователей и субъектов персональных данных в указанной сфере является крайне необходимым.

Ключевые слова: правонарушения, информационные технологии, информационно-телекоммуникационная сеть Интернет, электронный документ, электронная подпись, операторы информационных системы, пользователь, субъект персональных данных.

Ilya Viktorovich SOROKIN

postgraduate student

Moscow Finance and Law University MFUA

DIRECTIONS FOR IMPROVING THE COUNTERACTION TO OFFENSES COMMITTED WITH THE USE OF INFORMATION TECHNOLOGY

Abstract. The constant growth of the number of users, both individuals and legal entities (companies), exchanging information in electronic form through the information and telecommunication network «Internet», including through electronic documents through information system operators, also using electronic signatures, constant growth the number of requirements for a unified identification and authentication system, information system operators, hosting providers,

site owners with the need to provide, process and disseminate personal data of individuals (subjects of personal data), as well as an increase in the number of fraud methods and their constant transformation, raise the question of how to improve countermeasures offenses committed using information technology. Thus, the issue of ensuring the security of the information sphere and information security of the Russian Federation is becoming more and more urgent, and the improvement of the directions of countering offenses and protecting the rights of users and subjects of personal data in this area is essential.

Keywords: Offenses, information technology, information and telecommunication network Internet, electronic document, electronic signature, operators of information systems, user, subject of personal data.

В соответствии с п. 2 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». (далее – 149-ФЗ РФ) информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. В соответствии со ст. 3 149-ФЗ установлены принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации, в частности о недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия, также ст. 2 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее 152-ФЗ) установлено обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

Основные направления противодействия правонарушениям, совершаемых с использованием информационных технологий, должны быть направлены на защиту сбора, хранения, обработки, использование информации (предоставления) и распространения информации, что подтверждается принципами и нормами изложенными в Конституции РФ. В соответствии со ст. 23 и ст. 24 Конституции РФ каждый имеет право на неприкосновенность частной жизни; сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются, а также государственной защитой указанных прав в соответствии со ст. 45 Конституции РФ.

В соответствии с п. 1 Указа Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» (Далее – Доктрина информационной

безопасности РФ) под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений и пп. 2 п. 8 Доктрины информационной безопасности РФ национальными интересами в информационной сфере являются, в частности, обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации.

Направления совершенствования противодействия правонарушениям, совершаемых с использованием информационных технологий должны концентрироваться на субъектах сбора, хранения, обработки, использование (предоставления) и распространения информации, которыми, как правило, являются единая система идентификации и аутентификации, операторы информационных системы, провайдеры хостинга, операторы связи, владельцы сайтов, на выявлении правонарушений действий их сотрудников, имеющих доступ к информации и действиями с ней.

В соответствии с пп. «г», «д», «е» п. 2 Доктрины информационной безопасности РФ должностные лица государственных органов (силы обеспечения информационной безопасности) должны обеспечивать информационную безопасность правовыми, организационными, техническими и другими средствами (средства обеспечения информационной безопасности), аналогия указанных норм также изложены в п. 1 и п. 2 ч. 1 ст. 16 149-ФЗ РФ, что защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа.

Тем не менее, в настоящее время при получении информации, лицами, не имеющим права на доступ к ней, в частности о субъекте персональных данных и совершения с помощью данной информации неправомерных (мошеннических) действий, с целью хищения

недвижимых и движимых вещей – денежных средств с банковских счетов физических лиц с помощью технических и информационных систем, сайтов в информационно-телекоммуникационной сети Интернет кредитными организациями, как правило, потерпевшей стороне не возвращаются похищенные средства, если потерпевший сам сообщил или предоставил информацию о своих персональных данных (вкладах, счетах, пин-кодов и т.д.). Указанные действия кредитных организаций не правомерны и нарушают права своих клиентов (субъекте персональных данных, потерпевших), так как в соответствии с нормами гл. 8 ГК РФ клиент кредитной организации (потерпевшая сторона) не заключала договор с лицом, не имеющим права на доступ к информации о нем, то есть в отсутствие волеизъявления одной из сторон договор не может считаться сделкой, и, следовательно, не заключен¹. Кроме того, как правило, клиент банка (потерпевшая сторона) введен в заблуждение и считает, что предоставляет информацию о себе добросовестной стороне (кредитной организации) именно на основании того, что к его персональным данным уже, частично, предоставлен несанкционированный доступ и (или) данные переданы лицам (недобросовестной стороне), не имеющим права на доступ к ним.

Можно сделать вывод, что осуществление мер, направленных на совершенствование противодействия правонарушениям, совершаемых с использованием информационных технологий, должны обеспечиваться государственными органами РФ и субъектами, ответственными за сбор, хранение, обработку, использование (предоставление) и распространение информации, а также, нести ответственность за неблагоприятные последствия нарушения порядка доступа к информации (несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации). В частности, кредитными организациями должны быть обеспечены такие механизмы безопасности операций по счетам клиентов, что даже в случае получения несанкционированного доступа к информации их клиентов должна обеспечиваться сохранность денежных средств и транзакций по счетам клиентов (недопустимость хищения денежных средств клиентов).

¹ Хейло А.В., Юзефович Ж.Ю. Правовая квалификация сделок, подписанных неустановленным лицом // Научный аспект. 2019. Т. 3. № 2. С. 379–386.

Расул Ахматович ТЕКЕЕВ

аспирант

Саратовская государственная юридическая академия;

главный специалист отдела прокуратуры

Карачаево-Черкесской Республики

СОСТОЯНИЕ ПРЕСТУПНОСТИ, СВЯЗАННОЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В статье рассмотрены статистические показатели преступности, связанной с использованием информационно-телекоммуникационных технологий или компьютерной информации. Проанализированы данные, в том числе в динамическом аспекте, с приведением сведений о зарегистрированных преступлениях данной категории, их уровня раскрываемости, степени участия правоохранительных органов, а также с указанием числа отдельных процессуальных решений в рамках уголовно-процессуального закона. Рассмотрены структурные элементы киберпреступности, удельный вес в ней некоторых корыстных преступлений против собственности, преступлений в сфере незаконного оборота наркотиков и других.

Ключевые слова: преступления, связанные с использованием информационных технологий; состояние преступности; компьютерная информация; киберпреступность; сеть Интернет.

Rasul Akhmatovich TEKEEV

postgraduate student

Saratov State Law Academy,

chief specialist of the Prosecutor's office

of the Karachay-Cherkess Republic

STATE OF CRIME RELATED TO THE USE OF INFORMATION TECHNOLOGIES

Abstract. The article deals with statistical indicators of crime related to the use of information and telecommunications technologies or computer information. Analyzed data, including in the dynamic aspect, with information about registered crimes of this category, their level of detection, the degree of participation of law enforcement agencies, as well as indicating the number of individual procedural decisions under the criminal procedure law. The structural elements of «cybercrime» are considered, as well as the specific weight of some self-serving crimes against property, crimes in the field of drug trafficking, and others.

Keywords: crimes related to the use of information technologies; state of crime; computer information; cybercrime; Internet network.

Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования

функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы¹.

В числе таковых внутренних угроз в последние годы обозначена проблема преступности в различных сферах общественных отношений, связанной с использованием информационных технологий. Особую актуальность представляет борьба с такими противоправными проявлениями в обозначенной области, как:

- преступления, связанные с хищением чужого имущества с использованием информационно-телекоммуникационных услуг в широком смысле;
- преступления в сфере незаконного оборота наркотиков через сеть Интернет, в том числе так называемые преступные «закладки» наркотических средств и психотропных веществ;
- спам, производство и рассылка вредоносных программ и различных вирусов, в том числе атака на критически значимые ресурсы государственного уровня;
- «утечка» персональных данных граждан, раскрытие конфиденциальной информации;
- преступные схемы легализации (отмывания) криминальных денежных средств и имущества;
- противоправная деятельность в сети Интернет в отношении несовершеннолетних, включая преступления против половой свободы и половой неприкосновенности последних и др.

Противодействие преступным проявлениям в информационном пространстве, выявление причин и условий их совершения, совершенствование методики расследования данных преступлений, а также повышение эффективности прокурорского надзора предполагает анализ и изучение состояния преступности в этой сфере и обеспечение ее достоверности.

Содержание данного признака характеризует распространенность преступности и определяется общим количеством со-

¹ П. 10 Доктрины информационной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // Официальный интернет портал правовой информации. URL: <http://www.pravo.gov.ru> (дата обращения: 06.12.2016).

вершенных преступлений, а также числом лиц, их совершивших, на определенной территории за конкретный период времени².

Во исполнение мероприятий, предусмотренных протоколом оперативного совещания Совета Безопасности РФ, о повышении эффективности борьбы с преступлениями в сфере компьютерной информации (утв. Президентом РФ 26 апреля 2017 г. № Пр-805), форма федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений», начиная с 2018 г. дополнена разд. 11 «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выявленных и предварительно расследованных субъектами регистрации»³.

За период с 2018 г. по сентябрь 2020 г. на территории РФ зарегистрировано 832 118 преступлений, совершенных с использованием информационно-телекоммуникационных технологий⁴, из которых доля тяжких и особо тяжких – 46,2 %, что также свидетельствует о характере и степени общественной опасности. Причем, на протяжении указанного периода наблюдается положительная динамика, прирост данных преступлений в 2019 г. составил 68,5 %, а в 2020 г. – 23,3 % соответственно.

На деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, приходится одно из четырех регистрируемых в текущем году преступлений (363 тыс.). Ранее отмечавшиеся практически двукратные темпы их увеличения несколько замедлились и по итогам 9 месяцев составляют 77 %. Как и прежде, больше половины всех

² Криминология и предупреждение преступлений: учебник / под общ. ред. В.И. Гладких. М., 2019 // СПС «Гарант». URL: <http://www.garant.ru/> (дата обращения: 23.09.2020).

³ *Гурин А.Д.* Обеспечение достоверности официальных статистических данных о преступлениях в сфере информационных технологий // Законность. 2020. № 2.

⁴ Здесь и далее использованы данные раздела 11 формы федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» // Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: <http://crimestat.ru/analytics> (дата обращения: 10.11.2020).

киберпреступлений совершается с использованием сети Интернет (209,7 тыс.), свыше 42 % – при помощи средств мобильной связи (155,2 тыс.)⁵.

Традиционно лидером по выявлению преступлений в информационной сфере являются органы внутренних дел, которые за анализируемый период выявили 818 732 преступления (это около 98 % всех зарегистрированных). Вместе с тем в выявлении данных преступных актов принимают участие и органы ФСБ России, следственные органы СК РФ, органы прокуратуры, ФСИН России и др.

Закрепление на уровне Стратегии национальной безопасности РФ (утв. Указом Президента РФ от 31 декабря 2015 г. № 683) факта появления новых форм противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий (п. 22), обуславливают, в том числе повсеместное участие правоохранительных органов в пресечении указанных преступлений в пределах предоставленных полномочий.

О низкой раскрываемости преступлений, совершаемых с использованием информационных технологий, свидетельствуют соответствующие статистические данные.

С 2018 г. по сентябрь 2020 г. предварительно расследовано 178 246 преступлений, по отношению к общему числу зарегистрированных преступлений всего лишь пятая их часть (21 %). Порядка 87 % из их числа направлено в суд с обвинительным заключением, обвинительным актом, обвинительным постановлением, по 21 345 преступлениям уголовные дела были прекращены, либо вынесены постановления об отказе в возбуждении уголовного дела – это практически 12 % от числа расследованных. Правоохранительными органами было выявлено 115 753 лица, совершивших указанные преступления.

подавляющее большинство преступлений (85 %) предварительно расследованных, отнесено уголовно-процессуальным законом к подследственности органов внутренних дел, что соответствует и общей выявляемости, приведенной выше.

⁵ Состояние преступности в России за январь – сентябрь 2020 г. Генеральная прокуратура Российской Федерации, Главное управление правовой статистики и информационных технологий. М., 2020. С. 6. URL: https://genproc.gov.ru/upload/iblock/925/sbornik_9_2020.pdf (дата обращения: 23.09.2020).

За 9 месяцев 2020 г. раскрываемость киберпреступлений составила по России 23 %, в отдельных регионах наблюдается «высокая» относительно общероссийского показателя раскрываемость: Псковская область – 43,5 %, Карачаево-Черкесская Республика – 59 %, Республика Дагестан – 66,2 %, Республика Ингушетия – 47,8 %, Чеченская Республика – 58,9 %, Оренбургская область – 40,3 %, Республика Мордовия – 43,3 %, Чукотский автономный округ – 54,8 %⁶.

Для полноты картины относительно уровня раскрываемости необходимо привести данные о количестве принятых решений в рамках ч. 1 ст.208 УПК РФ о приостановлении предварительного следствия.

За период 2018 – сентябрь 2020 гг. по различным основаниям, предусмотренным уголовно-процессуальным законом по 559 454 преступлениям уголовные дела были приостановлены, что составляет 67 % от числа зарегистрированных. Значительная часть (99.2 %) уголовных дел приостановлены именно за неустановлением лица, подлежащего привлечению в качестве обвиняемого (п. 1 ч. 1 ст. 208 УПК РФ), что, безусловно, актуализирует очевидные проблемы эффективности борьбы с преступностью в сфере информационных технологий и требует принятия действенных мер в данной области.

Рассмотрим некоторые статистические показатели в структуре преступности, связанной с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

За неполные три года в анализируемой сфере совершено 255 874 тайных хищения чужого имущества (ст. 158 УК РФ), путем мошенничества, предусмотренного ст. 159 УК РФ, совершено 358 889 преступлений, 5838 вымогательств. На эти три состава преступлений против собственности приходится 74,5 % всей зарегистрированной преступности данной категории. Как отмечает МВД России, за 9 месяцев 2020 г. четыре таких преступления из пяти

⁶ Состояние преступности в России за январь – сентябрь 2020 г. Генеральная прокуратура Российской Федерации, Главное управление правовой статистики и информационных технологий. М., 2020. С. 59–62. URL: https://genproc.gov.ru/upload/iblock/925/sbornik_9_2020.pdf (дата обращения: 23.09.2020).

(81,5 %) совершаются путем кражи или мошенничества: 296 тыс. (+83,5 %) ⁷.

Несмотря на принятые законодателем и реализуемые правоохранительными органами меры, достаточно значительным остается число совершенных деяний, предусмотренных ст. 171² УК РФ (незаконные организация и проведение азартных игр), их зарегистрировано 2324 преступления.

В сфере незаконного оборота наркотиков совершено 73 755 преступлений с использованием информационных технологий, из них подавляющее большинство приходится на преступные деяния, предусмотренные ст. 228¹ УК РФ – около 99 %.

Всего в сфере компьютерной информации (глава 28 УК РФ) за 2018 г. – сентябрь 2020 г. совершено 8446 преступлений. При этом по относительно новому составу преступления, предусмотренного ст. 274¹ УК РФ (введена в действие с 1 января 2018 г. ⁸) – неправомерное воздействие на критическую информационную инфраструктуру РФ, за 9 месяцев 2020 г. зарегистрировано 18 случаев с выявлением 9 лиц их совершивших.

Приведенные в статье статистические показатели подтверждают актуальность проблемы борьбы с преступностью, связанной с использованием информационных технологий, указывают на значительный характер их числа в общей статистике преступности и потенциальную угрозу дальнейшего роста. Перечисленные факторы вкпе со складывающейся устойчивой негативной динамикой низкой раскрываемости данных преступных актов требуют активизации правоохранительных органов и принятии дополнительных мер по их предупреждению.

⁷ Состояние преступности в России за январь-сентябрь 2020 г. МВД России. ФКУ «Главный информационно-аналитический центр». М., 2020. С. 3. URL https://xn--b1aew.xn--p1ai/upload/site1/document_journal/11-2020.pdf (дата обращения: 23.09.2022).

⁸ Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации”» // Официальный интернет портал правовой информации. URL: <http://www.pravo.gov.ru> (дата обращения: 26.07.2017).

София Сергеевна ЧЕПЕЦ

студент

Московский государственный юридический университет

им. О.Е. Кутафина

СИСТЕМА РАСПОЗНАВАНИЯ ЛИЦ В РОССИИ: ЭФФЕКТИВНАЯ ПОМОЩЬ В ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ ИЛИ НАРУШЕНИЕ ПРАВ И СВОБОД ЧЕЛОВЕКА?

Аннотация. Система распознавания лиц обладает диалектическим единством. С одной стороны, она способна оказать помощь в противодействии преступности, с другой – может стать инструментом нарушения конституционных прав и свобод человека. Автором приводятся примеры и точки зрения, отражающие справедливость обоих аспектов. В качестве вывода обоснованы возможные пути примирения этих крайних позиций и легального применения данной технологии в России.

Ключевые слова: система распознавания лиц, технологии, борьба с преступностью, права и свободы, камеры видеонаблюдения.

Sofia Sergeevna CHERETS

student

Kutafin Moscow State Law University

THE SYSTEM OF FACE RECOGNITION IN RUSSIA: EFFECTIVE ASSISTANCE IN COMBATING CRIME OR VIOLATION OF HUMAN RIGHTS AND FREEDOMS?

Abstract. The article examines the widely used system of face recognition in two aspects: as an assistance in the fight against crime and as a violation of constitutional human rights and freedoms. There are various examples, points of view, which reflect the fairness of both aspects. In the conclusion the author proposes and argues possible ways of finding a compromise and legal application of this technology in Russia.

Keywords: face recognition system, technology, crime fighting, rights and freedoms, closed circuit television.

На данный момент цифровые технологии внедрились практически во все сферы человеческой жизни. Этот феномен XXI в. далеко не всегда можно рассматривать как положительный. Как отметил В.С. Овчинский, «...интернет и приватность – понятия несовместимые. Причем, если раньше человек, лишившись приватности в духовном пространстве, хотя бы теоретически мог сохранять ее

в физическом, то с переходом общества в цифровую реальность интернета всего, приватности не осталось нигде»¹.

Не так давно создана в разных уголках мира система распознавания лиц – программа определения образов, задача которой состоит в автоматическом выделении лица на изображении и его идентификации путем сопоставления и анализа биометрических данных. Лицо любого человека имеет уникальное строение, и задачей данной системы является нахождение его на фотографии или в видеопотоке, сравнение с загруженной биометрической базой и идентификация на ее основе человека.

Появление гаджетов и умных систем значительно расширило возможности противодействия преступности. В начале 2020 г. в десятке городов нашей страны в пилотном режиме запустили систему распознавания лиц. В Москве камеры с данной функцией работают с 2017 г.: «тест доказал эффективность системы, и с января 2020 г. к модулю распознавания лиц были подключены уже 105 тысяч потоков с камер. Только за январские праздники система помогла задержать 34 чел., находившихся в федеральном розыске»².

Представители метрополитена отмечают, что благодаря данной функции число правонарушений в московском метро сократилось вдвое за последние 2,5 года, а мэр Москвы спрогнозировал, что лица, находящиеся в розыске, будут распознаваться за доли секунды³. Применительно к другим субъектам РФ можно сказать, что не все готовы выделять средства на внедрение подобных технологий, поскольку имеются более серьезные проблемы, требующие финансов для их решения⁴.

Система распознавания лиц в зарубежных странах доказывает эффективность. Например, в 2015 г. китайские власти запустили проект по созданию национальной базы данных на основе системы распознавания лиц. Система наблюдения в Китае самая большая

¹ Овчинский В.С. Криминология цифрового мира. М., 2018. С. 122.

² URL: <https://www.kommersant.ru/doc/4503379>. Коммерсантъ.2020. 25 сентября. (дата обращения: 27.10.2020).

³ URL: <https://www.interfax.ru/moscow/692390> (дата обращения: 27.10.2020).

⁴ URL: <https://www.gazeta.ru/social/2020/09/25/13268293.shtml> (дата обращения: 28.10.2020).

в мире и насчитывает более 200 млн. камер. Это привело к тому, что правоохранительным органам потребовалось всего 7 минут, чтобы отследить местонахождение журналиста ВВС в столице Китая – Пекине, с населением больше 21 млн чел. В настоящее время там же для полицейских разрабатываются смарт-очки с системой распознавания лиц, которые оборудованы камерой и связаны с базой данных правоохранительных органов. На поиск лица в базе потребуется 2–3 минуты, а в случае нахождения сотрудники получают информацию о человеке и его домашний адрес. Первые тестирования проходят в г. Чжэнчжоу.

В 2016 г. распознавание лиц начали тестировать в Лондоне. В сентябре 2017 г. с помощью данной технологии был обнаружен и арестован Х., организовавший взрыв на станции метро «Парсонс-грин». В США в 2018 г. данная технология за несколько месяцев работы помогла предотвратить въезд в страну 26 подозреваемых в совершении преступлений. Национальным центром по делам пропавших без вести и эксплуатируемых детей в Нью-Дели в Индии с помощью системы распознавания лиц всего за четыре дня было обнаружено и идентифицировано около трех тысяч детей, пропавших без вести⁵.

Приведенные примеры свидетельствуют о высокой значимости этой технологии, однако возникает определенное противоречие со ст. 23 Конституции РФ, которая гласит, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Обострение противоречия между конфиденциальностью и цифровизацией обуславливается стремительным развитием технологий отслеживания и анализа данных, а также огромным объемом доступных данных о пользователях в специальных базах.

Развитие технических средств противодействия преступности в современном мире может граничить с нарушением прав человека. С одной стороны, технологии расширяют пространство свободы, с другой – делают человека подконтрольным. Данные, получае-

⁵ URL: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html>_(дата обращения: 04.11.2020).

мые с камер, регулярно объединяются с определенными личными данными и могут быть использованы третьими лицами в разных целях, и эта проблема в настоящее время не рассматривается законодательством большинства стран. Демонстрирует это ситуация, когда через «Даркнет» девушка смогла заказать подробный отчет о всех своих перемещениях за месяц, собранный на основе системы распознавания лиц. Даркнет – это скрытая сеть, файлообмен в которой происходит анонимно (поскольку IP-адреса недоступны публично), и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства. Именно поэтому его могут использовать (и используют) как инструмент для осуществления коммуникации в подпольях и незаконной деятельности⁶. В 2015 г. анонимный пользователь сайта благодаря уязвимости системы получил доступ к трансляциям 20 тыс. камер г. Москвы.

Несмотря на то, что в Департаменте информационных технологий Правительства г. Москвы утверждают, что записи с камер городской системы видеонаблюдения представляют собой исключительно изображения и не содержат персональных данных граждан, тот факт, что девушка смогла получить данные такого рода, свидетельствует о наличии уязвимостей.

Получаются распространения факты злоупотребления доступом к таким персональным данным: бывший сотрудник отдела технической защиты информации создал свою собственную программно-информационную систему, содержащую адреса, паспорта и прочую персональную информацию, и так как он имел доступ к базе данных, куда вносятся сведения из учреждений, продавал эти сведения третьим лицам – за нарушение неприкосновенности частной жизни суд назначил виновному наказание в виде штрафа.

Опасения тотального вторжения и контроля со стороны государства порождают запреты использования системы распознавания лиц: недавно власти г. Сан-Франциско запретили дальнейшее использование технологии распознавания лиц правоохранительными органами, а американский союз гражданских свобод, в доказательство уязвимости и неточности системы провел эксперимент, в ходе

⁶ *Jessica A. Wood. The Darknet: A Digital Copyright Revolution // Richmond Journal of Law & Technology. 2010. Vol. 16. Iss. 4.*

которого 28 конгрессменов США были приняты системой за преступников. Американцы настаивают на том, что правоохранительным органам необходимо сначала получить согласие на использование такой технологии⁷.

Еще не так давно информация, которая была получена из публичных мест, не считалась сведениями о частной жизни отдельного гражданина в силу негласного принципа, в основе которого мысль о том, что частная жизнь на частной территории, а в публичных местах частной жизни не может быть по определению. Вероятно, данный принцип отделения частной жизни от публичной имел место только до появления систем распознавания и отслеживания.

В настоящее время подготовлен законопроект о внесении изменений в ч. 1 ст. 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в соответствии с которым биометрическими персональными данными будут признаваться сведения, характеризующие физиологические, биологические и генетические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных. Исключения предусмотрены для случаев, возникающих в связи с реализацией международных договоров РФ, с осуществлением правосудия и исполнением судебных актов, с проведением обязательной государственной дактилоскопической регистрации, обязательной государственной геномной регистрации и в соответствии со специальным законодательством РФ⁸. Таким образом, будет расширяться поле уголовно-правовой охраны защиты персональных данных.

Некоторые юристы считают, что само видеоизображение человека не является биометрическими персональными данными, пока оно не переведено в математический код и не сравнивается с другими кодами из базы шаблонов⁹. В законе от 27 июля 2006 г. № 152-ФЗ

⁷ URL: <https://www.vedomosti.ru/technology/articles/2019/08/02/807944-tehnologiyu-raspoznavaniya-lits> (дата обращения: 04.11.2020).

⁸ Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 24 апреля 2020 г.) «О персональных данных» (с изм. и доп., вступ. в силу с 29 декабря 2020 г.) // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/> (дата обращения: 23.10.2020).

«О персональных данных» перечислены случаи, когда можно использовать биометрические данные человека без его согласия. Под данные исключения не подпадает информация, собираемая Департаментом информационных технологий Правительства г. Москвы и аккумулируемая в Едином центре хранения данных. Роскомнадзор разъяснил, что необходимо принимать во внимание цель, которую преследует оператор при осуществлении действий, связанных с обработкой персональных данных; в случае, если они используются оператором для установления личности субъекта персональных данных, то данная обработка должна осуществляться в строгом соответствии со ст. 11 Федерального закона «О персональных данных»¹⁰.

Можно прийти к выводу, что правомерность использования данной технологии должна оцениваться в каждом случае с учетом конкретных обстоятельств. Большинство организаций, осуществляющих сбор и обработку биометрических персональных данных и выступающих операторами в РФ, соблюдая законность, крайне редко предоставляют открытый доступ к внутренней политике работы с персональными данными. Большинство из них относят к персональным данным клиентов только сведения об имени, контактные данные и информацию о месте жительства, но видеонаблюдение позволяет при необходимости мгновенно найти информацию о дате, времени, направлении движения интересующего человека, видеокadres с изображением его лица, а особые функции могут помочь отследить дальнейший маршрут следования лица после момента обнаружения.

Таким образом, система распознавания лиц в состоянии оказать огромную помощь в противодействии преступности, поимке лиц, находящихся в розыске, нахождении пропавших без вести, однако следует учесть, что наряду с пользой, она сопряжена с большими рисками. Существование таких систем, которые скрыты от глаз человека, – это нарушение гражданских свобод, потому что люди

⁹ URL: <https://www.vedomosti.ru/technology/articles/2019/11/26/817135-vlasti-sledit> (дата обращения: 28.10.2020).

¹⁰ Разъяснения Роскомнадзора «О вопросах отнесения фото- и видео-изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/> (дата обращения: 23.10.2020).

ведут себя иначе, если подозревают, что за ними наблюдают. Если человек знает об этом, он дважды подумает, прежде чем решится на преступление.

Полагаем, что в России необходимы четкие рамки использования такой технологии, устанавливающие право на ее применение не повсеместно, и только специальными подразделениями и службами, либо же их исключительное право доступа к таким данным в случаях необходимости (например, отслеживания преступников). Зарубежными специалистами отмечается, что нужно принимать законы, касающиеся распознавания лиц, где следует определить, кто с кем делится какой информацией и кто принимает такие решения¹¹.

Необходимо законодательно установить запрет на передачу данных неуполномоченным на их обработку третьим лицам и создать усложненный доступ к этим данным. В качестве примера можно привести законы о биометрических данных в штатах Иллинойс и Техас, которые устанавливают, что субъекты, собирающие и использующие эти данные, должны выполнять ряд базовых информационных практик и протоколов конфиденциальности, получать информированное согласие на сбор биометрических данных, обеспечивать обязательную защиту и ограничение на срок хранения, запрет на их использование с целью получения прибыли, ограничение прав передачи третьим лицам и частные основания для подачи иска в случае нарушения этих норм.

В конечном счете, потребуется также уточнение объема общественных отношений, подлежащих уголовно-правовой охране. Потребуется разъяснения Пленума Верховного Суда РФ о практике применения ст. 137 («Нарушение неприкосновенности частной жизни») УК РФ в части понимания частной жизни и сбора сведений путем использования таких систем, определения ответственных лиц.

Технология распознавания лиц открывает безграничные возможности отслеживать информацию о личности и перемещениях человека, практически мгновенно сохранять, распространять и анализировать ее. Развитие этой технологии в будущем может привести к тому, что конфиденциальность частной информации

¹¹ URL: <https://www.vedomosti.ru/technology/articles/2019/08/02/807944-tehnologiyu-raspoznavaniya-lits> (дата обращения: 05.11.2020).

человека будет нарушаться. Благополучие человечества возможно лишь в том случае, если будет законодательное достойное регулирование технологии распознавания лиц, прежде чем эти системы слишком прочно войдут в повседневную жизнь. Иначе людям будет знаком мир, в котором при каждом появлении в общественном месте их будут автоматически идентифицировать, заносить информацию в профиль и, возможно, использовать ее без их ведома.

Дмитрий Анатольевич ЧЕРНОУСОВ

аспирант

Московский финансово-юридический университет МФЮА

ПРЕСТУПЛЕНИЯ И ПРАВОНАРУШЕНИЯ ПРОТИВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В СЕТИ ИНТЕРНЕТ И ФАКТОРЫ, СПОСОБСТВУЮЩИЕ ИМ

Аннотация. В статье рассмотрены преступления и правонарушения против интеллектуальной собственности в сети Интернет и факторы, способствующие совершению таковых. Приведена статистика преступлений с использованием информационно-коммуникационных технологий, судебная практика и произведено обобщение актуальных проблем, которые дают возможность роста незаконного использования информационно-телекоммуникационных технологий для незаконных действий.

Ключевые слова: интеллектуальная собственность, информационная безопасность, право, преступления, авторское право.

Dmitry Anatol'evich CHERNOUSOV

postgraduate student

Moscow University of Finance and Law MFUA

CRIMES AND OFFENSES AGAINST INTELLECTUAL PROPERTY ON THE INTERNET AND PROMOTING FACTORS

Abstract. This article examines the crimes and offenses against intellectual property on the Internet and the factors contributing to their commission. The statistics of crimes with the use of information and communication technologies, judicial practice are presented, and a generalization of urgent problems that make it possible to increase the illegal use of information and telecommunication technologies for illegal actions is made.

Keywords: intellectual property, information security, law, crimes, copyright.

С момента появления сети Интернет в широком доступе, она стала не только средством общения для большого количества людей, но и местом, где размещается огромное количество материалов, так или иначе являющихся объектами интеллектуального права. Начиная с сайтов, которые представляют собой, порой сложные по структуре и программному коду Интернет-страницы, и заканчивая простыми вещами вроде фотографий в блогах. С каждым днем количество информации, передающейся по сети Интернет, хранящейся в нем,

и использующей его, увеличивается. Если в 1993 г. Интернет передавал около 1 % информации, то к 2000 г. цифра выросла до 51 %, и в 2007 г. стала более 97 %¹. Касаясь субъектов интеллектуального права, например, Интернет-сайтов, статистика выглядит следующим образом: 1994 г. – 2,7 тыс. сайтов, 2001 г. – 29,2 млн сайтов, 2006 г. 85,5 млн, к настоящему времени чуть более 1,7 млрд².

При таком объеме передаваемой информации, размещаемых в сети Интернет объектах интеллектуального права остро стоит вопрос о том, как защитить информацию и интеллектуальную собственность передаваемую и размещаемую в сети Интернет, от покушений преступников и третьих лиц.

В связи с тем, что на текущий момент преступления и правонарушения с использованием информационных технологий представляют собой огромный их пласт, с которым государство и общество вынуждено бороться каждый день. Так, например, согласно статистике, опубликованной Генеральной прокуратурой РФ за 2019 г., в структуре преступности, наиболее вероятные и возможные преступления с использованием информационных технологий это: кражи – 38,2 %, мошенничества – 12,7 %, соответственно, общая доля данных типов преступлений представляет собой 50,9 %. При этом удельный вес отдельных видов преступлений от общего числа всех зарегистрированных видов преступлений, для преступлений, совершенных с использованием информационно-телекоммуникационных технологий составляет 14,5 %³. Те же показатели за период январь – сентябрь 2020 г. составляют кражи – 37,4 %, мошенничества – 16,1 %, соответственно, общая доля данных типов преступлений представляет собой 53,5 %, а удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, от общего числа

¹ Hilbert M., López P. The World's Technological Capacity to Store, Communicate, and Compute Information // Science. 2011. Vol. 332. № 6025. P. 60–65. URL: <http://www.martinhilbert.net/WorldInfoCapacity.html> (дата обращения: 09.11.2020).

² Как росло количество веб-сайтов в мире // Коммерсантъ. 2019. 2 ноября. URL: <https://www.kommersant.ru/doc/4147760> (дата обращения: 09.11.2020).

³ Состояние преступности в России за январь – декабрь 2019 г. Генеральная прокуратура РФ. Москва. С. 22–23. URL: https://genproc.gov.ru/upload/iblock/034/sbornik_12_2019.pdf (дата обращения: 23.09.2020).

преступлений 23,6 %⁴ и является самым большим показателем среди иных выделяемых видов преступлений. При этом наблюдается динамика роста данного типа преступлений.

Несмотря на то что, как объект интеллектуальной собственности, авторское право, например, получило признание совсем недавно, вопрос был поставлен даже в разрезе защиты данных прав на международном уровне, правда по историческим меркам недавно, о чем приняты соответствующие международные программы сотрудничества, соглашения конвенции⁵. Но молодость данного вида объекта права не отменяет его значимости для государства и граждан.

Среди правонарушений часто можно встретить нарушение авторских прав на произведение, установленных ст. 1255 ГК РФ: исключительное право на произведение; право авторства; право автора на имя; право на неприкосновенность произведения; право на обнародование произведения.

Московский городской суд рассматривает в качестве суда первой инстанции гражданские дела, которые связаны с защитой авторских и (или) смежных прав, кроме прав на фотографические произведения и произведения, полученные способами, аналогичными фотографии, в информационно-телекоммуникационных сетях, в том числе в сети Интернет, и по которым им приняты предварительные обеспечительные меры в соответствии со ст. 144¹ кодекса, в соответствии с положениями ч. 3 ст. 26 ГПК РФ.

Однако согласно данным статистики из рассмотренных Московским городским судом дел о защите авторских прав из рассмотренных в целом судами общей юрисдикции и мировыми судами по первой инстанции дел по гражданскому судопроизводству – 19,6 млн, на защиту авторских прав приходится ничтожно малое количество – 1008 дел, то есть 0,005 %⁶. Что говорит об отсутствии

⁴ Состояние преступности в России за январь-сентябрь 2020 г. Генеральная прокуратура РФ. Москва. С. 12, 39. URL: https://genproc.gov.ru/upload/iblock/925/sbornik_9_2020.pdf (дата обращения: 23.09.2020).

⁵ Юзефович Ж.Ю. Международно-правовая охрана авторских прав // Вестник Московского университета МВД России. 2014. № 6. С. 107–110.

⁶ Обзор судебной статистики о деятельности федеральных судов общей юрисдикции и мировых судей в 2019 год. Судебный департамент при Верховном Суде Российской Федерации. М., 2020. С. 51, 54. URL: https://cdep.sudrf.ru/userimages/sudebnaya_statistika/2020/Obzor_sudebnoy_statistiki_o_deyatelnosti_federalnih_sudov_obshechey_yurisdiksi_i_mirovih_sudey_v_2019_godu.pdf (дата обращения: 23.09.2020).

правовой грамотности в области защиты интеллектуальных прав и в частности авторского права, равно как и культуры защиты и использования авторских прав на, как видится, желаемом и требуемом уровне.

Данному факту способствует правовой нигилизм, распространяемый в сети Интернет, после ухудшения ситуации и роста социальной значимости его в 2000-е годы. И перерождающийся в социальную проблему среди населения как России, так и других стран, поскольку сеть Интернет явление трансграничное, за счет, так называемых, непрофессиональных Интернет-коммуникаторов (лиц позиционирующих себя как «простые люди из народа»)⁷.

Следующими факторами можно считать отсутствие информационно-коммуникационной грамотности в области безопасности информации и коммуникации, а также широкое распространение и доступность информационно-телекоммуникационных технологий обширному кругу лиц вне зависимости от возраста, уровня образования и социального статуса.

Данные факторы имеют граничные группы риска. Так, например, дети в возрасте от 5 до 11 лет обладая доступом в интернет, личными мобильными устройствами со средствами связи, не обладают обычно необходимым «багажом» знаний в области информационной безопасности. И входят в группу риска для таких преступлений как мошенничество и кража.

Другая группа риска состоит из людей в возрасте от 55 лет и старше, ввиду отсутствия у них в «активный» период жизни опыта применения информационно-телекоммуникационных технологий, широко используемых в настоящее время. Например, онлайн банкинг.

Широкое распространение мобильных устройств с доступом в сеть интернет, а также широкое использование их для доступа в сеть представляет собой само по себе огромное количество рисков, которые перекликаются с нижеуказанными факторами.

Несовершенство программного обеспечения, ввиду написания программ человеком, которая предполагает возможность ошибок и яв-

⁷ Карнаушенко Л.В. Правовой нигилизм непрофессиональных интернет-коммуникаторов как социальная проблема современной России // Вестник Краснодарского университета МВД России. 2016. № 4 (34). С. 102–105.

ляется следующим существенным фактором влияющим на возможность совершения преступлений или правонарушений. Количество ошибок в программном обеспечении даже крупных софтверных компаний, таких как Apple, Microsoft по отчетам компаний специализирующихся на информационной безопасности, выходит за все разумные пределы. Microsoft выпускает обновления безопасности минимум раз в месяц, «закрывая» ранее найденные и ставшие известными критические ошибки. Apple также не отстает от своего конкурента.

В мире проводятся конкурсы по информационной безопасности, в рамках которых специалистам предлагается, используя собственные разработки «взламывать» устройства, получать к ним удаленный доступ и полностью перехватывать управление ими. Результаты конкурсов неутешительные. 8 ноября 2020 года в Китае завершились ежегодные соревнования «этичных хакеров» - специалистов в области информационной безопасности – Tianfu Cup, в ходе которого исследователи в течение трех попыток по пять минут «взламывали» устройство или программное обеспечение. При этом, они применяли только авторские эксплойты. В результате специалистам по информационной безопасности удалось «взломать» последнюю версию iOS 14 на iPhone11 Pro, Samsung Galaxy S20, Window 10 v2004, Ubuntu, Chrome и другое программное обеспечение и устройство⁸.

Аппаратные ошибки, ошибки в построении систем и оборудования так же являются существенным фактором при совершении правонарушений и преступлений. Как пример можно рассмотреть IP-камеры с предустановленным, неизменяемым логином и паролем, который может быть как подобран методом перебора, так и быть одинаковым по умолчанию у всех одинаковых моделей камер. Этот фактор способствует неправомерному доступу к тайне личной жизни и соответственно преступлениям и правонарушениям связанным с этой возможностью.

Малый размер компенсации за нарушение прав как фактор увеличивающий возможность преступлений и правонарушений, например права на интеллектуальную собственность, в разрезе имеющейся судебной практики, так же имеет место быть. При этом

⁸ URL: https://t.me/true_secator/1128 (дата обращения: 10.11.2020).

принудительная форма реализации ответственности возникает в том случае когда поведение лица исключает добровольность⁹.

В соответствии с положениями ст. 1301 ГК РФ предусматривает три возможных варианта расчета компенсации:

- в размере от 10 000 до 5 000 000 руб., определяемом по усмотрению суда, исходя из характера нарушения;
- в двукратном размере стоимости контрафактных экземпляров произведения;
- в двукратном размере стоимости права использования произведения, определяемой исходя из цены, которая при сравнимых обстоятельствах обычно взимается за правомерное использование произведения тем способом, который использовал нарушитель.

Суды исходят из целого комплекса факторов при назначении компенсации за нарушенное право. И ожидать, согласно данным статистики, компенсацию в размере заявленных исковых требований возможно лишь в 25 % случаев. Также судебная практика устанавливает, что компенсация за нарушенное право не имеет собой целью штрафа нарушителя и полного возмещения вреда, причиненного нарушением права¹⁰.

В связи с увеличением числа преступлений и правонарушений с использованием информационно-телекоммуникационных технологий, развитием сети Интернет и упрощением доступа к современным технологиям требуется повышенное внимание со стороны как государства и всех его ветвей власти, так и самого социума для уменьшения влияния каждого из факторов на рост количества преступлений и правонарушений с использованием информационно-коммуникационных технологий. Для чего необходима выработка политики, направленной на предотвращение возможностей совершения преступлений и правонарушений с использованием информационно-коммуникационных технологий, повышение грамотности всех слоев населения в области информационной безопасности и профилактику соответствующего вида преступлений и правонарушений.

⁹ Юзефович Ж.Ю. Функции юридической ответственности и формы их реализации по российскому законодательству: автореф. дис. ... канд. юрид. наук. Москва. 2004. С. 23.

¹⁰ Радецкая М.В., Туркина А.Е. Обзор судебной практики по вопросу взыскания компенсации за нарушение исключительного права на результат интеллектуальной деятельности или средство индивидуализации // Журнал Суда по интеллектуальным правам. 2020. № 27. С. 5–40.

Антон Павлович ЧИСТОВ

аспирант

Московский финансово-юридический университет МФЮА

К ВОПРОСУ О СУДЕБНОЙ ПРАКТИКЕ ПО ДЕЯНИЯМ, СОВЕРШЕННЫМ С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНОЙ ПЛАТФОРМЫ ИНСТАГРАММ

Аннотация. В статье исследуются особенности судебной практики по гражданским спорам и уголовным делам, а так же административным правонарушениям, связанным с социальной платформой Инстаграм. Дополнительно проведена систематизация наиболее частых правонарушений законодательства РФ с использованием данной социальной сети.

Ключевые слова: судебная практика, инстаграм, киберпреступность, правонарушение, преступление.

Anton Pavlovich CHISTOV

postgraduate student

Moscow University of Finance and Law MFUA

ON THE ISSUE OF JUDICIAL PRACTICE ON ACTS COMMITTED USING THE SOCIAL PLATFORM INSTAGRAM

Abstract. The article examines the features of judicial practice in civil disputes and criminal cases, as well as administrative offenses related to the social platform Instagram. Additionally, the systematization of the most frequent violations of the legislation of the Russian Federation was carried out using this social network.

Keywords: judicial practice, instagram, cybercrime, offense, crime.

Социальные сети, а также повсеместное использование сети Интернет в обычной жизни прочно вошло в привычку у населения РФ. Кроме позитивной цифровизации многих аспектов жизни, вместе с развитием социальных сетей, большая часть классического криминального рынка ушло вслед за рядовыми гражданами в сеть. Таким образом, киберпреступность стала, по своему существу, обыденностью в жизни рядового пользователя сети Интернет.

Между тем, исследователи права указывают, что современные попытки борьбы с киберпреступностью в РФ, да и по существу, в международном формате, носят скорее превентивный и устраши-

тельный характер, нежели системный¹. Основная причина относительных неудач в борьбе с киберпреступностью – малое количество специалистов кибернетической безопасности, малое количество успешного опыта поиска, поимки и привлечения к уголовной ответственности лиц, занимающихся преступлениями в сфере компьютерных технологий.

Однако немаловажным фактором слабости правоохранительной системы РФ является так же крайне низкий уровень правосознания граждан РФ, сталкивающихся с киберпреступлениями чуть ли не ежедневно, а также отсутствие положительной практики по привлечению киберпреступников в РФ к уголовной ответственности². Автор настоящей публикации считает, что большую роль в становлении института защиты прав пользователей в сети Интернет должно сыграть неминуемое развитие понятия «ответственности» за противозаконные действия в сети Интернет³.

Между тем, в РФ на данный момент существует практика привлечения к уголовной ответственности лиц, совершивших преступление с использованием социальных сетей, мессенджеров и сеть Интернет в целом⁴. Не смотря на достаточно ограниченное количество уголовных дел, такая судебная практика сама по себе является достаточно важным началом для дальнейшего развития института киберзащиты граждан государства как от внешних воздействий (взлом или атака на персональные данные извне территории РФ), так и аналогичные действия, совершаемые на территории РФ.

В связи с изложенным автором предпринята попытка провести анализ судебной практики прямо связанной с социальной сетью Инстаграм, как одной из самой популярной в среде под-

¹ Пучков Д.В. К вопросу взаимосвязи кибернетических технологий и уголовного права // Социально-политические науки. 2017.

² Немов М.В. Киберпреступность как новая криминальная угроза // Эпоха науки. 2017. № 9. С. 53–59.

³ Юзефович Ж.Ю. Актуальные проблемы гражданского права и процесса свободные лицензии на объекты авторских прав в Российской Федерации // Вестник Московского университета МВД России. 2012. № 9. С. 63–65.

⁴ Зверьянская Л.Л. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений // Научно-методический электронный журнал «Концепт». 2016. № Т. 15. С. 881–885.

ростков среди всего мира⁵ и вместе с тем наиболее опасной для осуществления психологического воздействия на личность будущего потерпевшего⁶.

Актуальность осуществления такого вида исследования подтверждается тем, что на момент осуществления публикации настоящей работы еще ни один из современных исследователей права не выделял особенности судебной практики по спорам в конкретной социальной сети. А между тем, такая единоместная консолидация актуальной судебной практики позволит практикующим юристам определить особенности таких споров для дальнейшего избегания ошибок в судах.

Особенно пристального внимания заслуживают судебные споры в области совершения преступлений с использованием социальной сети инстаграм. Причем, как правило, преступники привлекаются либо по ст. 159 («Мошенничество»)⁷ УК РФ, 163 («Вымогательство») УК РФ⁸. Как уже отмечали специалисты кибербезопасности, предметом мошенничества является, как правило, либо доступ к данным из личных переписок, либо доступом к аккаунту в социальной сети.

Необходимо отметить, между тем, схожесть основополагающего действия, которое необходимо для окончания такого киберпреступления по существу: психологическое воздействие на потерпевшего.

Традиционный порядок действий преступника при совершении раскрываемых преступлений достаточно прост (*таблица 1*).

⁵ Заплетина С.Н., Заплетин В.В., Кийвери И.В., Соловьева М.А. Киберпреступность как угроза информационно-психологической безопасности личности подростка // Научная дискуссия: вопросы педагогики и психологии. 2017. № 4 (61). С. 61–68.

⁶ Кузнецова О.А., Баранова Д.В., Золотко М.А., Кузнецов А.В. Инстаграм как фактор жизненной деформации // Экономика и предпринимательство. 2020. № 1 (114). С. 974–977; Исмаилова К.Э. Способы эмоционального воздействия на интернет-пользователя (на материале аккаунта в сети инстаграм) // Актуальные проблемы лингвистики: взгляд молодых исследователей: сборник научных статей / под ред. Г.Р. Власян, М.А. Самковой. Челябинск, 2020. С. 49–53.

⁷ Приговор Северодвинского районного суда Архангельской области от 24 января 2020 г. по делу № 1-86/2020 1-878/2019. URL: <https://sudact.ru/regular/doc/wzVKP1Y2EfNH/> (дата обращения: 27.10.2020).

Таблица 1

Порядок действий преступника

<i>Взлом с целью шантажа (вымогательство)</i>	<i>Мошенничество</i>
1. Взлом аккаунта (получение доступа к информации), в том числе посредством кражи устройства, виртуального взлома, «подбора пароля»	1. Создание виртуального магазина посредством социальной сети инстаграм. 1.1. Загрузка подробной информации о товарах и услугах
2. Психологическое давление на потерпевшую	
3. Вымогательство с угрозой обнародование информации как широкому кругу лиц, так и конкретному лицу (супруг или супруга, иные близкие родственники)	3. Получение предоплаты за товар или услугу, которую преступник не собирался передавать или оказывать покупателю

В последнее время в судебной практике появились судебные разбирательства, связанные с использованием уникальных с точки зрения Российского законодательства методов и способов совершения киберпреступлений, однако с точки зрения киберпреступников, устаревших еще 7–10 лет назад⁹.

Между тем, споры о защите прав граждан в сети интернет в гражданском процессе так же не теряет своей актуальности.

Так, нередко судебные споры, связанные с нарушением авторских прав на уникальный контент¹⁰. Причем нарушение авторского права контента, ранее опубликованного в интернете, не обязательно должно быть осуществлено так же в социальной сети или мессенджере на большую аудиторию¹¹. В таких спорах, необходимо в пер-

⁸ Приговор Кировского районного суда г. Махачкалы от 11 декабря 2019 г. по делу № 1-697/2019. URL: <https://sudact.ru/regular/doc/iR5MYdpyYX1N/> (дата обращения: 27.10.2020).

⁹ Постановление Урванского районного суда Кабардино-Балканской республики от 25 декабря 2019 г. по делу № 1-305/2019. URL: <https://sudact.ru/regular/doc/6yEwVg6YyP1O/> (дата обращения: 27.10.2020).

¹⁰ Решение Волжского городского суда Республики Марий Эл № 2-1500/2019 от 17 января 2020 г. URL: <https://sudact.ru/regular/doc/dd1ZN653wUbH/> (дата обращения: 01.06.2020).

¹¹ Заочное решение Московского районного суда города Казани РТ по делу № 2-2363/2019 от 19 декабря 2019 г. URL: <https://sudact.ru/regular/doc/fD1EppmTmdxs/> (дата обращения: 03.06.2020).

вую очередь осуществить фиксацию правонарушения посредством услуг нотариуса в виде составления протокола осмотра интернет-страницы¹². Интересно отметить, что, в среднем, за такой услугой, как составление протокола осмотра интернет-страницы в России обращаются 20–25 тыс. человек в год¹³.

Преступления, преследуемые в соответствии с КоАП РФ, с использованием социальной сети инстаграм отличаются рядом специфических свойств. Автор настоящей работы выделяет сразу несколько основных направлений привлечения к административной ответственности (таблица 2).

Таблица 2

**Основные направления привлечения
к административной ответственности**

<i>Размещение запрещенного контента</i>	<i>Публикация заведомо ложного контента</i>	<i>Оскорбление</i>
1. Запрещенные в РФ организации, входящие в особый реестр ¹⁴ . 2. «Нацистская» (свастика и аналогичные символы) с целью пропаганды фашизма ¹⁵ .	Чаще всего, с участием представителей власти	Публичное («открытое») оскорбление с прямым указанием на личность пострадавшего лица

По завершению краткого обзора судебной практики по делам, связанным с социальной платформой инстаграм, необходимо отметить начавшийся адаптационный период принятия судебной системой информационных технологий во всех видах судопроизводства.

¹² Онлайн-доказательства для офлайн защиты: статистика и примеры нотариусов. Нотариат.рф. URL: <https://notariat.ru/ru-ru/news/onlajn-dokazatelstva-dlya-oflajn-zashity-statistika-i-primery-notariusov1> (дата обращения: 06.10.2020).

¹³ См.: там же.

¹⁴ Постановление Бабаюртского районного суда Республики Дагестан от 30 января 2020 г. по делу № 5-21/2020 от 30 января 2020 г. URL: <https://sudact.ru/regular/doc/602lbqqI8eWs/> (дата обращения: 02.10.2020).

¹⁵ Постановление Бийского городского суда Алтайского края от 17 января 2020 г. по делу № 5-35/2020. URL: <https://sudact.ru/regular/doc/eVnFB2ArR6Uw/> (дата обращения: 11.10.2020).

Таким образом, развитие судебной практики, связанной с конкретной социальной платформой (социальной сетью), сигнализирует ученым в области права о необходимости дальнейшего исследования в данном направлении.

Современные юристы участвуют в создании определенного вектора дальнейшего развития судебной практики не только в области уголовных споров (борьба с киберпреступностью), но и гражданско-правовых споров, прямо связанных с активным использованием социальной сети инстаграм.

Алина Николаевна ШАНИНА

студент

Институт права и национальной безопасности

Тамбовского государственного университета им. Г.Р. Державина

**ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ: АКТУАЛЬНЫЕ ПРОБЛЕМЫ
ПРОТИВОДЕЙСТВИЯ И СОВРЕМЕННОЕ СОСТОЯНИЕ
В РОССИЙСКОЙ ФЕДЕРАЦИИ
И СУБЪЕКТАХ РОССИЙСКОЙ ФЕДЕРАЦИИ
(НА ПРИМЕРЕ ТАМБОВСКОЙ ОБЛАСТИ)**

Аннотация. В статье раскрыта сущность преступлений в сфере информационных технологий, дана их криминалистическая характеристика, отражена статистика и состояние рассматриваемого вида преступности в РФ (на примере Тамбовской области). Выделены актуальные проблемы противодействия данным преступлениям, тезисно отражены пути их решения, проанализированы точки зрения, выдвинутые в научной литературе.

Ключевые слова: преступления в сфере информационных технологий, компьютерные программы, компьютерные устройства, информационная безопасность, цифровизация общества.

Alina Nikolaevna SHANINA

student

Institute of Law and National Security

of Tambov State University named after G.R. Derzhavin

**CRIMES IN THE SPHERE OF INFORMATION
TECHNOLOGIES: CURRENT PROBLEMS
OF COUNTERACTION AND THE CURRENT STATE
IN THE RUSSIAN FEDERATION AND THE SUBJECTS
OF THE RUSSIAN FEDERATION
(ON THE EXAMPLE OF THE TAMBOV REGION)**

Abstract. This article reveals the essence of crimes in the field of information technology, gives their forensic characteristics, reflects the statistics and state of the considered type of crime at present in the Russian Federation and the constituent entities of the Russian Federation using the example of the Tambov region. The author also highlighted the urgent problems of countering these crimes, the thesis reflects the ways of their solution, analyzed the points of view put forward in the scientific literature.

Keywords: information technology crimes, computer programs, computer devices, information security, digitalization of society.

Стремительное развитие научно-технического прогресса и всеобщей цифровизации общества привело к внедрению ин-

формационных технологий во все без исключения сферы жизни общества и государства, начиная с бытовых и заканчивая политическими и межгосударственными. Такая тенденция порождает как положительные, так и негативные последствия, ведь злоупотребление информационными технологиями представляет общественную опасность и влечет причинение вреда. Поэтому противодействие подобному злоупотреблению становится все более актуальным и приоритетным направлением.

УК РФ преступления в сфере информационных технологий устанавливает в гл. 28 «Неправомерный доступ к компьютерной информации», включающей 4 статьи (ст. 272–274¹), которая постоянно реформируется законодателем в соответствии с реалиями современности (например, в 2011 г. в ст. 273 УК РФ был добавлен особо квалифицирующий состав, изменена санкция, а также формулировка ч. 1 указанной статьи – понятие «программа для ЭВМ» заменено «компьютерной программой», поскольку на тот момент уже потеряло свою актуальность и вышло из обихода).

Рассматриваемые преступления характеризуются рядом специфических признаков, ранее неизвестных российскому уголовному законодательству. Во-первых, информационные преступные деяния всегда совершаются в особой среде, «кибернетическом виртуальном пространстве». Характерной особенностью такой нестандартной обстановки преступления является то, что субъект преступления в момент его совершения может находиться в любой географической точке, и для осуществления преступных действий он может задействовать несколько компьютеров независимо от их месторасположения друг от друга, то есть действовать удаленно. Помимо пространственного аспекта, особую значимость представляет и временной. Поскольку работа ряда компьютерных программ связана с установленным на устройстве временем, а преступник может его ситуационно изменять, то это создает значительные трудности в расследовании рассматриваемых преступлений. Исходя из этого, установить место и время совершения преступления крайне сложно и зачастую вообще невозможно¹.

¹ Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. 2013. С. 114.

Во-вторых, следовая картина рассматриваемой группы преступлений настолько специфична, что не рассматривается трасологией в традиционном формате. Ряд исследователей обоснованно выделяют ее в отдельную категорию, в частности, В.О. Давыдов, Е.Д. Малахвей, помимо материальных и идеальных следов, предлагают использовать понятие «виртуальных следов», присущее исключительно информационным преступлениям. Такие следы характеризуются тем, что могут быть зафиксированы только в цифровом формате, иначе говоря, в виде «образа формальной модели изменения состояния информации в памяти компьютерных устройств, вызванные алгоритмом установленного программного обеспечения и связанные с событием преступления»².

В-третьих, многообразие средств и способов совершения рассматриваемых преступлений обуславливает их доступность и широкую распространенность применения, как следствие, широкий перечень субъектов (вопреки общепринятому мнению, преступники данной сферы необязательно должны быть специалистами в сфере информационных технологий). Преступные посягательства рассматриваемой группы всегда совершаются при помощи информационных технологий. Это понятие включает в себя огромный перечень различных устройств: все многообразие видов компьютеров (стационарные компьютеры, смартфоны, ноутбуки и т.д.), компьютерные технологии (wi-fi, 4G и т.д.), компьютерные программы и приложения (Google Chrome, Тог и т.д.). На современном этапе развития основным и наиболее распространенным способом совершения информационных преступлений является использование программных обеспечений, а не самих устройств³.

В целом, неуклонная цифровизация общества во всем мире и в России, в том числе, приводит к тому, что информационные

² Давыдов В.О., Малахвей Е.Д. О некоторых аспектах криминалистической характеристики преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Тульского государственного университета. Экономические и юридические науки. 2019. С. 98.

³ Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2 (32). С. 162.

преступления выходят на первый план и приоритетное место для субъектов расследования, раскрытия и предупреждения преступных посягательств. Их сопряжение с ранее уже известными уголовному законодательству составами (в частности, с различными видами хищения, например, мошенничеством) свидетельствует о крайне высокой степени общественной опасности, а также о необходимости активного принятия эффективных мер по противодействию рассматриваемым деяниям. Так, например, только за январь – сентябрь 2020 г. в России зарегистрировано 363 034 (77 %) преступлений, совершенных с использованием информационных технологий, из них 184 736 (86,5 %) тяжких и особо тяжких⁴. Для сравнения, за январь – декабрь 2019 г. таких преступлений зарегистрировано 294 409 (68,5 %), из них 142 728 (48,5 %) тяжких и особо тяжких⁵. Вдобавок ко всему, преступления в сфере информационных технологий характеризуются высокой степенью латентности и анонимности преступников, поскольку тенденция развития современных технологий сводится к упрощению и удобству их использования, расширению их возможностей и, как следствие, способствует активному вовлечению лиц, не обладающих никакими специальными знаниями, умениями и криминальным опытом, в преступную деятельность⁶.

Темпы увеличения количества преступлений в сфере информационных технологий сохраняются и на уровне субъектов РФ. В силу специфики развития каждого региона, связанной с уровнем безработицы, плотности населения, правосознания и иными социально-экономическими факторами, распространение информационных преступлений неоднородно. В более развитых экономически и информационно субъектах РФ, количество таких преступлений выше, тогда как в субъектах с низкими темпами цифровизации

⁴ Краткая характеристика состояния преступности в Российской Федерации за январь – сентябрь 2020 г. URL: <https://xn--b1aew.xn--p1ai/reports/item/21551069/> (дата обращения: 30.10.2020).

⁵ Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2019 г. URL: <https://xn--b1aew.xn--p1ai/reports/item/19412450/> (дата обращения: 30.10.2020).

⁶ *Кратива И.И., Прудникова И.В.* Криминологическая характеристика преступлений, совершаемых с использованием современных телекоммуникационных технологий // Закон и право. 2020. № 10. С. 170.

данный показатель составляет сравнительно небольшое число. Например, в Тамбовской области количество преступлений в сфере информационных технологий относительно ряда других регионов невелико и, как правило, связано с различными видами хищений. Анализ судебной практики говорит о том, что для данного региона не характерно многообразие используемых средств и способов совершения информационных преступных деяний, обычно они типичны и не связаны со сложным, профессиональным использованием компьютерных устройств. В качестве иллюстрации выдвинутого тезиса приведем пример из судебной практики.

В соответствии с приговором Котовского городского суда от 25 января 2012 г. по делу № 1-9/2012 А. умышленно незаконным способом завладел информацией, касающейся логина и пароля Ф., с целью авторизации на сайте, находящемся в его пользовании, а затем, используя находящиеся в его квартире стационарный компьютер, в комплектацию которого входит программное обеспечение, предназначенное для доступа к сети Интернет, после чего без согласия собственника информации Ф. осуществил неправомерный доступ к охраняемой законом компьютерной информации, размещенной на сайте, и, авторизовавшись, разместил на соответствующем сайте надписи и изображение, что привело к модификации информации, то есть к изменению ее содержания по сравнению с первоначальной.

Суд квалифицировал действия А. в соответствии с ч. 1 ст. 272 УК РФ как неправомерный доступ к охраняемой законом компьютерной информации, повлекший модификацию компьютерной информации, и назначил ему наказание в виде штрафа в размере 10 000 руб.⁷

Поскольку преступления в сфере информационных технологий являются сравнительно новыми для российского уголовного законодательства, обладают своей спецификой и представляют собой довольно сложные преступные деяния, то принимаемые меры по противодействию им сталкиваются с рядом проблем. Во-первых, в целях наиболее эффективного расследования и раскрытия рассматриваемых преступных посягательств, как правило, требуется

⁷ Приговор Котовского городского суда от 25 января 2012 г. по делу № 1-9/2012. URL: <https://clck.ru/RghV6> (дата обращения: 30.10.2020).

привлечение экспертов, специализирующихся в области компьютерных устройств. Однако в настоящее время в РФ существует проблема недостатка соответствующих экспертов, что существенно замедляет производство судебных экспертиз и влияет на повышение их стоимости. Данная проблема требует комплексного решения и серьезного к нему подхода. По мнению В.В. Гончар, эффективный результат может дать только ориентация высших учебных заведений на подготовку экспертов соответствующего профиля, а также их взаимодействие с организациями, специализирующимися в области информационной безопасности⁸.

Во-вторых, в расследовании и раскрытии информационных преступлений выделяются проблемы идентификации пользователей программ, ресурсов и серверов сети Интернет, находящихся вне юрисдикции РФ. Использование иностранных ресурсов преступниками не только обеспечивает качественное сокрытие совершенного противоправного деяния, но и фактически лишает правоохранительные органы возможности получить какую-либо криминалистически значимую информацию. В этой связи В.О. Давыдов и И.В. Тишутина считают целесообразным расширить возможности используемой правоохранительными органами подсистемы ИБД-Ф «Дистанционное мошенничество», позволяющей собирать необходимые сведения о преступлениях, совершенных посредством дистанционного доступа и управления⁹.

В-третьих, темпы развития законодательства не всегда совпадают с темпами развития информационных технологий, что порождает большое количество пробелов и коллизий, невозможность полного урегулирования правоотношений в рассматриваемой области. Некоторые нормы права устаревают и не отвечают актуальным общественным требованиям, поэтому необходимо, чтобы им на смену своевременно принимались новые и при этом органично

⁸ Гончар В.В. Совершенствование расследования преступлений в сфере информационных технологий // Эпоха науки. 2017. № 11. С. 29.

⁹ Давыдов В.О., Тишутина И.В. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2020. № 2 (14). С. 85.

вписывались в действующую правовую систему. С.В. Иванцов наиболее эффективной мерой для решения указанной проблемы видит реформирование ряда действующих нормативно-правовых актов, в частности, включение в Федеральный закон от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» таких положений, которые «учитывали бы специфику предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных сетей»¹⁰.

Таким образом, преступления в сфере информационных технологий являются одной из наиболее актуальных и общественно опасных групп противоправных деяний как на уровне государства, так и на уровне регионов. Рассматриваемые преступные посягательства навсегда вошли в нынешние реалии и прочно закрепились в них. Тенденция развития информационной сферы позволяет сделать вывод о том, что в будущем преступления в сфере информационных технологий будут только усложняться и распространяться, поэтому крайне важно уже на данном этапе обеспечить необходимые меры противодействия таким преступным посягательствам.

¹⁰ Иванцов С.В. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей: вопросы предупреждения // Криминологический журнал. 2019. № 2. С. 37.

Анна Алексеевна Шепелёва
студент

*Институт права и национальной безопасности
Тамбовского государственного университета им. Г.Р. Державина*

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В КАЧЕСТВЕ СРЕДСТВА ВОВЛЕЧЕНИЯ ПОДРОСТКОВ В ПРЕСТУПНУЮ ДЕЯТЕЛЬНОСТЬ

Аннотация. Жизнь в постиндустриальном обществе имеет как позитивные, так и негативные аспекты. Интернет-пространство дает обществу большие возможности, предоставляя огромный объем информации, которая содержит в себе ответы практически на все возникающие у человека вопроса. Однако возможность безграничного доступа к информационным ресурсам способствует развитию преступности. Самой уязвимой к влиянию Интернет-преступников является подростковая часть населения. Молодые люди, проводя практически все свое свободное время в Интернете, ввиду своего любопытства и правовой непросвещенности попадают под влияние преступников, совершая впоследствии различного рода преступные деяния. Обусловлено такое явление особенностями подросткового возраста, характеризующимся протестом обществу, негативным настроением относительно правил и законов.

Ключевые слова: подростки, подростковая преступность, Интернет, информационные технологии, запрещенный контент.

Anna Alekseevna SHEPELEVA
student

*Institute of Law and National Security
of Tambov State University named after G.R. Derzhavin*

USING INFORMATION TECHNOLOGY AS A MEANS OF INVOLVING ADOLESCENTS IN CRIMINAL ACTIVITY

Abstract. Life in a post-industrial society has both positive and negative aspects. The Internet space gives society great opportunities, providing a huge amount of information that contains answers to almost all questions that a person has. However, the possibility of unlimited access to information resources contributes to the development of crime. The most vulnerable to the influence of cybercriminals are the teenage population. Young people, spending almost all their free time on the Internet, because of their curiosity and legal ignorance, fall under the influence of criminals, and therefore commit various kinds of criminal acts. This phenomenon is due to the peculiarities of adolescence, characterized by a protest from society, a negative mood regarding the rules and laws.

Keywords: teenagers, juvenile delinquency, the Internet, information technology, prohibited content.

Развитие информационных технологий влияет на правосознание подрастающего поколения, его поведение при взаимо-

действию с социумом. Подростки, имея неограниченный доступ к сети Интернет, могут воспользоваться размещенным там запрещенным контентом, взаимодействие с которым ведет к повышению уровня подростковой преступности. Дело в том, что в открытом доступе существуют аккаунты, группы и сообщества, которые могут способствовать вовлечению подростков в преступную деятельность.

Отметим, что основными видами преступной деятельности в таком случае следует считать: проституцию, детскую порнографию, незаконный оборот наркотиков, доведение до самоубийства (суицид).

Вовлечь подростка в преступную деятельность бывает достаточно просто, так как данную возрастную группу следует считать наиболее уязвимой к попаданию под чье-либо влияние, что, в свою очередь, ведет к тяжелым негативным последствиям.

О.В. Дамаскин, В.В. Красинский отмечают следующие причины, способствующие вовлечению подрастающего поколения в преступность: «Дифференциация в доступе отдельных категорий детей к качественному образованию, низкий уровень этического, гражданско-патриотического, культурного развития детей приводят к возникновению в подростковой среде межэтнической и межконфессиональной напряженности, ксенофобии, к дискриминационному поведению, травле сверстников («буллинг») и другим асоциальным явлениям»¹.

С учетом всех перечисленных условий подростковая преступность в России с годами лишь возрастает. Критичность ситуации выражается в том, что число подростков, поставленных в 2019 г. на учет, значительно возросло.

В соответствии с данными, размещенными на официальном сайте Генеральной прокуратуры РФ, «несовершеннолетние в России ежегодно совершают или участвуют более чем в 40 тыс. преступлений. Большинство несовершеннолетних (83 %) в 2019 г. совершили преступления против собственности, 8 % – против жизни

¹ Дамаскин О.В., Красинский В.В. Криминологическая характеристика механизма вовлечения несовершеннолетних в противоправную деятельность // Государство и право. 2020. № 8. С. 41–54.

и здоровья, более 4 % – это преступления, связанные с незаконным оборотом наркотиков»².

В основном, подростков в сети Интернет манят такие темы, как массовые убийства, сатанизм, наркомания, а также сообщества, располагающие информацией о каких-либо ритуалах, различных культах и т.п. В том числе встречается негативный контент, направленный непосредственно на дискриминацию, исходя из религиозных взглядов, национальной принадлежности, полового признака, возраста и т.д. Относя себя к таким группам, подростки выражают протест обществу. На такой протест, выраженный в сетевом общении, поступает реакция преступников, действующих посредством использования информационных технологий. Неспособные верно воспринимать и анализировать поступающую информацию подростки попадают под негативное влияние и, соответственно, совершают преступления. При этом вред они могут нанести как обществу, так и самому себе.

Несмотря на то, что правоохранительные органы активно противодействуют распространению в Интернете информации, способствующей повышению уровню подростковой преступности, экстремистам все же удается распространять свое влияние на подрастающее поколение, при этом значительно расширяя заинтересованную их деятельностью аудиторию.

Как происходит такое явление, отмечают в своей работе А.Л. Осипенко и В.С. Соловьев: «В сети организуются форумы, которые создают иллюзию, что указания, рекомендации, призывы, умело помещаемые модераторами в контекст обыденного общения, коллективно согласованы и поддерживаются большей частью общества. Помимо этого, в последнее время в связи с усилением активности правоохранительной деятельности в киберпространстве материалы экстремистской направленности массово переводятся в его «теневые» сегменты, доступ к которым новым участникам предоставляется только после их предварительной проверки на «лояльность»³.

² Генеральная прокуратура РФ. Показатели преступности в России. URL: <http://crimestat.ru/> (дата обращения: 31.10.2020).

³ *Осипенко А.Л., Соловьев В.С.* Киберугрозы в отношении несовершеннолетних и особенности противодействия им с применением информационных технологий // *Общество и право.* 2019. № 3 (69). С. 23–31.

Коммуникация в сети Интернет имеет свою специфику, которая выражается в том, что общение может быть как открытым (собеседники имеют представление друг о друге), так и анонимным (без указания имени и информации о собеседнике). Зачастую преступники предпочитают общаться с подростками анонимно, делая это для того, чтобы обезопасить себя и заинтересовать подростка, формируя свой образ лишь в его воображении.

Различные намерения преступников, использующих информационные технологии для связи с подростками, получили различное терминологическое закрепление. Таким образом, появились новые слова и словосочетания:

- кибербулинг (Интернет-травля) – действия в сети Интернет, характеризующиеся угрозами, негативными высказываниями со стороны недоброжелателя, направленные на провокацию собеседника, побуждению его к агрессивной ответной реакции;
- аутинг – действия в сети Интернет, направленные на публикацию информации о подростке без его осведомленности о таковом деянии;
- киберсталкинг – действия взрослых в сети Интернет, направленные на организацию личной встречи с подростком с целью вступления с ним в сексуальную связь;
- фрейпинг – получение злоумышленником возможности управлять учетной записью подростка без его ведома и т.д.

Говоря о действиях подростков, находящихся под влиянием негативного воздействия со стороны Интернет-преступников, отметим такое деяние как суицид.

Появлению желания совершить самоубийство у подростков способствует распространение в сети информации, говорящей об обесценивании человеческой жизни, ее бессмысленности. Сообщества такого типа имеют собственную символику, сленг, специальные изображения средств и способов совершения суицида. Помимо таковых имеются сообщества, содержащие информацию о занятиях или увлечениях, которые могут привести к получению увечий или же к смерти.

А.Л. Осипенко и В.С. Соловьев к таковым относят: скайукинг – покорение высоких строений без специального снаряжения, рупинг – незаконное проникновение на крыши высотных зданий,

зацепинг – проезд на крыше или подножке вагона поезда, трамвая, диггерство – изучение подземных коммуникаций»⁴.

Помимо этого в сети часто появляются видеозаписи, сделанные подростками, где те наносят увечья людям или животным. Молодые люди такими действиями вымещают свою агрессию на тех, у кого нет возможности за себя постоять. Как пример стоит рассмотреть своеобразное движение, именуемое «Dog hunters», суть которого заключается в истязании, избивании или убийстве собак.

В последнее время известно такое направление, идеология которого предполагает формирование среди подростков группировок, деятельность которых направлена на совершение антиобщественных деяний, в частности, унижение чести и достоинства личности, вымогательство.

Пристального влияния правоохранительных органов удостоились преступления, связанные с половой неприкосновенностью подростков. На просторах Интернета педофилы находятся в поисках подростков, которые обделены вниманием, оказались в трудной жизненной ситуации и нуждаются в поддержке со стороны. Пользуясь ситуацией, преступники входят в доверие к ним, впоследствии совершая действия сексуального характера. Примером такого взаимодействия следует считать: запрос преступником у подростка интимных фото, общение на сексуальные темы, направление подросткам порнографического материала или собственных непристойных фото- и видеоматериалов и т.п.

Не стоит также оставлять без внимания наркопреступность и вовлечение в нее подростков. У подростков возникает интерес попробовать запрещенные вещества или же получить денежные средства при их транспортировке. Узнают молодые люди о наркобизнесе и обо всем, связанным с ним, из различных Интернет-сообществ, содержащих информацию о правильном хранении, перевозке и применении наркотических средств.

Таким образом, информационные технологии широко используются подростками, причем не всегда в положительном ключе. Существует множество сообществ, групп и аккаунтов, основной

⁴ Там же.

задачей которых является вовлечение подрастающего поколения в преступную деятельность. С развитием информационных технологий развивается и киберпреступность, порождая новые движения и направления, к которым подростки охотно присоединяются, с целью показать свой протест обществу. Правоохранительные органы, в свою очередь, занимаются решением данной проблемы, отслеживая Интернет-преступников, в последствии привлекая их к ответственности. Однако не всегда удается найти виновного ввиду того, что тот действует анонимно.

С целью предотвращения вступления подростков в преступные сообщества, на наш взгляд, следует усилить родительский контроль за деятельностью подростков в социальных сетях, уделять больше внимания их воспитанию, при возникновении конфликтной ситуации обращаться к психологу, чтобы ребенок не стал искать решение проблемы в социальных сетях.

Правоохранительным органам, в свою очередь, следует усовершенствовать владение информационными технологиями с целью своевременного обнаружения и устранения источника преступного воздействия на общество.

СПИСОК СОКРАЩЕНИЙ

LIST OF ABBREVIATIONS

АПК РФ – Арбитражный процессуальный кодекс Российской Федерации

ГК РФ – Гражданский кодекс Российской Федерации

ГПК РФ – Гражданский процессуальный кодекс Российской Федерации

НК РФ – Налоговый кодекс Российской Федерации

СЗ РФ – Собрание законодательства Российской Федерации

УК РФ – Уголовный кодекс Российской Федерации

УПК РФ – Уголовно-процессуальный кодекс Российской Федерации

Научное издание

**ПРОТИВОДЕЙСТВИЕ ПРАВОНАРУШЕНИЯМ,
СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

***Сборник статей по материалам
научно-практической конференции
(III школы-семинара молодых ученых-юристов)***

г. Москва, 11 ноября 2020 г.

Редактор – *Д.А. Семенова*
Компьютерная верстка *Н.В. Бессарабовой*

Подписано к изданию 01.06.2021. Формат 60x84^{1/16}.
Гарнитура Times New Roman Суг. Усл.-печ. л. 14. Тираж ... экз. Зак. № _____.

Отпечатано в ООО «ИПЦ „Маска“»
117246, Москва, Научный проезд, д. 20, стр. 9, оф. 212
Телефон: +7 (495) 510-32-98