МЕЖДУНАРОДНЫЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ

УГОЛОВНАЯ ПОЛИТИКА И ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В ИНФОРМАЦИОННУЮ ЭРУ

Материалы межвузовской студенческой
научно-практической конференции
с международным участием

26 ноября 2021 г.

Москва
2022

УДК 343.2/343.3/.7
ББК 67.408
А 43

А 43 Уголовная политика и проблемы борьбы с преступностью в информационную эру: материалы межвузовской студенческой научно-практической конференции с международным участием (26 ноября 2021 г.) / Отв. ред. к.ю.н., доцент А.А. Ходусов, д.ю.н., доцент А.М. Смирнов. – М.: Международный юридический институт, 2022. – 79 с.

Сборник научных статей студентов и курсантов содержит материалы межвузовской студенческой научно-практической конференции с международным участием на тему: «Уголовная политика и проблемы борьбы с преступностью в информационную эру», проходившей в Международном юридическом институте 26 ноября 2021 г.

В сборник вошли статьи по ключевым вопросам борьбы с преступностью в информационную эру, противодействия преступности и формирования российской уголовной политики с учетом современных условий функционирования отечественной системы обеспечения безопасности личности, общества и государства

Тексты выступлений участников научно-практической конференции изложены в оригинальном авторском формате.

ОГЛАВЛЕНИЕ

Азарова А.С.,
студентка 3 курса Института правоохранительной деятельности Саратовской государственной юридической академии,

Azarova A.S.,
3rd year student of the Institute of Law Enforcement of the Saratov State Law Academy,

НЕКОТОРЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В ДАРКНЕТЕ

SOME PROBLEMS OF COUNTERING CRIME IN THE DARKNET

Аннотация: в статье рассматриваются отдельные вопросы, касающиеся криминальной деятельности в сети даркнет. Анализируются официальные статистические данные, литературные источники, на основе которых выделяется ряд рекомендаций, направленных на повышение эффективности деятельности государственных органов по противодействию совершаемым в скрытой сети общественно опасным деяниям.

Abstract: the article discusses certain issues related to criminal activity on the darknet. The author analyzes the official statistical data, literary sources, on the basis of which a number of recommendations are identified, aimed at increasing the efficiency of the activities of state bodies in countering socially dangerous acts committed in a hidden network.

Ключевые слова: даркнет, преступность, наркоторговля, коронавирус, методы противодействия преступлениям.

Key words: darknet, crime, drug trafficking, coronavirus, methods of combating crime.

В последние годы правовые системы мира столкнулись с «новой» средой, на формирование которой большое влияние оказали информационно-коммуникационные технологии. В связи с этим многие группы правоотношений, традиционно существовавшие в «материальном» виде, перемещаются в киберпространство. В настоящей статье речь пойдет о даркнете, кардинально изменившем современную преступность и представляющем собой теневой рынок с многомиллионными оборотами. Любая высокая технология имеет тройное применение: гражданское, военное и криминальное [1, с. 22]. Последнее делает рассматриваемую проблему чрезвычайно актуальной.

Доступ к даркнету осуществляется через особые браузеры, такие как Tor, который изначально был военным проектом США, а позже распространился по всему миру. О востребованности даркнета среди россиян свидетельствуют данные официальной статистики, согласно которым только за 11 июля 2019 года более 600 тысяч наших соотечественников воспользовались браузером Tor. В этот день по количеству пользователей Россия заняла первое место, оставив позади США и Иран [2]. Среди высказанных объяснений были боты хакеров, попытка властей дестабилизировать даркнет и массированная рекламная кампания наркоторговцев.

Помимо даркнета существует также такое понятие, как deep web («глубокая сеть»), составляющая по оценкам экспертов 96%-99% от общего объема интернета. При этом контент, расположенный в данной части всемирной сети, хоть и не индексируется поисковиками, но является абсолютно законным и безопасным. Сюда относятся медицинские карточки, платный контент, закрытые форумы и прочие конфиденциальные данные. Что касается даркнета, то он в свою очередь лишь входит в состав «глубокой сети» и занимает около 5% от ее объема, хотя точные цифры неизвестны.

Одними из наиболее популярных категорий инструментов и услуг, представленных на dark web, являются организация DDoS-атак, взломы, шпионаж, кража клиентских баз,

корпоративной и персональной финансовой информация [3]. Д. Бартлетт также указывает на такие общественно опасные деяния, совершаемые в даркнете, как размещение порнографического контента, продажа оружия, поиск убийц по найму, нарушение прав на интеллектуальную собственность, виртуальная валюта [4, с. 180]. Наряду с этим, даркнет довольно успешно используется и во благо, например, для развития креативных форм общения. Поэтому особое внимание нужно обратить на то, что преступными должны считаться не технологии, а цели, для достижения которых они могут быть использованы.

Таким образом, мы разделяем точку зрения исследователей, говорящих о невозможности и ненужности запрета даркнета [5, с. 11]. Ведь он выступает лишь как инструмент, который приобретает общественную опасность в связи с преступными целями пользователей, а не сам по себе. Помимо этого, очевидно, что государства пока еще не в состоянии полностью заблокировать использование даркнета, что вызвано многочисленными сложностями, связанными со спецификой работы этой сети. Более того, немалая часть преступлений представлена и в традиционном интернете, что свидетельствует о переоцененности криминального значения темной сети. Мы считаем, что наиболее верным направлением дальнейшей деятельности в данной сфере будет разработка новых правовых и технических средств борьбы с опасными проявлениями даркнета.

На увеличение аудитории даркнета повлияла и новая коронавирусная инфекция с глобальным локдауном. В 2020 году за несколько дней были приобретены 130 доменов, связанных с коронавирусом, которые потенциально могут использоваться для незаконных целей. В частности, активизировались мошенники, продающие «вакцины» от коронавируса. В России к началу пандемии Tor посещали 380 тысяч пользователей в сутки, а в конце апреля – около 400 тысяч [6]. Информации о том, какой объем продаж в даркнете занимают те, что осуществляются на территории России, нет. Однако русский язык используется чаще всего, а именно в 41% случаев по состоянию на 2015 год [7].

Впервые даркнет, а именно Tor, обратил на себя внимание правоохранительных органов в связи с деятельностью анонимной площадки по торговле запрещенными психоактивными веществами под названием «Шелковый путь», работавшей с 2011 по 2013 год, где было представлено около 340 видов наркотиков. После закрытия у сайта появились подражатели, количество которых в скрытой сети в настоящее время только растет [8, с. 177].

Положительным влиянием коронавируса оказалось сокращение в России рынка наркотиков, вызванное усложнением работы «кладменов». На форумах в даркнете даже появились темы «Как забрать клад в режиме самоизоляции». Интересный опрос по данному поводу был проведен Фондом содействия защите здоровья и социальной справедливости им. Андрея Рылькова. Выяснилось, что из-за карантина 55,7% пользователей стало сложнее забирать «закладки», а 38% пожаловались на дефицит психоактивных веществ [9].

Вместе с тем, в целом рынок наркоторговли продолжает процветать. Так, в 2020 году он составил 35 600 кг, что равно примерно 1/5 от общемировых данных по изъятию психоактивных веществ [10]. Стабильно высокий объем реализуемых наркотических средств помогает поддерживать и огромный массив запрещенной к распространению информации, находящейся в даркнете. В связи с этим полагаем необходимым отнести пропаганду наркотических средств и психотропных веществ к числу особо опасных деяний, перенеся данный состав из Кодекса об административных правонарушениях РФ в Уголовный кодекс РФ.

Для решения проблемы распространения информации криминального характера нужно применить ряд мер. А.В. Бахмисов выделяет среди них следующие [11, с. 96]. Во-первых, необходима разработка механизмов идентификации лиц, нарушающих законодательство РФ в «невидимом» сегменте Интернета, установления владельца сайта, оператора информационной системы, его пользователя. Помимо этого, для пресечения незаконной деятельности важно разработать технические возможности блокирования и уничтожения запрещенной к распространению информации из сети Интернет. Причем особняком стоит вопрос о том, кто же

возьмет на себя соответствующие полномочия. Представляется, что головным исполнителем данного рода решений необходимо назначить Министерство цифрового развития, связи и массовых коммуникаций РФ.

Во-вторых, для создания определенности в работе государственных органов требуется создать классификатор запрещенной к распространению информации, содержащейся в даркнете. На наш взгляд, центральным критерием подобной классификации должна стать степень ее опасности. Обязанность проведения экспертного анализа такой информации следует возложить на подведомственную Минцифре РФ Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Кроме того, повышению эффективности мер, направленных на противодействие преступлениям, совершаемым бесконтактным способом, послужит постоянное взаимодействие сотрудников правоохранительных органов с учеными и экспертами в области информационных технологий для выработки новых методик борьбы с интернет-преступностью. Для более успешного выявления и пресечения преступлений в даркнете должно быть налажено более тесное взаимодействие между правоохранительными органами и органами исполнительной власти РФ.

На основе вышеизложенного мы приходим к выводу о том, что даркнет довольно сильно криминализирован и содержит значительное число ресурсов, нарушающих уголовные законы. Само его существование некоторые авторы оценивают как угрозу национальной безопасности России [12, с. 204]. Одной из важнейших задач законодателя в связке с практикующими юристами и учеными выступает разработка соответствующих современности нормативных правовых актов и методик противодействия преступности в даркнете. Наконец, должна быть усовершенствована работа правоохранительных органов и органов исполнительной власти РФ, в том числе предложенными нами в настоящей статье способами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. М.: Норма, 2020. 352 с.
2. Россия бьет рекорд за рекордом в даркнете. Что происходит? // URL: https://www.bbc.com/russian/news-49007476 (дата обращения: 14.11.2021).
3. DarkNet – какие угрозы живут в тени. Часть 1 // URL: https://stakhanovets.ru/blog/darknet-kakie-ugrozy-zhivut-v-teni-chast-1/ (дата обращения: 14.11.2021).
4. Бартлетт Д. Подпольный интернет: темная сторона мировой паутины. М.: Эксмо, 2017. 352 с.
5. Васильев А.А., Ибрагимов Ж.И., Васильева О.В. Даркнет как ускользающая сфера правового регулирования // Юрислингвистика. 2019. № 12. С. 10-12.
6. Даркнет на карантине: как изменились аудитория и доходы нелегальных площадок // URL: https://thebell.io/darknet-na-karantine-kak-izmenilis-auditoriya-i-dohody-nelegalnyh-ploshhadok (дата обращения: 15.11.2021).
7. Going Deeper: Exploring the Deep Web // URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploring-the-deep-web (дата обращения: 15.11.2021).
8. Долгиева М.М. Криптовалютная наркоторговля в России и за рубежом // Вестник Воронежского института МВД России. 2018. № 4. С. 177-182.
9. Эпидемия и психоактивные вещества // URL: https://telegra.ph/EHpidemiya-i-psihoaktivnye-veshchestva-04-11 (дата обращения: 15.11.2021).
10. Официальная статистика за 2021 год употребление наркотиков в России // URL: https://narkonet.info/oficialnaja-statistika-za-2021-god-upotreblenie-narkotikov-v-rossii/ (дата обращения: 15.11.2021).

11. Бахмисов А.В. Проблемы распространения информации в «невидимом» сегменте интернета // Академическая мысль. 2021. № 1 (14). С. 94-98.

12. Галий А.А. Даркнет, как угроза национальной безопасности Российской Федерации / А.А. Галий, И.В. Слюсарь // Вестник науки. 2018. Т. 1. № 9. С. 204-205.

Антюфеев Д.А.,
курсант 4 курса прокурорско-следственного факультета Военного университета имени князя Александра Невского Министерства обороны Российской Федерации,

Antyufeev D. A,
4th year cadet of the Prosecutorial and Investigative Faculty of the Prince Alexander Nevsky Military University of the Ministry of Defense of the Russian Federation,

МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ И ОТГРАНИЧЕНИЯ ОТ СМЕЖНЫХ СОСТАВОВ ПРЕСТУПЛЕНИЙ

FRAUD IN THE SPHERE OF COMPUTER INFORMATION: PROBLEMS OF QUALIFICATION AND RESTRICTIONS FROM RELATED OFFENSES

Аннотация: IT-технологии стали новой реальностью всех сфер общественной жизни, в том числе криминальной. Преступники активно используют компьютерные технологии при совершении преступлений экономической направленности, что существенно упрощает им доступ к имуществу и имущественным правам. Указанная тенденция стала причиной введения в Уголовный кодекс Российской Федерации Федеральным законом от 29 ноября 2012 г. № 207-ФЗ нового состава преступления – «Мошенничество в сфере компьютерной информации» (ст. 159.6 УК РФ). Однако данный состав преступления при всей его необходимости для уголовно-правовой защиты имущества и имущественных прав обладает существенными недостатками, снижающими его эффективное правоприменение. В статье рассматриваются проблемные вопросы квалификации состава преступления, связанного с мошенничеством в сфере компьютерной информации и отграничения данного состава преступления от смежных составов исходя из положений уголовного законодательства РФ.

Abstract: IT technologies have become a new reality in all spheres of public life, including criminal ones. Criminals actively use computer technology to commit economic crimes, which greatly simplifies their access to property and property rights. This trend was the reason for the introduction into the Criminal Code of the Russian Federation by Federal Law No. 207-FZ of November 29, 2012, a new corpus delicti – «Fraud in the field of computer information» (Article 159.6 of the Criminal Code of the Russian Federation). However, this corpus delicti, with all its necessity for the criminal legal protection of property and property rights, has significant drawbacks that reduce its effective enforcement. The article deals with the problematic issues of qualifying the corpus delicti associated with fraud in the field of computer information and the delimitation of this corpus delicti from adjacent corpus delicti based on the provisions of the criminal legislation of the Russian Federation.

Ключевые слова: квалификация преступления, мошенничество, компьютерная информация, киберпреступность.

Key words: qualification of corpus delicti, fraud, computer information, cybercrime.

Мошенничество в сфере компьютерной информации – это приобретение права или хищение имущества, принадлежащего иному лицу либо организации путем ввода, блокирования, удаления, модификации компьютерной информации, или какого-либо иного вмешательства в обеспечение и функционирование средств обработки, хранения, передачи цифровых данных или информационно-телекоммуникационных сетей.

В 2012 году в Уголовный кодекс Российской Федерации (далее – УК РФ) были введены новые составы преступных деяний в области компьютерной информации, которые можно разделить на группы: финансовая группа; высокотехнологичная группа.

Среди новых составов преступления можно выделить мошенничество (ст. 159.3 УК РФ) [1], осуществляемое через использование электронных средств и способов платежа, мошенничество (ст. 159.6 УК РФ), осуществляемое в сфере компьютерной информации. Введение этих составов мошенничества обусловлено ростом цифровизации российской экономики, которая требует соответствующей реакции со стороны законодателей и правоприменителей.

Исследуемый вид мошенничества выделен в УК РФ в отдельный состав и рассматривается в качестве специального состава мошенничества. При этом стоит отметить, что многие ученые придерживаются мнения, что данный вид мошенничества обладает главной отличительной особенностью по сравнению с другими видами, которая связана со сложностью данной формы хищения, как с позиции квалификации, так и с позиции расследования.

Мошенничество в области компьютерной и информационной информации является совершенно новым составом хищения, никоим образом, не связанным с основным составом мошенничества.

Мошенничество в сфере компьютерной информации, которое совершено через неправомерный доступ к цифровой информации, посредством создания, распространения или использования вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273, 274.1 УК РФ. В ситуациях, когда перехват информации, неправомерный доступ к цифровой информации является способом хищения денежных средств, то квалификация по ч. 3 ст. 272 УК РФ излишняя.

Вместе с тем в постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [3] значится, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ (п. 20), а согласно п. 21 Постановления, если хищение было совершено посредством использования учетных данных собственника имущества, при этом способ получения доступа к таким данным не имеет значения, то такое совершенное противоправное деяние квалифицируется как кража. При этом российским законодателем поясняется, что такая квалификация будет иметь место в том случае, если виновное лицо в ходе совершения данного противоправного деяния не оказало на программное обеспечение компьютеров, серверов воздействия неправомерного характера.

Также Верховным Судом РФ закрепляется, что в случае, когда хищение чужого имущества или получение на него права произошло посредством распространения в сети Интернет информационных сведений, являющихся заведомо ложными, тогда имеет место быть состав мошенничества, который необходимо квалифицировать по ст. 159, а не ст. 159.6 УК РФ.

Под корыстной заинтересованностью лица понимают стремление лица получить выгоду имущественного характера через совершение неправомерных действий. Отсутствие обращения имущества в собственную пользу разрешает отграничить этот состав преступления от разного рода высокотехнологичных хищений, когда имущество обращается непосредственно в пользу лица [5; с. 22].

Одним из типичных способов совершения данных преступлений является использование специального, установленного на устройство потерпевшего лица вредоносного программного обеспечения. Использование такого обеспечения по отправке смс-сообщений без ведома пользователя (даже при случайной загрузке самим пользователем), является вводом конкретной информации. Действия программы по удалению уже отправленных сообщений для сокрытия собственной деятельности от пользователя является уничтожение цифровой информации.

Деяния, связанные с использованием программ «троянцев-вымогателей», квалифицируются по ст. 159.6 УК РФ. Такие программы шифруют файлы пользователя, блокируют экран устройства для выдвижения последующих требований выкупа. Способом совершения преступления в таком случае является блокирование цифровой информации, расположенной на компьютере. При этом возможное отсутствие злоупотребления или обмана не будет помехой, так как мошенничество, осуществленное в области компьютерной информации, относится к особым видам хищения. В этом случае также возможна дополнительная квалификация по ст. 273 УК РФ, так как создание вредоносного программного обеспечения не входит само по себе в описание способа совершения деяния, предусмотренного ст. 159.6.

В ходе рассмотрения состава исследуемого преступления можно сделать вывод, что объектом является одновременно чужое имущество и компьютерная информация.

Основными признаками состава преступления, предусмотренного ст. 159.6 УК РФ, являются 1) действия преступного лица, которые направлены на незаконное получение доступа к защищенной информации потерпевшего лица и 2) умысел, который направлен на хищение имущества лица, на информацию которого направлено преступное посягательство [6; с. 78]. Такие действия преступным лицом могут осуществляться различными способами: посредством взлома паролей, получение доступа к реквизитам банковских карт или счетов потерпевшего и т. д.

Анализ юридической доктрины и правоприменительной практики показывает, что рассматриваемое противоправное деяние может быть классифицировано на разные группы исходя из способа, которым оно было совершено.

К первой группе относятся хищения, совершенные с использованием мобильной связи, а именно путем получения доступа к денежным средствам потерпевшего при помощи телефона, который был изъят из его владения, с помощью которого преступник идентифицирует себя как собственник при использовании услуги «мобильного банка» и производит неправомерные манипуляции с банковскими счетами владельца телефона.

Во вторую группу классифицируют хищения, которые связаны с тем, что преступник завладевает номером мобильного телефона, который связан с банковскими счетами жертвы. В таких случаях преступник также получает доступ к денежным средствам потерпевшего, находящихся на этих банковских счетах.

Мошенники также могут вводить потерпевшего в заблуждения путем обмана через смс-сообщения либо звонки от имени сотрудников банка, а также посредством установки на мобильных телефонах потерпевших вирусного программного обеспечения, дающего доступ к управлению денежными средствами на банковских счетах.

К третьей группе относится хищение, которое может происходить при попытке потерпевшего осуществить приобретение товаров или услуг посредством сети Интернет. В таком случае необходимые для осуществления каких-либо операций реквизиты карты могут быть получены при добровольном вводе их потерпевшим на специально созданных сайтах, внешне напоминающие какие-либо ресурсы, например, известных интернет-магазинов.

Таким образом, исходя из приведенной классификации, можно говорить о том, что обязательным элементом рассматриваемого состава преступного деяния выступает непосредственно компьютерная информация. Однако целесообразно отметить, что не во всех случаях посягательство может быть направлено непосредственно (напрямую) на указанный объект. Таким образом, мошенничество в сфере компьютерной информации не стоит трактовать именно как хищение, которое совершается посредством применения глобальной сети Интернет.

Одна их проблем квалификации рассматриваемого преступного деяния связана с тем, что в составе мошенничества в сфере компьютерной информации отсутствует основной признак мошенничества, выражающийся в хищении посредством обмана или злоупотребления доверием.

Этот порок был заложен в данном составе изначально. Так, в пояснительной записке к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской

Федерации и иные законодательные акты Российской Федерации» было предложено выделить в самостоятельный состав компьютерное мошенничество как хищение или приобретение права на чужое имущество, сопряженное с преодолением компьютерной защиты имущества (имущественных прав) [7; с. 138]. Таким образом, авторы законопроекта изначально указали, что данное преступление совершается не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе, то есть данное деяние не является мошенничеством.

В результате произошло «размытие» понятия «мошенничество» при формулировании диспозиции ст. 159.6 УК РФ. Ведь общепринято, что мошенничество – это хищение путем обмана или злоупотребления доверием.

Позиция законодателя при формулировании ст. 159.6 УК РФ вошла в противоречие и с действовавшим в то время постановлением Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» [2] (утратил силу в связи с вынесением постановлением Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48), где говорилось об обмане или злоупотреблении доверием как об объективной стороне состава мошенничества; при этом в роли объекта обмана всегда выступает физическое лицо, соответственно, другими словами, в составе преступления мошенничества потерпевшим лицом всегда является физическое лицо, а никак не компьютер или компьютерная информация.

Также одной из проблем квалификации является конкуренция составов преступлений, которые предусмотрены ст. 159.6 и ст. 272 УК РФ. Так, отграничение следует производить по предмету и объекту посягательства. В ст. 272 УК РФ предметом посягательства является и информация, содержащаяся в компьютере, и компьютер, который выступает носителем информации, а объектом деяния выступают общественные отношения, обеспечивающие безопасность информации. В случае наличия состава ст. 159.6 УК РФ предметом деяния является полученная незаконным путем информации: ее используют для хищения или приобретения права на чужое имущество; тем самым общественные отношения, обеспечивающие сохранность чужого имущества, рассматриваются в качестве объекта.

Но при этом следует отметить, что безопасность компьютерной информации может выступать дополнительным объектом мошенничества, а хищение собственности – дополнительным объектом неправомерного доступа к компьютерной информации, совершенного с корыстными целями.

Обращаясь к разграничению ст. 159.6 и ч. 2 ст. 272 УК РФ, предусматривающей неправомерный доступ к компьютерной информации, совершенный с корыстными целями, можно сказать, что на первый взгляд объективная сторона рассматриваемых составов имеет много сходства. Но стоит учесть, что ввод, удаление, блокирование, модификация или любое иное вмешательство в информацию это лишь способ совершения мошенничества, в то время как, согласно диспозиции ст. 272 УК РФ, названные характеристики являются обязательными последствиями преступления, за которое наступает уголовная ответственность [4; с. 64].

Здесь также стоит отметить, что одним из последствий деяния, предусмотренного ст. 272 УК РФ, выступает именно уничтожение информации. Диспозиция же ст. 159.6 УК РФ говорит о том, что мошенничество может быть совершено путем удаления информации. То есть уже на этом этапе видно различие между составами. Однако правоприменитель зачастую не разграничивает между собой уничтожение информации и ее удаление, хотя по своей сущности – это абсолютно различные деяния. Уничтожение и удаление рассматриваются судами в каждом из этих случаев, как создание условий, при которых использование информации невозможно.

Разграничение стоит проводить и по субъективной стороне: деяние, предусмотренное ст. 159.6 УК РФ, характеризуется прямым умыслом, при этом обязательное условие состоит в том, что виновный руководствуется материальными целями. В отличие от мошенничества в сфере компьютерной информации при неправомерном доступе, согласно ч. 2 ст. 272 УК РФ, для преступника важно получение определенной информации, которая в дальнейшем поможет

злоумышленнику получить выгоду имущественного характера, не связанную с незаконным приобретением имущества.

Таким образом, проведенное исследование позволило выявить следующие особенности квалификации мошенничества, осуществленного в сфере компьютерной информации:

1) преступное деяние, которое предусмотрено ст. 159.6 не является мошенничеством в его классическом понимании, это новый состав хищения, совершенного вследствие другого способа данного деяния;

2) необходимо положительно оценить усиление наказания за данное деяние, отмену специального расчета объема ущерба применительно к этому деянию;

3) при квалификации данного преступного деяния правоприменителю важно принять во внимание определение понятий, данных в рекомендация по реализации прокурорского надзора, направленного на контроль исполнения законодательства при расследовании и раскрытии преступных деяний в области компьютерной информации;

4) важно широкое обсуждение тенденций вынесения Верховным Судом рекомендаций о квалификации по совокупности целого и части деяния, включая деяния, предусмотренные ст. 159.6 и ст. 272 УК РФ;

5) отграничение мошенничества, связанного с компьютерной информацией от смежных составов (ст. 158 и ст. 159 УК РФ) необходимо проводить по способу совершения преступного деяния.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.
2. Постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» (утратило силу) // Бюллетень Верховного Суда Российской Федерации, февраль 2008 г., № 2
3. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда Российской Федерации, февраль 2018 г., № 2
4. Безверхов А.Г. Хищение чужого имущества в условиях становления цифровой экономики // Уголовное право: стратегия развития в XXI веке: материалы XVII Международной научно-практической конференции. – М.: РГ-Пресс, – 2020. – С. 329-333.
5. Кузнецов А.А. Отграничение мошенничества от смежных составов преступлений. Тенденции развития науки и образования. – 2017. – № 26. – С. 44-50.
6. Кули-Заде Т.А. Проблемы квалификации мошенничества в сфере компьютерной информации // Российская юстиция. – 2019. – № 4. – С. 21-23.
7. Харитонов А.Н., Никульченкова Е.В. Квалификация мошенничества в сфере компьютерной информации // Российская юстиция. – 2019. – № 11. – С. 35-38.

Афанасьева А.С.
Курсант 4 курса Актюбинского Юридического института МВД РК им. М. Букенбаева

Afanasyeva A.S.
4th year cadet of the Aktobe Law Institute of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Bukenbaeva

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

TOPICAL ISSUES OF CYBERSECURITY IN THE REPUBLIC OF KAZAKHSTAN

Аннотация: Статья посвящена анализу таких глобальных угроз, как киберпреступность. Проанализированы их специфические аспекты. Особое внимание уделяется специфическим особенностям киберпреступности как явлению, в частности латентность (скрытность) компьютерных преступлений; трансграничность, легкость уничтожения и изменения компьютерной информации и т. д. Также автором отмечается, что для эффективного противодействия киберугрозам необходима стратегия взаимодействия в сфере кибербезопасности, способная защитить как государство, так и ее граждан, приведены некоторые направления и методы по ее реализации.

Abstract: The article is devoted to the analysis of such global threats as cybercrime. Their specific aspects are analyzed. Special attention is paid to the specific features of cybercrime as a phenomenon, in particular the latency (secrecy) of computer crimes; transboundary, ease of destruction and alteration of computer information, etc. The author also notes that in order to effectively counter cyber threats, a strategy of interaction in the field of cybersecurity is needed, capable of protecting both the state and its citizens, some directions and methods for its implementation are given.

Ключевые слова: киберпреступность, борьба с киберпреступностью, «Киберщит Казахстана», кибербезопасность.

Key words: cybercrime, combating cybercrime, «Cyber shield of Kazakhstan», cybersecurity.

Высокий темп развития информационных и коммуникационных технологий в Казахстане вызывает вопросы относительно защиты соответствующей инфраструктуры. Поскольку ее повреждение или разрушение может иметь значительные последствия для безопасности страны. Кроме того, увеличение числа пользователей интернета и расширение предоставляемых онлайн услуг привели к росту киберпреступности, в основном в финансовой сфере [1].

Киберпреступления в зависимости от объекта, от предмета посягательства, от способов совершения подразделяют на виды.

По объекту посягательства выделяются следующие группы киберпреступлений:

1) экономические компьютерные преступления;

2) компьютерные преступления против личных прав и неприкосновенности частной сферы;

3) компьютерные преступления против общественных и государственных интересов.

Киберпреступность оценивается как один из наиболее опасных видов преступности, которая вызывает необходимость глобального развития когнитивных и технологических навыков и компетенции правоохранительных органов в обеспечении информационной безопасности. Наиболее важными характеристиками этого типа преступлений обычно являются особая сложность его обнаружения и расследования, чрезвычайно высокая латентность, прозрачность национальных границ для преступников и отсутствие единой правовой основы для

борьбы с ним. Часто особо крупные размеры ущерба и высокопрофессиональный состав лиц, совершающих подобные преступления. Наглядный пример – выявленная в Алматы преступная группа, которая с помощью системы электронного «интернет-банкинга» занималась хищением денег со счетов предпринимателей. По версии следствия, преступники отправляли письма не только от имени Генеральной прокуратуры, но и в налоговую комиссию, Министерство финансов, Комиссию государственных доходов Министерства финансов Республики Казахстан и различных служб. После запуска предпринимателями вредоносной программы производилась ее активация. Затем, получив удаленный доступ к зараженным компьютерам и конфиденциальной информации, преступники перечисляли деньги на заранее открытые счета в банках второго уровня [2].

За первое полугодие 2021 г., по данным службы реагирования на компьютерные инциденты KZ-CERT, было зарегистрировано более 13,9 тыс. случаев нарушения компьютерной безопасности, что на 20,1% больше, чем за аналогичный период 2020 г. Это самый высокий показатель за время наблюдения в целом [3].

По вышеуказанным причинам одной из наиболее актуальных проблем в Республике Казахстан является противодействие киберпреступности.

В Казахстане особое внимание, подтверждающее актуальность исследования данного вопроса, было уделено еще в 2017 г. Будучи Главой государства, Первый Президент Казахстана – Елбасы Н. Назарбаев в своем Послании «Третья модернизация Казахстана: Глобальная конкурентоспособность» обратил внимание на актуальность проблемы борьбы с киберпреступностью. Тогда Правительству и Комитету национальной безопасности Республики Казахстан было поручено принять меры по созданию системы «Киберщит Казахстана». 30 июня того же года постановлением Правительства Республики Казахстан № 407 утверждена Концепция кибербезопасности («Киберщит Казахстана»).

В октябре 2017 г. принят План мероприятий по реализации Концепции кибербезопасности, по которому стандарты информационной безопасности усовершенствованы и закреплены законодательно. Кроме того, отраслевой закон ввел понятие «киберстрахование», которое позволяет возмещать материальный ущерб организации в результате ИТ-инцидентов, а также моральный ущерб, причиненный физическому лицу в результате утечки данных. Впервые в стране определен уполномоченный орган в области защиты персональных данных – Комитет информационной безопасности МЦРИАП Республики Казахстан.

Уже с 2018 г. одним из активных участников реализации мероприятий Концепции «Киберщит Казахстана» и Государственной программы «Цифровой Казахстан» становится акционерное общество «Государственная техническая служба» (АО «ГТС»). Благодаря значительным результатам компании в развитии системы кибербезопасности в своей отрасли, за 2019-2020 гг., согласно официальному отчету Международного союза электросвязи, Республика Казахстан занимает 31 место в Международном рейтинге киберготовности. И это учитывая, что в 2018-2019 гг. Казахстан занимал 40 место, а в отчете Международного союза электросвязи за 2017-2018 гг. Казахстан занимал 83 место. Такие существенные результаты были достигнуты за пару лет в рамках реализации Концепции «Киберщит». Так, уже более 10 лет АО «ГТС» работает для защиты электронной границы Казахстана и осуществляет монопольные виды деятельности в сферах информатизации и обеспечения информационной безопасности.

В 2020 году приняты правила сбора и обработки персональных данных, в которых изложены порядок и требования к обработке персональных данных от стадии сбора до стадии уничтожения. В 2020 году правоприменительная практика начала отслеживать нарушения требований к защите персональных данных для ЭИР (проверка в отношении оператора связи, субъектов частного предпринимательства) и законодательства об электронных документах и ЭЦП.

В 2020 году 17 центральных государственных органов централизованно оснащены средствами антивирусной защиты, предотвращения компьютерных атак и утечек информации,

мониторинга событий информационной безопасности. В результате внедрения указанных программно-технических средств Национальным координационным центром информационной безопасности в государственных органах зафиксировано более 55 тысяч уникальных типов событий, приведших к 4 тысячам инцидентов информационной безопасности. С целью обеспечения информационной безопасности в государственных органах и создания условий для развития отечественных производителей продукции электронной промышленности и программного обеспечения создан Реестр доверенной продукции электронной промышленности и программного обеспечения. В 2019 г. приняты поправки в законодательство о государственных закупках, согласно которым продукция электронной промышленности и программного обеспечения включена в Реестр и закупается в приоритетном порядке. Данная норма вступила в силу с 1 января 2020 г. На сегодняшний день в Реестр включены 85 наименований электронной промышленности и программного обеспечения от 34 производителей (программное обеспечение, персональные компьютеры, автоматические телефонные станции, генераторы шума, сетевые фильтры и т. д.) [4].

Также ратифицировано соглашение о расширенном партнерстве и сотрудничестве между нашей страной и Европейским союзом и его государствами-членами. В ней говорится, что стороны укрепляют сотрудничество, в том числе путем обмена передовым опытом, в целях предупреждения и борьбы с преступными действиями, совершенными с использованием коммуникационных сетей и информационных систем или против таких сетей и систем [5].

В действующем Уголовном кодексе Республики Казахстан киберпреступности посвящена целая глава «Преступления в сфере компьютеризации и связи», в ней 9 статей, регулирующих правоотношения в этой сфере и предусматривающих уголовную ответственность. С моей точки зрения, необходимо внимательнее подойти к теме современной киберпреступности, поскольку преступность растет, а ее проявления разнообразны – от простых мелких нарушений до глобальных вторжений.

В заключение хочу подчеркнуть, что защита собственного информационного пространства, оценка и разработка мер по устранению потенциальных угроз – это основные задачи любого государства, так как все больше информации влияет на общественные отношения.

Таким образом, быстрая информатизация, масштабы возможных последствий преступлений в киберпространстве требуют от государства особого внимания к развитию национальной системы кибербезопасности. Первоочередные шаги в этом направлении должны предусматривать разработку необходимой нормативно-правовой базы и повышение эффективности работы соответствующих институциональных структур с учетом зарубежного опыта в этой сфере.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. https://zerde.gov.kz/activity/ict/publication/2221 – свободный доступ (дата посещения 15.11.21)
2. https://www.parlam.kz/ru/blogs/smagylov/Details/4/41406 – свободный доступ (дата посещения 15.11.21)
3. https://kapital.kz/tehnology/97025/kolichestvo-kiberatak-v-rk-vyroslo-na-20-za-god.html – свободный доступ (дата посещения 16.11.21)
4. https://primeminister.kz/ru/news/reviews/fishingovye-sayty-spear-phishing-whaling-kibershchit-kazahstana-sovershenstvuet-sistemu-bezopasnosti-2675856 – свободный доступ (дата посещения 16.11.21)
5. https://adilet.zan.kz/rus/docs/Z970000113 – свободный доступ (дата посещения 16.11.21)

Бабич А.А.,
майор полиции
адъюнкт второго года обучения ФПНПиНК
Московского Университета МВД России имени В.Я.Кикотя,

Babich A.A.
police major,
adjunct of the second year of study at the faculty of training scientific,
pedagogical and scientific personnel
Moscow University
of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot,

МИГРАЦИЯ КАК ГЛАВНАЯ УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СТРАН-ПАРТНЕРОВ РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКИ КАЗАХСТАН

MIGRATION AS THE MAIN THREAT TO THE NATIONAL SECURITY OF THE PARTNER COUNTRIES OF THE RUSSIAN FEDERATION AND THE REPUBLIC OF KAZAKHSTAN

Аннотация: В статье рассматривается тема влияния миграционных процессов на преступность в Российской Федерации и Республике Казахстан. Анализируются статистические данные по рейтингу преступности в регионах России и Казахстана. Проводится сравнительный анализ количества преступлений, совершенных за пятилетний период в рассматриваемых странах. Анализируются детерминанты преступности мигрантов.

Abstract: The article examines the influence of migration processes on crime in the Russian Federation and the Republic of Kazakhstan. Statistical data on the crime rating in the regions of Russia and Kazakhstan are analyzed. A comparative analysis of the number of crimes committed over a five-year period in the countries under consideration is carried out. The determinants of migrant crime are analyzed. The main provisions of the article are summarized.

Ключевые слова: миграционные процессы, миграция, латентность, преступность.

Key words: migration processes, migration, latency, crime.

Миграционные процессы, обусловленные социальными условиями общественного развития, имеют как антикриминогенное, так и криминогенное значение. В Российской Федерации дефидент «миграция» употребляется в различных вариациях (миграционная политика, миграционные процессы, трудовая миграция и т. д.), однако определения этого термина в нормативных-правовых актах не существует. Согласно законодательству Республики Казахстан, термин «миграция» определяет постоянное или временное, добровольное или вынужденное перемещение физических лиц из одного государства в другое, а также внутри государства. Исходя из анализа миграционных процессов и ном их регулирующих, данное определение в полной мере отражает сущность понятия «миграция».

Следует отметить, что на современном этапе развития общества, наблюдается мощный диссонирующий миграционный тренд. В сравнении с советским периодом, для которого была характерна антимиграционная политика, ориентированная на естественный прирост и механическое распределение населения, с учетом потребностей промышленного производства. С учетом политических тенденций, миграция населения на сегодняшний момент приобретает массовые и угрожающие масштабы, обусловленные социально-экономическими условиями проживания населения.

Географическое расположение Республики Казахстан, в центральной части материка Евразия, служит путепроводом между странами Ближнего Востока, Европы и Азии. Миграционный поток преимущественно трудовых и нелегальных мигрантов, транзитным путем следует через Казахстан в Российскую Федерацию. Упрощенный порядок въезда, в рамках безвизового режима между Россией и Казахстаном создает условия прозрачности государственных границ и служит криминогенным фоном для нелегальной миграции.

Следует отметить, что миграционные процессы, характеризуются высокой латентностью, выражающейся в существенной разнице между количественными показателями мигрантов стран исхода и принимающими странами. Причинным комплексом, в данном контексте являются слабое информационное взаимодействие между странами-донорами и странами-реципиентами мигрантов, отсутствие визового режима для стран-участников СНГ, слабая оснащенность некоторых участков государственных границ. Данное обстоятельство свидетельствует о «неурегулированности» преступности мигрантов, прибывающих с нарушением правил миграционного законодательства и находящихся вне поли зрения правоохранительных служб.

В региональном разрезе по количеству зарегистрированных преступлений за 2020 год, совершенных гражданами СНГ и иностранцами, в Республике Казахстан представляются следующие данные: г. Нур-Султан – 52 граждане СНГ, 25 иностранцы; Акмолинская область – 41 граждане СНГ, 10 иностранцы; Актюбинская область – 47 граждане СНГ, 1 иностранцы; г. Алматы – 275 граждане СНГ, 38 иностранцы; Алматинская область – 199 граждане СНГ,12 иностранцы; Атырауская область – 47 граждане СНГ, 12 иностранцы; Восточно-Казахстанская область – 47 граждане СНГ, 1 иностранцы; Жамбылская область – 110 граждане СНГ, 13 иностранцы; Западно-Казахстанская – 66 граждане СНГ, 2 иностранцы; Карагандинская область – 73 совершено гражданами СНГ, 4 иностранными гражданами [1].

В Российской Федерации, регионы с наибольшими показателями по количеству совершенных преступлений иностранными гражданами и апатридами за 2020 год, регионы располагаются следующим образом: Челябинская область – 651; Ростовская область – 667; Самарская область – 717; Свердловская область – 839; Краснодарский край – 887; Республика Крым – 945; г. Санкт-Петербург-2469; Московская область – 4690; г. Москва – 6118 преступлений [2].

Анализируя вышеизложенные данные, приходим к выводу, что основная доля преступлений, субъектами которых являются иностранные граждане и апатридами, совершается в крупных населенных пунктах. Возможности столичного города, развитая инфраструктура, возможность затеряться в условиях мегаполиса, служат факторами миграционной привлекательности.

В 2016 году в Республике Казахстан совершено 2 844 преступления гражданами СНГ, 222 преступления иностранными лицами (прирост составил +8,2% в сравнении с 2015 годом); в 2017 году совершено 3077 преступлений гражданами СНГ, иностранными лицами совершено 219 преступлений (-1,4% в сравнении с 2016 годом); в 2018 году 3067 преступлений совершено гражданами СНГ, иностранными лицами – 171 преступление (-21,9 в сравнении с 2015 годом); в 2019 году – 2204 гражданами СНГ, иностранными гражданами – 118 преступлений (-25,5 в сравнении с 2018 годом); в 2020 году – 1642 гражданами СНГ, иностранцами совершено – 146 преступление (+23,7 по сравнению с 2019 годом) [1].

В Российской Федерации структура преступности иностранцев и лиц без гражданства выглядит следующим образом: в 2020 году – 31 693 преступления (-2,1% в сравнении с 2019 годом), в 2019 году – 34 917 преступления (-9,54 по сравнению с 2018 годом), в 2018 году – 38 598 преступлений (-6,0% в сравнении с 2017 годом), 2017 год – 41 047 преступлений (-6,6% в сравнении с 2016 годом), в 2016 году совершено – 43 933 преступления (-8,9 в сравнении с 2015 годом) [2].

Согласно зарегистрированным преступлениям иностранцев и лиц без гражданства, значительная часть преступлений совершается выходцами из стран СНГ, как было отмечено.

Кроме того, статистическая информация о преступлениях, регистрируется без учета латентной преступности, которая составляет большую часть в удельном весе преступности по всем видам преступлений.

Проанализировав состояние миграционной преступности в Российской Федерации и Республике Казахстан, можно сделать вывод о том, что усиление визового режима для стран СНГ является одной из необходимых мер, направленных на ужесточение миграционного контроля и обеспечение национальной безопасности стран. Движущиеся миграционные потоки, с учетом турбулентности политической обстановки, наплыв беженцев и нелегальных мигрантов, свидетельствуют о необходимости усиления технической оснащенности государственных границ, создания единого международного информационного миграционного пространства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Комитет по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан. Электронный ресурс: https://www.gov.kz/memleket/entities/pravstat

2. Портал правовой статистики Генеральной прокуратуры Российской Федерации. Электронный ресурс: http://crimestat.ru/offenses_chart

Бабченко А.И.
курсант 3 курса 191 учебного взвода
Московского областного филиала Московского университета
МВД Росии имени В.Я. Кикотя,

Babchenko A.I.
3st year cadet of the group 191
of the Moscow region brunch of the Moscow University
of the MIA of Russia named after V. Ya. Kikot',

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПРОБЛЕМЫ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ

ARTIFICIAL INTELLIGENCE: PROBLEMS INTERNATIONAL LAW REGULATION

Аннотация: В статье анализируется проблема правового регулирования деятельности искусственного интеллекта. Актуальность рассмотрения проблемы обусловлена активным развитием сферы робототехники при условии недостаточной правовой базы для их регулирования.

Abstract: The article analyzes the problem of legal regulation of artificial intelligence. The urgency of examining the problem is active development of the field of robotics, provided there is insufficient legal basis for their regulation.

Ключевые слова: искусственный интеллект, «умный робот», автономные системы, правовое регулирование, субъект права, ответственность, электронная личность.

Key word: artificial intelligence, «smart robot», autonomous systems, legal regulation, subject of law, responsibility, electronic personality.

«Искусственный интеллект – тот случай, когда нужно быть достаточно дальновидными в вопросах регулирования, иначе может оказаться слишком поздно» – И. Маск, генеральный директор Tesla. Актуальность умозаключения И. Маска не подвергается сомнению, т. к. в настоящее время случаи причинения вреда жизни и здоровью людей уже известны на практике:

– в 2018 г. в штате Аризона беспилотное такси Uber сбил женщину, переходившую дорогу в ночное время суток. Женщине был причинен тяжкий вред здоровью, от которого она скончалась в больнице [5];

– в 2020 году произошло нападение самоуправляемого дрона на члена национальной армии, в результате чего военнослужащий погиб [6].

Данные случаи не единственные в мировой истории, однако до сих пор достаточная правовая база для регулирования случаев причинения вреда людям искусственным интеллектом отсутствует как в отдельных государствах, так и на международном уровне.

Первой попыткой международного урегулирования деятельности искусственного интеллекта стала конференция в Азиломаре (2017 г.), в ходе которой были приняты основные положения, касающиеся искусственного интеллекта, которые получили название Азиломарские принципы. К ним относятся: предотвращение гонок, безопасность, человеческие ценности, свобода и неприкосновенность частной жизни, человеческий контроль, общее благополучие и т. д. [4].

Среди принципов нашел свое отражение и принцип ответственности за деятельность искусственного интеллекта, который закрепляет, что ответственность за последствия

неправильного использования искусственного интеллекта лежит полностью на создателях таких систем.

С учетом возможностей современных автономных роботов такой подход является не объективным, т. к. искусственный интеллект способен анализировать и принимать решения без помощи человека (пользователя, создателя).

В Резолюции 2015/2103(INL) Civil Law Rules on Robotics (Гражданское право в области робототехники) (далее – Резолюция), принятой Европейским парламентом, был предложен подход рассмотрения искусственного интеллекта как субъекта права.

В п. 59 Резолюции написано: «Призывает Комиссию при проведении оценки воздействия ее будущего законодательного документа изучить, проанализировать и рассмотреть последствия всех возможных правовых решений, таких как: создание определенного правового статуса для роботов в долгосрочной перспективе, чтобы, по крайней мере, самые сложные автономные роботы могли быть признаны имеющими статус электронных лиц, ответственных за возмещение любого ущерба, который они могут причинить, и, возможно, применение электронной личности в случаях, когда роботы принимают автономные решения или иным образом взаимодействуют с третьими сторонами независимо» [1].

Резолюция предлагает наделить «интеллектуального робота» такими характеристиками как: «приобретение автономности с помощью датчиков и/или путем обмена данными со своей средой (взаимное подключение), а также обмен и анализ этих данных; самообучение на основе опыта и взаимодействия (необязательный критерий); по крайней мере, незначительная физическая поддержка; адаптация его поведения и действий к окружающей среде; отсутствие жизни в биологическом смысле» [1].

Таким образом, предполагается наделить статусом электронной личности не любого «умного робота», а лишь самые сложные автономные системы.

Отдельные страны, такие как Китай, США, Южная Корея и др., активно разрабатывают собственную политику в области правового регулирования «умных роботов».

В Южной Корее в 2008 г. был утвержден Закон № 9014 «О содействии развитию и распространению умных роботов». В данном Законе закреплено понятие «умный робот» – «механическое устройство, которое самостоятельно воспринимает внешнюю среду, распознает обстоятельства, в которых работает, и движется самостоятельно» [2].

Принятый в Южной Корее Закон предполагает дальнейшее развитие этой сферы права. В нем утверждается обязанность разработки и распространения нового закона, который бы регламентировал нормы морали в развитии робототехники. В Южной Корее этим нормативным правовым актом должна стать Хартия этики умных роботов.

В США разработали «Thenationalartificialintelligenceresearchanddevelopmentstrategicplan» (Национальный стратегический план исследований и разработок в области искусственного интеллекта), которым утверждено развитие сферы искусственного интеллекта по семи направлениям:

1. Создание долгосрочных инвестиции в исследования искусственного интеллекта.
2. Разработка эффективных методов сотрудничества человека и искусственного интеллекта.
3. Понимание и решение этических, правовых и социальных проблем.
4. Обеспечение безопасности и защиты систем искусственного интеллекта.
5. Разработка общих общедоступных наборов данных и сред для обучения и тестирования искусственного интеллекта.
6. Измерение и оценивание технологии искусственного интеллекта с помощью стандартов и критериев.
7. Анализ национальных потребностей в кадрах для исследований и разработок в области искусственного интеллекта [3].

Не только законодатели всех стран пытаются урегулировать сферу робототехники, но и мировые компании. Например, компания «Майкрософт» выпустила в 2018 г. книгу «The Future Computed: Artificial Intelligence and its role in society» (Компьютер будущего: Искусственный интеллект и его роль в обществе), в которой предложила следующие принципы работы искусственного интеллекта: «справедливость, надежность и безопасность, тайна личной жизни и приватность, всесторонность, прозрачность, подконтрольность». «Майкрософт» считает, что, базируясь и соблюдая эти принципы, искусственный интеллект сможет стать частью любого продукта и сервиса, которые люди будут использовать как на работе, так и дома каждый день.

«Майкрософт» утверждает, что правильное проектирование «умных роботов» будет способствовать принятию более справедливого решения, потому что компьютер являются чисто логической и, теоретической системой, которая не подвержены сознательным и бессознательным предубеждениям, влияющим на принятие решений человеком. Так же компания предложила ввести «клятву Гиппократа» для программистов.

Таким образом, страны всего мира, а также крупные компании иностранных государств разрабатывают предложения по регулированию деятельности искусственного интеллекта. Активно идет создание научных основ функционирования искусственного интеллекта, на основании которых в дальнейшем будут разрабатываться нормативные правовые акты.

Проблема правового регулирования деятельности искусственного интеллекта непосредственно связана с проблемой привлечения к ответственности за вред, причиненный искусственным интеллектом. В настоящее время можно выделить следующие подходы к рассмотрению данной проблемы:

1. Искусственный интеллект как юридическое лицо, т. к. юридическое лицо является искусственно созданным субъектом права. Такого подхода придерживаются В.В. Архипов, В.Б. Наумов и ряд других ученых. В российском уголовном праве искусственный интеллект как юридическое лицо не сможет быть привлечено к уголовной ответственности, т. к. ответственность за преступную деятельность юридического лица несут руководитель, сотрудники и иные лица, участвующие в совершении преступления.

2. Искусственный интеллект как животное. Однако нормы к животным не смогут быть применены полностью относительно роботов. Российское уголовное право не допускает аналогию его применения, т. е. для привлечения робота к уголовной ответственности необходимо разработать отдельную совокупность норм. Еще одним препятствием применения этих норм является то, что они введены для домашних животных, которые в обычных условиях не должны причинять вред.

3. Ответственность конкретных лиц, которые должны были предвидеть причинение вреда искусственным интеллектом. К таким лицам можно отнести: создателя, пользователя, продавца либо лицо, которое умышленно использовало искусственный интеллект в целях совершения преступления.

4. Искусственный интеллект как электронная личность, т. е. искусственный интеллект самостоятельно несет ответственность за совершенные им противоправные деяния.

Таким образом, международное законодательство, как и законодательство отдельных стран находится на начальном этапе своего развития. Сейчас перед законодателями всех государств остро стоит проблема ответственности за противоправные деяния искусственного интеллекта.

Наиболее актуальным подходом является рассмотрение искусственного интеллекта с точки зрения самостоятельного субъекта права. Однако такой подход требует детальной разработки и законодательного закрепления (квалификация деяний искусственного интеллекта; меры наказания, применяемые к искусственному интеллекту и т. д.).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Резолюция Европейского парламента от 16 февраля 2017 года с рекомендациями Комиссии по нормам гражданского права в области робототехники (2015/2103(INL)) // Европейский Парламент: сайт. – Режим доступа: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (Дата обращения: 14.11.2021).
2. Закон о содействии развитию и распространению умных роботов № 9014 от 28.03.2008 (ред. от 06.01.2016) // Проект «Робоправо»: сайт. – Режим доступа: https://robopravo.ru/zakon_iuzhnoi_koriei_2008 (Дата обращения: 16.11.2021).
3. Национальный стратегический план исследований и разработок в области искусственного интеллекта // Flia: сайт. – Режим доступа: https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf (Дата обращения: 19.11.2021).
4. Азиломарские принципы искусственного интеллекта // Проект «Робоправо»: сайт. – Режим доступа: https://robopravo.ru/azilomarskiie_printsipy_ii (Дата обращения: 16.11.2021).
5. В США предъявили обвинения оператору беспилотного автомобиля Uber, насмерть сбившего женщину // LIFE: сайт. – Режим доступа: https://life.ru/p/1345533 (Дата обращения: 15.11.2021).
6. Дрон под управлением искусственного интеллекта впервые в истории убил человека // MKRU: сайт. – Режим доступа: https://www.mk.ru/incident/2021/05/31/dron-pod-upravleniem-iskusstvennogo-intellekta-vpervye-v-istorii-ubil-cheloveka.html (Дата обращения: 10.11.2021).

Болотина О.Р.
курсант 3 курса 191 учебного взвода
Московского областного филиала Московского университета
МВД России имени В.Я. Кикотя,

Bolotina O.R,
3st year cadet of the group number 191
of the Moscow regional brunch of the Moscow University
of the MIA of Russia named after V. Ya. Kikot',

ФЕНОМЕН «КИБЕРБУЛЛИНГА» И «БУЛЛИНГА» В РОССИИ: АНАЛИЗ ПОДХОДОВ К ОПРЕДЕЛЕНИЮ

THE PHENOMENON OF «CYBERBULLING» AND «BULLING» IN RUSSIA: ANALYSIS OF APPROACHES TO DETERMINING

Аннотация: В данной статье был проведен анализ подходов к определению таких понятий как «кибербуллинг» и «буллинг» в России.

Abstract: This article analyzes approaches to the definition of such concepts as «cyberbullying» and «bullying» in Russia

Ключевые слова: Кибербуллинг, булиинг, травля в школах.

Keywords: Cyberbullying, bullying, bullying in schools.

Одной из самых, пожалуй, распространенных на сегодняшний день проблем является травля детей сверстниками, которая значительно увеличивает риск совершения суицида среди молодежи, приводит к повышению уровня насилия и агрессии, влияет на успеваемость и взаимоотношения в коллективе [6, с. 175].

Если эти деяния совершаются посредством информационно-телекоммуникационной сети «Интернет», то стоит говорить уже о «кибербуллинге» или «хейтерстве». Обратившись к буквальному переводу данного термина, мы убедимся, что он тоже заимствован, за основу взято слово опять же из английского языка «hate» – ненавидеть, ненависть [4, с. 154].

Под буллингом понимается регулярное психологическое или физическое давление на человека, которое может проявляться в качестве угрозы, оскорбления, издевательства, шантажа, а также избиения потерпевшего. Буллинг не является поведением в стандартном понимании, а является особой формой разрушительного взаимодействия, включающего в себя множество специфических типов и подтипов агрессивного поведения. В переводе с английского языка «bullying» означает запугивание, травлю, или агрессивное преследование одного из членов коллектива [4, с. 156]. По мнению многих авторов, в частности Р.В. Агушевой, «под травлей подразумевается систематическое психологическое или физическое давление на жертву, это могут быть угрозы, оскорбления, насмешки и прочее» [1, с. 338].

Разберем основные, существующие в науке определения и подходы к проблеме буллинга, представив их в таблице 1.

Указанные в таблице характеристики позволяют понять разницу между буллингом и случайными конфликтами, дракой и ссорой, которые иногда происходят между людьми. Буллинг в большей степени отличается наличием специфических характеристик: длительность, асимметричность сил жертвы и обидчика, типы участников ситуации закреплены (преступник, жертва, свидетель, помощник буллера, защитник жертвы), преступник обладает правами, а жертва не имеет собственной позиции и не предпринимает в основном никаких действий для

того, чтобы защитить себя. В конфликтной же ситуации обе стороны отстаивают свои позиции и в процессе участники могут сменяться.

Таблица 1

Основные подходы к определению буллинга

Автор	Определение
Роланд (1988)	Атаки разного характера
Таттум (1989)	Психологическое и/или физическое насилие над индивидуумом, который не может себя защитить в такой ситуации. Насилие со стороны отдельного человека или же группы людей обычно довольно продолжительное.
Безаг В. (1989)	Регулярные нападения (социальные, физические, психологические, словесные) со стороны человека, превосходящего по силе или группы лиц с целью причинения страданий и достижения тем самым собственного удовлетворения.
Ольвеус Д. (1991)	Физическое насилие или угрозы в сторону слабого, бессильного человека. Это особый вид насилия, который запугивает индивидуума и заставляет чувствовать изолированным и лишенным свободы действия на протяжении долгого времени.
Хед (1994)	Психологическое и/или физическое насилие над индивидуумом, который не в состоянии себя защитить в этой ситуации. Насилие со стороны отдельного человека или же группы людей обычно довольно продолжительное и мотивированно желанием причинения боли, стресса.
Хальцер (1996)	Неоднократное проявление доминирующего поведения со стороны нападающего в отношении жертвы.
Кривцова С.В. (2011)	Одни несовершеннолетние агрессируют против других. При этом характерно неравенство сил и неоднократность, что является одними из главных признаков буллинга.

Главные характеристики буллинга:

1. Неоднократный и/или периодичный.
2. Умышленный.
3. Наносящий вред.
4. Злоупотребляющий силой или влиянием [2, с. 128].

Смежные буллингу понятия:

1. Моббинг – слухи, сплетни, жесткие и непристойные шутки, высмеивание и обзывательства.
2. Кибертравля – угрозы, оскорбления в форме писем/сообщений/комментариев, публикация и распространение личной информации.
3. Виктимблейминг – обвинение человека, который находится под давлением и перекладывание на него всей ответственности.
4. Харассмент – сексуальные домогательства.
5. Сталкинг – назойливое внимание, постоянное преследование жертвы в реальной и виртуальной жизни.
6. Хейзинг – обряд инициации (дедовщина).
7. Аутинг – публичное разглашение компрометирующей жертву информации о сексуальной ориентации или гендерной идентичности [2, с. 191].

В России выделяют следующие виды:

— эмоциональное насилие – доведение до эмоционального напряжения жертвы, унижение и снижение его самооценки, основным средством воздействия является голос обидчика (распространены прозвища, записки, предвзятые оценки, издевательства, унижения в присутствии других детей и т. д.). Такой вид актуален для детей, отличающихся от большинства, например, имеющих акцент, дефекты речи, низкий уровень интеллекта;

— физическое насилие (сопровождающееся эмоциональным) – причинение телесных повреждений (поведение, характерное для мужского пола);

— сексуальное насилие или совращение – использование несовершеннолетнего взрослым или другим подростком для удовлетворения сексуальных потребностей или получения выгоды;

— экономическое насилие – контроль над другим человеком при помощи денежных средств. Жертва может быть принуждена к кражам с целью обвинения ее в этих действиях [3, с. 301].

Факторы, влияющие на проявление буллингового поведения:

— личные факторы – отсутствие воспитания, заниженная/ завышенная самооценка и излишняя эмоциональность;

— факторы поведения – мешающее другим людям поведение, вандализм, прогулы и низкая успеваемость в учебном заведении, ранние сексуальные контакты, ранняя судимость;

— социальные факторы – влияние СМИ, культ насилия в обществе, поведение родителей, люди в круге общения с отклоняющимся поведением.

— конфликты внутри семьи;

— проблемы в жизни – наступление фазы полового созревания и связанные с этим проблемы физиологического и психологического характера [3, с. 182]

— Кроме вышеперечисленных факторов, буллинговое поведение может проявиться по причинам: неудовлетворяющей внешности, манер нестандартно одеваться, диалекта, высокой физической силы, страха, тревожности, депрессии, заболеваний опорно-двигательного аппарата и низкой/высокой популярности. С точки зрения личных проблем мотивами могут быть: месть, зависть, неприязнь и борьба за власть.

Таким образом, исходя из изложенной выше информации, можно сделать вывод, что буллинг – это форма деструктивного межличностного взаимодействия. Человек или группа осознанно выступают в качестве обидчика, а другая жертва, которая явно слабее умственно или физически, долгосрочно и систематически подвергается физическому, психологическому, эмоциональному насилию и агрессии.

Как показывают многочисленные зарубежные исследования, на данный момент проблема травли актуальна во всем мире. Стоит отметить, что в России данная проблема также существует, но на нее, к сожалению, не обращают должного внимания. Всемирная организация здравоохранения провела исследование кибербуллинга в 2009–2010 гг., 2013–2014 гг. в отношении несовершеннолетних, в возрасте 11–15 лет. Результаты такого исследования показали, что Россия занимает лидирующие позиции. Каждый пятый ребенок становился жертвой буллера. По данным исследования РОЦИТ, проведенного в 2017 году, жертвой кибербуллинга стал каждый второй подросток [4, с.156].

В обществе уже давно высказываются предложения относительно внесения отдельной статьи в уголовное законодательство Российской Федерации, предусматривающую ответственность за травлю (буллинг) или же отдельном федеральном законе – по примеру Украины. Кодекс Украины об административных правонарушениях дополнен статьей 173-4, раскрывающей понятие «буллинга», а также ответственность за указанное деяние. В законе «Об образовании» предусмотрели типичные признаки буллинга (травли). А также расширили права и обязанности участников образовательного процесса [8].

В Российской Федерации работа пока ведется не на должном уровне. Из средств массовой информации поступают сообщения о том, что в Государственной думе поддержали идею

введения уголовной ответственности за буллинг в сети Интернет. Якобы уже подготовлен важный законопроект, который должны были внести на рассмотрение [9]. Но, к сожалению, ознакомиться с ним нам не удалось. По версии тех же средств массовой информации со ссылкой на инициаторов данного законопроекта, предлагается ввести административные штрафы за угрозы, шантаж, издевательства, размещение в сети сцен побоев с участием детей. В КоАП РФ планируют ввести новую статью – «Унижение человеческого достоинства несовершеннолетних». За те же нарушения, которые совершаются систематически, могут установить уголовную ответственность и дополнить УК РФ двумя новыми статьями о наказании за систематическую травлю детей и за организацию публичного кибербуллинга в Интернете и мобильных сетях [10].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Агушева В.Р. школьный буллинг: Социально-психологические причины и правовая ответственность. Евразийский Юридический журнал. Издательство: Евразийский научно-исследовательский институт проблем права (Уфа). № 9 (112) 2017.
2. Андреева Г.М. Социальная психология: учебник. – М.: Аспект Пресс, 2017.
3. Ильин Е. П. Психология агрессивного поведения: учебник. – Санкт-Петербург: Питер, 2018.
4. Раненкова Е.А. Проблемы борьбы с буллингом и скулшутингом: совершенствование уголовного законодательства Российской Федерации. В сборнике: Актуальные проблемы уголовного законодательства на современном этапе. сборник научных трудов Международной научно-практической конференции. 2020. С. 151-156.
5. Раненкова Е.А., Шемчук С.Ю. К вопросу защиты жизни детей в российских школах. В сборнике: Уголовно-правовая охрана конституционных прав и свобод граждан, суверенитета и территориальной целостности Российской Федерации. сборник научных трудов Международной научно-практической конференции. Москва, 2021. С. 272-276.
6. Флерова А.Д., Раненкова Е.А. Основные направления профилактики буллинга среди несовершеннолетних в образовательных организациях. В сборнике: Уголовное судопроизводство по делам несовершеннолетних и ювенальная юстиция: проблемы и перспективы развития (правовые, социальные и психолого-педагогические аспекты). Сборник статей научно-представительских мероприятий. Коллектив авторов. 2021. С. 175-178
7. Шемчук С.Ю. От травли до расстрела: как предотвратить насилие в образовательных организациях. В сборнике: Уголовное судопроизводство по делам несовершеннолетних и ювенальная юстиция: проблемы и перспективы развития (правовые, социальные и психолого-педагогические аспекты). Сборник статей научно-представительских мероприятий. Коллектив авторов. 2021. С. 187-190.
8. Рада ввела ответственность за буллинг: за травлю будут жестко штрафовать. Электронный ресурс [URL: https://www.segodnya.ua/]. Режим доступа: https://www.segodnya.ua/ukraine/rada-vvela-otvetstvennost-za-bulling-za-travlyu-budut-zhestko-shtrafovat-1199139.html (дата обращения: 19.09.2021).
9. Травля под статьей. Электронный ресурс [URL: https://rg.ru/]. Режим доступа: https://rg.ru/2020/08/10/zakonoproekt-o-borbe-s-travlej-v-seti-vnesut-v-gosdumu-oseniu.html (дата обращения 20.09.2021).
10. Что грозит за травлю в Интернете? Электронный ресурс [URL: https://zen.yandex.ru/]. Режим доступа:https://zen.yandex.ru/media/lawyer_secret/chto-grozit-za-travliu-v-internete--5f34e3b9e3b4966301ef6ddc (дата обращения 20.09.2021).

Бородин М.С.
Курсант 4 курса прокурорско-следственного факультета
ФГКОУВО ВУМОРФ

Borodin M.S.
Fourth-year cadet of prosecuting and investigating faculty
of the Military University of the Russian Defense Ministry

УГОЛОВНОЕ ПРАВО В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ИЛИ КАК ПРОТИВОДЕЙСТВОВАТЬ КИБЕРПРЕСТУПНОСТИ

CRIMINAL LAW IN THE ERA OF DIGITAL TRANSFORMATION OR HOW TO COUNTER CYBERCRIME

Аннотация. В статье рассмотрен ряд проблем, возникающих при совершении преступлений в сфере информационных технологий. Проанализированы положения законодательства и примеры из судебной практики. С опорой на научную литературу и правоприменительную практику сформулирована авторская позиция по поставленным вопросам.

Annotation. The article considers a number of problems that arise when committing crimes in the field of information technology. Provisions of the legislation and examples from judicial practice are analyzed. Based on scientific literature and law enforcement practice, the author's position on the issues raised is formulated.

Ключевые слова: кибепреступность, информационные технологии, мошенничество, криптовалюта.

Keywords: cybercrime, information technology, fraud, cryptocurrency.

Цифровая революция не только принесла пользу экономике и социуму, но и открыла для криминалитета новые способы совершения преступлений – с использованием IT-технологий. Согласно данным официальной статистики, за прошедший год зарегистрировано более 294 тысяч преступлений, совершенных с использованием информационно-телекоммуникационных технологий – на 70% больше, чем в 2018 году. При этом рост статистического трафика налицо – за январь-сентябрь текущего года с применением IT-технологий совершено на 77% больше деяний – по сравнению с аналогичным периодом 2019 года.

При анализе вышеуказанных показателей необходимо учитывать, что категория «киберпреступность» не сводится к деяниям, предусмотренным главой 28 Уголовного кодекса РФ, а представляет собой широкий пласт преступлений, в частности против личности, экономики и общественной безопасности, где обязательным элементом подготовки, совершения или сокрытия выступают информационные технологии.

Криминальный IT-скачок не мог остаться без внимания со стороны правоохранительных органов. Так, в конце прошлого года в структуре Главного следственного управления Следственного комитета РФ и в системе Министерства внутренних дел РФ созданы подразделения по расследованию киберпреступлений и преступлений в сфере высоких технологий. Формирование специализированных структур – необходимый шаг для борьбы с киберпреступлениями, характеризующимися трансграничностью и неочевидностью. Благодаря их созданию появляется возможность улучшить качество расследования киберпреступлений – за счет организационного обособления следственных подразделений. Это обусловлено не только ростом количества совершаемых преступлений, но и продиктовано спецификой рассматриваемой категории дел, которая требует определенного набора профессиональных знаний и умений. Следователи сформированных подразделений смогут не только

сконцентрироваться на расследовании IT-криминала, но и получить возможность к прохождению соответствующей подготовки, которая необходима как для установления обстоятельств произошедшего преступления – криминалистическая и процессуальная составляющие, так и для безукоризненной квалификации криминального события – материальный аспект.

Ситуация с киберпреступностью осложняется широкомасштабным распространением коронавируса, последовавшим за ним экономическим упадком и информационной изоляцией (удаленная работа, сокращение штата и финансовый кризис) отличная почва для IT-криминала. Сложившаяся обстановка требует принятия мер государственного реагирования, в том числе средствами уголовно-правового воздействия. Далее рассмотрим актуальные проблемы, связанные с киберпреступностью, – мошенничество, «пробив» и электронные кошельки.

Хищения перешли в онлайн как следствие развития информационных технологий. Отсутствие физического контакта между преступником и потерпевшим не только облегчает совершение преступления, но и позволяет скрыть следы криминальной активности. В условиях коронавирусной пандемии поле деятельности для злоумышленников расширилось: продажа фейковых цифровых пропусков, направление несуществующих штрафов и т. д. Традиционные для новой эры способы дистанционных хищений: фишинг и вишинг, – также активно используются преступниками.

При квалификации конкретных фактических обстоятельств необходимо провести четкую линию демаркации между различными формами посягательств против собственности. Как известно, хищения могут совершаться в различных формах, в том числе мошенничества и кражи. Применительно к цифровой сфере в законодательстве и практике имеется ряд спорных моментов.

Так, мошенничество совершается путем обмана или злоупотребления доверием. Согласно п. 2 постановления Пленума Верховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» под обманом как способом совершения хищения или приобретения права на чужое имущество может состоять в сознательном сообщении (представлении) заведомо ложных, не соответствующих действительности сведений, либо в умолчании об истинных фактах, либо в умышленных действиях, направленных на введение владельца имущества или иного лица в заблуждение. При этом злоупотребление доверием при мошенничестве заключается в использовании с корыстной целью доверительных отношений с владельцем имущества или иным лицом, уполномоченным принимать решения о передаче этого имущества третьим лицам (п. 3 постановления Пленума ВС РФ № 48).

Исходя из рекомендаций высшей судебной инстанции, следует заключить, что при мошенничестве виновный воздействует на психику потерпевшего – с целью получения имущества или приобретения права на имущество. Иными словами, при мошенничестве имущество или право на имущество выводятся из сферы законного владения за счет непосредственного или опосредованного контакта между виновным и потерпевшим.

Несмотря на аксиоматичность вышеприведенного положения, законодательство не всегда отвечает духу уголовного права и стандартам юридической техники в данном отношении. В 2012 году УК РФ дополнен новым видом мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ). Думается, что с позиций теории уголовного права и рекомендаций высшей судебной инстанции данное преступление не является мошенничеством [1, с. 64], поскольку хищение совершается не путем воздействия на психику потерпевшего, а посредством «вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей». Как указано в постановлении Пленума ВС РФ № 48, под вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей понимается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим

программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него (п. 20). Как мы видим, в данном случае отсутствует связка «человек-человек», а хищение совершается исключительно путем IT-манипуляций с информацией. По нашему мнению, мошенничество в сфере компьютерной информации не обладает ключевым признаком рассматриваемой формы хищений, а является самостоятельным преступлением, посягающим на собственность.

В то же время за последние годы сформировалась судебная практика по применению ст. 159.6 УК РФ. Особый интерес вызывает вопрос о необходимости дополнительной квалификации данного преступления по совокупности с деяниями, закрепленными в гл. 28 УК РФ. Так, Советским районным судом г. Томска подсудимый признан виновным в совершении преступлений, предусмотренных ч. 4 ст. 159.6, ч. 2 ст. 273 УК РФ, при следующих обстоятельствах. Курочкин Р.Ю. для хищения денежных средств граждан со счетов карт Сбербанк России совершал рассылку SMS-сообщений, в которых содержалась ссылка для загрузки вредоносных программ, предназначенных для удаленного управления устройством пользователя. Получив данные о мобильном устройстве, злоумышленники формировали команду с абонентского номера зараженного сотового телефона SMS-сообщения, содержащего информацию о переводе денежных средств в определенной сумме, на сервисный номер «900» SMS-сервиса «Мобильный банк» ОАО «Сбербанк России». В результате денежные средства попадали на подконтрольный Курочкину Р.Ю. банковский счет, а затем выводились на электронные кошельки «Bitcoin» и «QIWI» (дело № 1-275/2018).

Следует заметить, что для совершения хищений в режиме «онлайн» у злоумышленников должен быть минимальный пакет информации о предполагаемой жертве. В этих целях преступники нередко пользуются услугами «пробива» (если самостоятельно не являются их поставщиками). Суть «пробива» заключается в деятельности по сбору и анализу информации о конкретной личности или организации – как из открытых источников, так и посредством неправомерного доступа к персональным данным или иной охраняемой законом тайне. Сейчас на просторах Telegram существует большое количество каналов, где интересанты могут приобрести полный комплект информации о персоне – от паспортных данных и номера сотового телефона до сведений о банковских счетах. Такая обширная информационная база создает плацдарм для криминальной деятельности во многих общественных сферах, связанных с конфиденциальными сведениями.

При наличии предусмотренных уголовным законом условий деятельность «пробивщиков» может быть квалифицирована в соответствии с тремя статьями УК РФ – ч.2 ст.137 (Нарушение неприкосновенности частной жизни, совершенное лицом с использованием своего служебного положения), ч.2 ст.138 (Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан, совершенные лицом с использованием своего служебного положения), ч.ч. 2-4 ст.183 УК РФ (Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну). Несмотря на обширное уголовно-правовое покрытие, требуется усиление процессуальной и оперативной активности в части противодействия незаконному обороту персональной информации.

После прохождения «информационной стадии» хищения и непосредственного его совершения злоумышленники занимаются сокрытием преступно полученных доходов. Широкой популярностью у криминалитета пользуются электронные кошельки, которые дают возможность «отмыть» похищенные денежные средства. Кроме того, электронные кошельки, в частности биткоин-платформы, стали дистанционной площадкой для совершения иных преступлений, в том числе связанных с незаконным оборотом наркотиков.

Как установлено приговором Тюменского районного суда Тюменской области, за хранение наркотических средств с целью их последующего сбыта И. получил от неустановленного лица «Биткоин код» на сумму, эквивалентную 180 тыс. руб. Далее он активировал «Биткоин код» на электронной валютной финансовой бирже – площадке BTC-e.com, тем самым зачислил на виртуальный неперсонифицированный счет электронной площадки данные денежные средства. Затем И. совершил ряд последовательных финансовых операций. Он конвертировал валюту, зачислил денежные средства на виртуальный неперсонифицированный счет, перевел их на банковскую карту на имя Л., не осведомленного о преступной деятельности И., под предлогом оплаты товара и ввел денежные средства в наличный оборот путем снятия со счета посредством банковского терминала. В общей сложности с учетом комиссий и курса валют И. легализовал е-средства на общую сумму 173 650 руб. 92 коп. (дело № 1–261/2017).

В целом современная уголовно-правовая база для противодействия киберпреступности отвечает потребностям времени и сложившейся правоприменительной практике. Однако следует признать, что специфика такого рода криминальных деяний состоит в их латентности, неочевидности и трансграничности, в связи с чем необходимо применение комплекса мер по предупреждению и ликвидации последствий преступлений в сфере IT, в частности: выработка стратегий кибербезопасности на всех уровнях, активное международное сотрудничество и приведение специального законодательства в соответствие с новейшими тенденциями в сфере информационных технологий.

Таким образом, действующее уголовное законодательство содержит необходимый регуляторный плацдарм для борьбы с киберпреступностью, для борьбы с которой необходимо усилить организационный, оперативный и процессуальный арсенал правоохранительных органов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Русскевич Е.А. Разъяснения Пленума ВС РФ о квалификации мошенничества в сфере компьютерной информации // Уголовный процесс. 2018. № 2. С. 63-69.

Гагарина В.М.
курсант 791 взвода 3 «Э» курса
Московского университета МВД России имени В.Я. Кикотя,

Gagarina V.M.,
3st year student of the Moscow University of the Ministry of Internal Affairs of Russia

ПРОБЛЕМА ЗАЩИТЫ ЛИЧНОСТИ ОТ НАСИЛЬСТВЕННЫХ ПРЕСТУПЛЕНИЙ

PROBLEM OF PERSONAL PROTECTION FROM VIOLENT CRIMES

Аннотация: В статье анализируется состояние криминологической обстановки насильственных действий, совершаемых против личности в мировой практике, рассматриваются основные методы и направления предупреждения данного вида правонарушений против личности. Следует отметить, что наблюдается стабильное сокращение показателей различных видов насильственных преступлений как в отечественной практике, так и на мировой арене.

Abstract: The article below analyzes the state of the criminological situation of violent acts committed against the individual in world practice, examines the main methods and directions for the prevention of this type of offenses against the individual. It should be noted that there has been a steady decline in the rates of various types of violent crimes both in domestic practice and on the world stage.

Ключевые слова: насильственные преступления, преступность, криминологическая обстановка, насильственные действия, преступления против личности

Key words: violent crimes, crime, criminological environment, violent acts, crimes against the person.

Для более полного и наглядного понимания акцентируемой темы данной статьи, первоначально, стоит разобрать понятие насильственных преступлений. Приняв за базис изучения российский и зарубежный передовой опыт в практике данного вида преступлений, можно сформулировать общее определение. Таким образом, насильственные преступления-преступления, связанные с применением силы и (или) нанесением телесных повреждений другому человеку, вопреки его желанию и воле. Вопрос серьезности совершенного насильственного преступления, как правило, определяется степенью физического вреда, причиненного жертве. Насильственные преступления влияют на общество внутри страны, на отдельные личности, затрагивают личную и сексуальную неприкосновенность и безопасность человека.

Одно из самых известных, но мало обсуждаемых в обществе насильственных преступлений, затрагивающих, преимущественно женщин – это насилие в семье или, так называемое «домашнее насилие». Согласно лекции американского профессора Лукенбилла, домашнее насилие было довольно серьезной дилеммой, которую ранее, многие боялись свободно выражать, так как в обществе было попросту не принято о таком говорить, люди боялись огласки, обсуждения со стороны других, но, на сегодняшний день, общество становится более категоричным и строгим в этом вопросе, процент граждан, замалчивающих проблему, становится меньше [1].

Со стороны американских властей также наблюдается серьезность отнесения к данному вопросу, если раньше, полиция просто появлялась на пороге, спрашивала, что случилось и покидала помещение, то сейчас, по новым законам, полиция должна арестовать подозреваемого в жестоком обращении без дальнейшего предупреждения и уведомления. Арест происходит с целью обеспечения безопасности потерпевшего от насилия супруга [2].

Что же касается России, согласно статистике МВД за 2020 год, женщины составляют 72,8 % пострадавших от насильственных действий по отношению к супругу, то есть, как раз от домашнего насилия. Из данных сведений можно сделать вывод о преимуществе доли насилия в семье относительно других видов насилия по отношению к личности. Возвращаясь к вопросу нормативного регулирования, то, на данный момент, в российской практике не существует специального закона и статьи о семейном насилии. Наиболее часто к таким ситуациям применяют статьи 111, 112, 115, 116, 119 УК РФ.

Что же делать личности для защиты себя, если она столкнется с насилием? В России существует служба спасения, в которую могут обратиться все граждане, которые столкнулись с противоправными действиями по отношению к ним, также государством были созданы различные бесплатные государственные службы психологической помощи, к примеру, вы можете обратиться в службу психологической помощи населению по номеру 8 (499) 791-20-50.

В Германии действует специальная программа помощи для пострадавших от домашнего насилия «Женские дома» «Frauenhaus», в данном заведении всем пострадавшим гарантируется защита в виде работы с психологом, также котловое, вещевое и жилищное обеспечение. Так же как и в России, существуют специальные телефоны доверия и поддержки.

С учетом вышеприведенного материала, очевидна необходимость освещения вопроса насилия в СМИ, пере смотрение и совершенствование законодательства в вопросах насилия, назначение наиболее твердого наказания для преступников, принятие законодательных актов, регулирующих такой аспект насилия, как домашнее насилие.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. https://www.legalmatch.com/law-library/article/what-are-the-different-types-of-violent-crime.html;

2. Сиба А.П. Применение мер безопасности в контексте исправления осужденных и предупреждения совершения новых преступлений // Северокавказский юридический вестник, 2015, №1.

Депутатова Н.М.
Студентка 3 курса бакалавриата
Международного юридического института,

Deputatova N.M.,
3rd year undergraduate student
International law Institute,

ПРОБЛЕМА КВАЛИФИКАЦИИ ПРИ НАРУШЕНИИ ПРАВИЛ ДОРОЖНОГО ДВИЖЕНИЯ И ЭКСПЛУАТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ АВТОПИЛОТИРУЕМЫХ, АРЕНДОВАННЫХ ТРАНСПОРТНЫХ СРЕДСТВ В ЦИФРОВУЮ ЭПОХУ

THE PROBLEM OF QUALIFICATION IN VIOLATION OF TRAFFIC RULES AND OPERATION WHEN USING AUTOPILOTED, RENTED VEHICLES IN THE DIGITAL AGE

Аннотация. В статье рассматриваются проблемы квалификации преступлений за нарушение правил дорожного движения и эксплуатации транспортных средств при использовании искусственного интеллекта в ходе беспилотного управления, арендованных транспортных средств.

Abstract. The article deals with the problems of qualification of crimes for violation of traffic rules and operation of vehicles when using artificial intelligence during unmanned control, rented vehicles.

Ключевые слова: квалификация преступления, нарушение правил дорожного движения, автопилотируемое транспортное средство, арендованное транспортное средство.

Keywords: qualification of a crime, violation of traffic rules, autopiloted vehicle, rented vehicle.

Информационно-технологический прогресс, который вызван тотальной информатизацией общества, меняет устройство действительности. Так называемая «цифра», повсеместная роботизация и автоматизация – все упомянутые термины перекраивают повседневность, делают ее максимально продуктивной и облегченной, побуждают законодателя совершенствовать установленные правовые нормы.

Автоматизированные механизмы под управлением искусственного интеллекта уже достаточно давно стали частью жизни общества, профессиональной сферы и даже личной жизни каждого, отдельного взятого человека. Новаторские проекты внедряются в области образования, промышленности – различного рода электронно-вычислительные машины, жилищной отрасли – популярная функция «умный дом» и т. п.

К технологиям современного формата относятся автотранспортные средства под управлением автопилота, которые медленно, но верно получают распространение в жизни общества.

Появление на дорогах общего пользования беспилотных транспортных средств актуализирует ряд вопросов, которые связаны с безопасностью пассажиров, других участников дорожного движения и пешеходов, в частности за возможные дорожно-транспортные происшествия с участием таких автомобилей и нанесенный ими вред. На вопрос об определении субъекта ответственности в данном случае ответить довольно непросто.

Разумеется, беспилотный автомобиль – это транспортное средство, характеризующееся повышенной опасностью. Первое ДТП с автопилотом и смертельным исходом произошло в США, когда автоматика не успела распознать опасность из-за слияния цвета предмета с ярким небом. Именно по этой причине не успел среагировать и сам водитель, вполне имевший

возможность взять управление машиной на себя. Поскольку происшествия с автопилотируемыми аппаратами имеют место, необходимо обоснование для привлечения к уголовной ответственности за допущенное дорожно-транспортное происшествие с применением беспилотного авто.

Самый основной момент заключается в конкретизации для данной ситуации формулировки основания уголовной ответственности за причинение вреда конкретным ДТП в диспозиции соответствующей нормы Уголовного Кодекса Российской Федерации [1]. Применительно к нашей теме – это статья 264 УК РФ. В рамках формулы «состава преступления» основополагающим является определение субъекта, который и понесет бремя ответственности. В точном соответствии с уголовным законом субъект вышеназванного преступления – это лицо, которое управляет транспортным средством. На ситуации – это водитель, согласно п.1.2. Правил Дорожного Движения [3], где указано: «Водитель – лицо, управляющее каким-либо транспортным средством… К водителю приравнивается обучающий вождению». Проблематика заключается в том, что в случае с автопилотом водитель де-факто отсутствует, а инженер, находящийся в салоне, таковым не является, т. к. не осуществляет управление.

12 марта 2021 года Правительством Российской Федерации был утвержден комплекс мероприятий по тестированию и поэтапному введению в эксплуатацию на общих дорогах автоматизированных транспортных средств под управлением искусственного интеллекта. 8 июня был представлен также законопроект «О высокоавтоматизированных транспортных средствах», который подготовлен Министерством Транспорта РФ. Данный документ закрепляет правила эксплуатации для автопилотных ТС, которые передвигаются по проезжей части без участия водителя. Как мы видим, проблема квалификации и определения субъекта преступления остается актуальной.

И.Н. Мосечкин, кандидат юридических наук, в своей диссертации [5] определяет ряд субъектов, «деятельность которых в сочетании с применением искусственного интеллекта, способна являться основанием для привлечения их к уголовной ответственности», относя их к числу:

1) производителя искусственного интеллекта. Соответственно, если причиной случившегося дорожно-транспортного происшествия является автопилот под управлением искусственного интеллекта и причинен вред человеку, то ответственность следует возлагать на производителя данной системы. Автор исключает квалификацию ДТП в таком случае по статье 264 УК РФ [1], т.к. сам разработчик не управлял транспортным средством, и полагает, что случившееся необходимо квалифицировать по пункту «в» части 2 статьи 238 УК РФ, т.е. как выполнение работ, не отвечающих требованиям безопасности жизни или здоровья потребителя, если они повлекли причинение смерти человеку по неосторожности.

2) продавца указанной продукции, которая оснащена искусственным интеллектом, или же производителя;

3) пользователя продукции;

4) иных лиц. К примеру, киберпреступника, осуществившего дистанционный взлом системы безопасности и кодов бортового компьютера.

Полагаем, что предложенные профессором Мосечкиным И.Н. основания для привлечения к уголовной ответственности являются основополагающими при квалификации дорожно-транспортных происшествий с участием автопилотируемых транспортных средств для практического их применения.

Также не менее важным вопросом являются столь популярные и пользующиеся спросом арендованные на короткий срок транспортные средства, так называемый «каршеринг». Он имеет как ряд своих плюсов, так и минусов. При детальном рассмотрении дорожно-транспортных происшествий с арендованными авто можно говорить об четко определенном субъекте совершенного преступления: водитель, управляющий транспортным средством и являющийся арендатором. Квалификация в случае ДТП осуществляется по статье 264 УК РФ [1]. Необходимо

четко понимать, в результате чего произошла авария – водитель не справился с управлением вследствие каких факторов? Использовал средство связи во время движения без специального устройства или все же имел место фактор технический, а именно случившаяся во время движения поломка и, к примеру, сбой в работе тормозной системы, к которому водитель никаким образом не причастен? Вопрос об определении субъекта преступления остается актуальным. В данном случае водителю необходимо оказать первую помощь пострадавшим, вызвать скорую спасательную бригаду, как указывают Правила Дорожного Движения [3], засвидетельствовать факт поломки, вызвать сотрудников ГИБДД и незамедлительно связаться с оператором, представляющим компанию-арендодателя. Если каршеринговый автомобиль попал в аварию не по вине водителя, и если виновник был установлен, то такой ущерб арендатор возмещать не обязан. В этом случае виновника произошедшего установят компетентные органы.

Подводя итог, отметим, что появление беспилотных транспортных средств и, как следствие, новых угроз безопасности человека и гражданина требует своевременного и полного отражения в системе законодательства Российской Федерации, в частности уголовного. Проблему квалификации необходимо решать принятием нормативно-правовых актов, регулирующих вопрос субъектного состава преступления.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уголовный кодекс Российской Федерации от 13.06.1996 (ред. от 01.07.2021) // Собрание законодательства Российской Федерации, 17.06.1996, №25, ст. 2954.
2. О проведении эксперимента по опытной эксплуатации на автомобильных дорогах общего пользования высокоавтоматизированных транспортных средств: Постановление Правительства Российской Федерации от 26.11.2018г. №1415 // Собрание законодательства Российской Федерации, 2018, N 49, ст. 7619
3. О Правилах дорожного движения: Постановление Правительства Российской Федерации от 23.10.1993 №1090 (ред. От 31.12.2020) // Собрание актов Президента и Правительства Российской Федерации, 22.11.1993, №47, ст. 4531.
4. Об утверждении состава и порядка представления собственником высокоавтоматизированного транспортного средства отчетности в испытательную лабораторию в ходе проведения эксперимента по опытной эксплуатации на автомобильных дорогах общего пользования высокоавтоматизированных транспортных средств и по его итогам:Приказ Минпромторга России от 08.06.2021 №2087 (зарегистрировано в Минюсте России 14.09.2021 №64995// Официальный интернет-портал правовой информации (www.pravo.gov.ru) 15.09.2021 г., N 0001202109150015.
5. Мосечкин, Илья Н. 2019. «Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления» // Вестник Санкт- Петербургского университета. Право 3: 461–476.

Казакова А.А.
курсант 3 курса 191 учебного взвода
Московского областного филиала Московского университета
МВД России имени В.Я. Кикотя,

KazakovaA.A.
3st year cadet of the group number 191
of the Moscow regional brunch of the Moscow University
ofthe MIA of Russia named after V.Ya. Kikot',

СТАТИСТИЧЕСКИЙ АНАЛИЗ МОШЕННИЧЕСКИХ ХИЩЕНИЙ, СОВЕРШАЕМЫХ ПУТЕМ ОБМАНА, ЗЛОУПОТРЕБЛЕНИЯ ДОВЕРИЯ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

STATISTICAL ANALYSIS OF FRAUD PERFORMED BY DECEPTION, BREACH OF TRUST IN THE SPHERE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Аннотация: В данной статье был проведен анализ данных о преступлениях в сфере информационно – телекоммуникационных технологий за период с 2016 года по 2021 год включительно.

Abstract: The article deals of analysis of the crime's information of the field of the information and telecommunication technologies for the period from 2016 to 2021 years.

Ключевые слова: Мошенничество; информационно – телекоммуникационные технологии; статистика преступлений; регистрация и раскрытие преступлений.

Key words: Fraud; information and telecommunication technologies; crime statistics; registration and disclosure of crimes

На начало 2021 года в России насчитывается 124 миллиона пользователей сети «Интернет». В период с 2020 по 2021 год количество пользователей в Российской Федерации увеличилось на 6,0 миллионов (+ 5,1%), а уровень проникновения интернета в России составляет 85,0% [1, с. 1].

Сеть «Интернет» богата различными ресурсами, которая предоставляет доступ к социальным сетям, информационным новостным сайтам, к сайтам банковских организаций, а также к сайтам организаций, занимающихся продажей билетов на культурно-массовые мероприятия, перевозкой пассажиров и т. д.

Из этого следует то, что у современных пользователей появляются возможности осуществлять действия в интернете посредством имеющихся там ресурсов, тем самым получать личную выгоду, так как виртуальное пространство находится под большой угрозой блокирования и проникновения в настоящее время.

В современном уголовном законодательстве к мошенничеству в сфере информационно-телекоммуникационных технологий принято относить преступления, предусмотренные ст. 159.3 УК РФ и ст. 159.6 УК РФ.

В связи с этим возникает вопрос о тщательном рассмотрении и сравнении статистических данных по мошенническим действиям, совершенным за прошедшие пять лет, а именно с 2016 года по 2021 год.

Из ежегодных отчетов ФКУ «ГИАЦ» МВД России можно увидеть статистику и динамику, а также провести анализ и составить реалистичную картину состояния преступности.

Состояние преступности за январь – декабрь 2016 года преступлений квалифицированным по ст. 159.3 УК РФ и ст. 159.6 УК РФ составляет: было зарегистрировано

208926 (4,2%) из них было раскрыто 54773 (-8,2%). Мошеннические действия за данный период составляют 9,7% [2, с. 3].

Состояние преступности за январь – декабрь 2017 года преступлений квалифицированным по ст.159.3. УК РФ и ст.159.6 УК РФ составляет: было зарегистрировано 222772 (6,6 %) из них было раскрыто 56178 (2, 6%).

Мошеннические действия за данный период составляют 10,8% [3, с. 3].

Из приведенных статистических данных за период с 2016 года по 2017 год можно увидеть то, что преступления, квалифицированные по ст. 159.3 УК РФ и ст. 159.6 увеличились на: зарегистрированные на 13846 (2,4%), раскрытые на 1405.

Но даже эти данные не дают нам полной картины, ведь здесь учитываются лишь зарегистрированные преступления, а сколько было не зарегистрированных преступлений останется вопросом.

Состояние преступности за январь-декабрь 2018 года: преступлений, квалифицированных по ст. 159.3 УК РФ и ст. 159.6 УК РФ зарегистрировано 215036 (-3,5%), из них было раскрыто 57418 (2,2%) [4, с. 7].

При сравнении данных за 2017 год и 2018 год можно безусловно заметить, что преступная деятельность в сфере мошенничества в информационных технологиях уменьшилась из количества зарегистрированных преступлений на 7736.

Состояние преступности за январь-декабрь 2019 года: преступлений, квалифицированных по ст. 159.3 УК РФ и ст. 159.6 УК РФ зарегистрировано 257187 (19,6%), из них было раскрыто 64378 (12,1%) [5, с. 31].

Данные за 2019 год смело дают возможность судить о резком скачке и увеличении преступных деяний.

Обуславливается это тем, что с каждым годом увеличивается количество разнообразных вариантов активных действий злоумышленников, ими осваиваются новые навыки и методы использования интернет-ресурсов, с помощью которых извлекается личная выгода и причиняется материальный и имущественный вред потерпевшему. Из вышесказанного следует, что сотрудникам правоохранительных органов необходимо успевать за прогрессом в области информационно-коммуникационных технологий и сферы компьютерной информации.

Пиком роста преступлений, связанных с рассматриваемым видом мошенничества можно считать 2020 год, а конкретно время распространения действий и ограничений, связанных с пандемией коронавируса. В России большая часть населения страны в этот период находилась дома и работала удаленно. Часто совершались онлайн покупки или продажи, что стало ярким поводом для еще более разработанных схем и действий злоумышленников по захвату личных данных пользователей интернет-ресурсов. Так, состояние преступности за 2020 год: зарегистрировано всего преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации 510396 (73,4%), раскрыто было 94942 (45,5%). Количество преступлений по ст. 159.3 УК РФ составляет 25820 (60,2%), а раскрыто было 8269 (72,5%). А по ст.159.6 УК РФ было зарегистрировано 761 (10,8%), а раскрыто 101 (53,0%) [6, с. 30]. По данным Генеральной прокуратуры РФ из статистических данных о преступности за январь-декабрь 2020 года зарегистрировано преступлений, совершенных с использованием или применением: сети «Интернет» – 300337; средств мобильной связи – 218739; расчетных (пластиковых) карт – 190167; компьютерной техники – 28653; программных средств – 10050; фиктивных электронных платежей – 1374 [7, с. 39]. Количество лиц, осужденных в 2020 году по ч. 1 ст. 159.3 УК РФ равен 1242, из них получили наказание в виде штрафа 178 человек. А по ч. 1 ст. 159.6 УК РФ осуждено было 3 человека и лишь 1 человек получил наказание в виде штрафа. Следовательно, можно сделать вывод о том, что самыми распространенными за приведенный период были преступления, квалифицированные по ч. 1 ст.159.3 УК РФ. [8, с. 1].

Из ежегодных отчетов ФКУ «ГИАЦ» МВД России за январь-октябрь 2021 года было зарегистрировано всего 454554 (8,1%) преступлений, а раскрыто 111628 (44,3%). По сравнению с аналогичным периодом прошлого года количество преступлений по ст. 159^3 УК РФ снизилось до 8699 (-64,6%) зарегистрированных, а раскрываемость преступлений понизилась до 548 (-92,9%). По ст. 159.6 УК РФ снижена регистрация данных преступлений до 363 (-41,0%), раскрываемость также понижена до 71 (-24,5%) преступления [9, с. 30]. Таким образом, мы наблюдаем как снижение выявляемых, так и раскрываемых преступлений в исследуемой сфере, что не может не вызывать озабоченности.

Исследование статистических показателей уровня мошенничества в сети «Интернет» и в сфере информационно-телекоммуникационных технологий позволяет сделать вывод о необходимости прилагать намного больше усилий для борьбы с ними. А с учетом того, что эти преступления относятся к категории высокотехнологичных деяний, это означает что их расследованием обязаны заниматься лица, имеющие профессиональную подготовку и знания в изучении данного вопроса. В виду того, что многие сотрудники не обладают тем опытом и знаниями, который нужен для выявления, раскрытия и расследования данных преступлений предстоит большая работа для получения ими ответствующих компетенций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Статистика интернет соцсетей в России на 2021 год // [Электронный ресурс]: [https://www.web-canape.ru]. URL: https://www.web-canape.ru/business/internet-i-socseti-v-rossii-v-2021-godu-vsya-statistika/ Дата обращения (23.11.2021).
2. Состояние преступности России МВД РФ ФКУ «Главный информационно-аналитический центр» // [Электронный ресурс]:[https://мвд.рф/reports/item/9338947/]. URL: https://мвд.рф/reports/item/9338947/ Дата обращения (25.11.2021).
3. Состояние преступности России МВД РФ ФКУ «Главный информационно-аналитический центр» // [Электронный ресурс]: [https://мвд.рф/reports/item/16053092/]. URL:https://мвд.рф/reports/item/16053092/Дата обращения (25.11.2021).
4. Состояние преступности России МВД РФ ФКУ «Главный информационно-аналитический центр» // [Электронный ресурс] : [https://мвд.рф/reports/item/19412450/]. URL: https://мвд.рф/reports/item/19412450/ Дата обращения (26.11.2021).
5. Состояние преступности России МВД РФ ФКУ «Главный информационно-аналитический центр» // [Электронный ресурс]: https://мвд.рф/reports/item/22678184/]URL: https://мвд.рф/reports/item/22678184/ дата обращения (27.11.2021).
6. Состояние преступности в России Генеральная прокуратура РФ (Главное управление правовой статистики и информационных технологий)// [Электронный ресурс]:[https://d-russia.ru/wp-content/uploads/2021/02/december.pdf]URL:https://d-russia.ru/wp-content/uploads/2021/02/december.pdf Дата обращения (28.11.2021).
7. Судебная статистика РФ //[Электронный ресурс]:[http://stat.апи-пресс.рф/stats/ug/t/14/s/17]URL:http://stat.апи-пресс.рф/stats/ug/t/14/s/17 Дата обращения (28.11.2021).
8. Состояние преступности России МВД РФ ФКУ «Главный информационно-аналитический центр» // [Электронный ресурс]:[https://мвд.рф/reports/item/27024130/] URL: https://мвд.рф/reports/item/27024130/ Дата обращения (28.11.2021).

Козьмин В.В.,
Студент 3курсабакалавриата
Международного юридического института,

Kozmin V. V.,
3rd year undergraduate student
International law Institute,

КЛЕВЕТА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ И ПУТИ ИХ РЕШЕНИЯ

DEFAMATION USING INFORMATION DIGITAL TECHNOLOGIES: QUALIFICATION PROBLEMS AND WAYS TO SOLVE THEM

Аннотация. В статье дается анализ уголовного законодательства Российской Федерации в области защиты чести и достоинства гражданина в период развития и массового использования информационных правовых технологий.

Abstract. The article analyzes the criminal legislation of the Russian Federation in the field of protecting the honor and dignity of a citizen during the development and mass use of information legal technologies.

Ключевые слова: клевета, информационные цифровые технологии, уголовное законодательство.

Keywords: libel, digital information technology, criminal law.

Цифровизация общественной жизни непосредственно ведет к появлению способов совершения преступлений путем использования информационных технологий. Популяризация и простота в использовании цифровых программ способствуют росту случаев распространения заведомо ложных сведений в отношении других лиц. В то же время уголовное законодательство зачастую не успевает эффективно развиваться. В связи со сложившимися обстоятельствами привлечение к уголовной ответственности за клевету в эру информационной цифровизации ставит ряд сложнейших уголовно-правовых и в том числе квалификационных вопросов:

1. Целая группа вопросов связана с *расширением способов совершения клеветы с использованием цифровых технологий*. На сегодняшний день, как никогда ранее, возникает вопрос о том, необходимо ли правовое регулирование в сфере цифровых технологий. Общедоступность и простота в использовании компьютерных программ, способных самостоятельно видоизменять и преобразовывать не только статичные, но и динамические изображения, несомненно, ведет к тенденции расширения использованию подобных программ, в том числе, в преступных целях.

На примере цифровых нейронных сетей, получивших популярность в последние несколько лет, можно сделать вывод о необходимости создания правового поля, регулировавшего использования программ, работающих на их основе. Цифровая нейронная сеть – это технология компьютерного самообучения, способная в автоматическом режиме выполнять различного рода функции эффективнее и быстрее, чем если бы человек выполнял ту же работу самостоятельно. Цифровые нейронные сети стали основой при создании технологии «DeepFake» (англ. Deep–глубокий, Fake– подделка). Данная технология позволяет изменять лица одних людей на фотографиях и видеозаписях на совершенно другие лица. Преступники используют эту технологию при создании видеоматериалов, зачастую, порнографического характера, заменяя лица настоящих актеров на лица знаменитостей. Проблема квалификации такого действия по

статье 128.1 Уголовного кодекса Российской Федерации «Клевета»[1] заключается в том, что человеку самостоятельно практически невозможно распознать подлинность такой видеозаписи. Государству необходимо создать свою программу с использованием цифровых нейронных сетей, которая в автоматическом режиме могла бы анализировать видеозаписи, размещенные в сети «Интернет», и определять их подлинность.

Российское уголовное законодательство неуклонно менялось с развитием цифровых технологий. В Уголовном кодексе Российской Федерации (УК РФ) постепенно вводились как квалифицированные составы преступлений, предусматривающие их совершение посредством использования сети «Интернет», так и отдельная глава 28 «Преступления в сфере компьютерной информации»[2]. Мы считаем, что данных мер недостаточно для устранения пробелов уголовного права России.

На наш взгляд, УК РФ нуждается в создании самостоятельного раздела, регулирующего преступления с использованием информационных цифровых технологий. Создание данного раздела приведет к структуризации подобных преступлений и упростит их квалификацию.

2. Второй важной проблемой современного российского уголовного законодательства является *отсутствие уголовной ответственности за распространение заведомо ложных сведений, порочащих деловую репутацию организаций*. Подобный состав отсутствует не только в УК РФ, но и в КоАП РФ[3]. Единственным источником права, регламентирующим право на защиту деловой репутации организаций, является статья 152 Гражданского Кодекса Российской Федерации «Защита чести, достоинства и деловой репутации»[4]. Мы считаем, что подобное отношение законодателя к организациям, осуществляющим свою деятельность на территории России, является недопустимым. Фактически у физических лиц появляется карт-бланш на причинение вреда деловой репутации юридических лиц. Таким образом, единственным способом защиты деловой репутации организации выступает гражданско-правовая защита. Данный правовой подход к защите деловой репутации организаций в цивилизованном государстве считаем недопустимым.

Для обоснования важности этой проблемы необходимо привести наглядный пример. Допустим, студент Международного Юридического института будет распространять заведомо ложные сведения об институте на своей странице в социальной сети, сообщая, что учебные стандарты не соответствуют нормам образования, аудитории непригодны для проведения в них занятий, а с потолка периодически сыпется штукатурка. Соответственно, такие сведения повлекут за собой последствия, заключающиеся в недоверии абитуриентов при поступлении в Международный юридический институт, что приведет к снижению доходов организации и, следовательно, к реальному падению качества учебного процесса. Однако, несмотря на негативные последствия для института, максимальной ответственностью для студента будет служить возмещение убытков организации и отчисление из учебного заведения. Таким образом, лицо избежит не только уголовной, но даже административной ответственности.

Данный пример доказывает, что возмещение вреда за клевету в рамках гражданского права не является достаточной мерой для такого деяния. Мы считаем, что необходимо ужесточить наказание за распространение заведомо ложных сведений в отношении организаций и внести в УК РФ этот состав преступления. На наш взгляд, ужесточение подобных мер приведет к снижению противоправных действий в данной сфере. По нашему мнению, возможно два варианта криминализации данного деяния.

---

[1] Уголовный кодекс Российской Федерации от 13.06.1996 (ред. от 01.07.2021) // СПС КонсультантПлюс // URL: http://www.consultant.ru/document/cons_doc_LAW_10699/.Ст. 128.1.

[2]Уголовный кодекс Российской Федерации от 13.06.1996 (ред. от 01.07.2021) // СПС КонсультантПлюс // URL: http://www.consultant.ru/document/cons_doc_LAW_10699/. Г. 28.

[3] Кодекс об административных правонарушениях Российской Федерации от 30.12.2001(ред. от 01.07.2021) // СПС КонсультантПлюс // URL: http://www.consultant.ru/document/cons_doc_LAW_34661/.

[4]Гражданский кодекс Российской Федерации от 30.11.1994 (ред. от 28.06.2021)// СПС КонсультантПлюс // URL:http://www.consultant.ru/document/cons_doc_LAW_5142/. Ч. 1. Ст. 152.

Мы считаем, что наиболее правильным вариантом добавления в Уголовный кодекс Российской Федерации состава преступления по клевете в отношении юридических лиц будет являться создание отдельной статьи в главе 23 УК РФ «Преступления против интересов службы в коммерческих и иных организациях»[5]. Предлагается следующая формулировка деяния: «Клевета в отношении коммерческих и иных организаций, если эти действия повлекли для организации потерю деловой репутации–», то есть, по нашему мнению, состав преступления должен быть материальным. Соответственно, негативные последствия от клеветы будут являться решающими для возбуждения уголовного дела.

На основании вышеизложенного следует, что уголовное законодательство России нуждается в улучшении. Необходимо, чтобы Уголовный Кодекс Российской Федерации соответствовал современным реалиям. Единственным способом реализации данной задачи является переструктуризация составов преступлений, предусматривающих совершение общественно опасных действий в информационном правовом поле. Также необходимо уделить особое внимание защите интересов юридических лиц. В первую очередь это важно не только с экономической точки зрения, затрагивающей в основном коммерческие организации, но также и с точки зрения государственной политики. Необходимо не только систематизировать российское уголовное законодательство, но и создать рабочий механизм, способный бороться с распространением клеветы в сети «Интернет» в реальном времени.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уголовный кодекс Российской Федерации от 13.06.1996 (ред. от 01.07.2021) // СПС КонсультантПлюс // URL: http://www.consultant.ru/document/cons_doc_LAW_10699/// [Дата обращения: 23.11.2021].

2. Кодекс об административных правонарушениях Российской Федерации от 30.12.2001 (ред. от 01.07.2021) // СПС КонсультантПлюс //URL: http://www.consultant.ru/document/cons_doc_LAW_34661/// [Дата обращения: 23.11.2021].

3. Гражданский кодекс Российской Федерации от 30.11.1994 (ред. от 28.06.2021) // СПС КонсультантПлюс // URL: http://www.consultant.ru/document/cons_doc_LAW_5142/// [Дата обращения: 23.11.2021].

[5]Уголовный кодекс Российской Федерации от 13.06.1996 (ред. от 01.07.2021) // СПС КонсультантПлюс // URL: http://www.consultant.ru/document/cons_doc_LAW_10699/. Г. 23.

Комарова К.С.
студент 4 курса,
Международный Юридический Институт,

Komarova K.S.
4nd year student
International Law Institute

ПРОБЛЕМЫ СОЗДАНИЯ АРЕСТНЫХ ДОМОВ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

PROBLEMS OF CREATING ARREST HOUSES ON THE TERRITORY OF THE RUSSIAN FEDERATION

Аннотация: Статья посвящена проблемам создания в Российской Федерации учреждений, исполняющих наказания в виде ареста. Раскрывается позиция сущности ареста, и его признаков. Определяются современные проблемы исполнения ареста, а также предлагаются пути их решения.

Resume: The article is devoted to the problems of creating institutions in the Russian Federation that execute penalties in the form of arrest. The position of the essence of the arrest and its signs is revealed. The modern problems of execution of arrest are defined, and the ways of their solution are offered.

Ключевые слова: арест, арестный дом, наказание, лишение свободы, изоляция, осужденный.

Key words: arrest, house of arrest, punishment, imprisonment, isolation, convict.

В российском уголовном законодательстве предусмотрены различные виды наказания, среди которых наиболее проблемным наказанием, связанным с лишением свободы, считается арест. В течение уже длительного времени судебная практика обходится без применения такого вида наказания. Причина данному – это отсутствие арестных домов. В регулировании данного наказания имеются существенные пробелы, которые отрицательно влияют на его восприятие в науке.

В настоящее время наказание в виде ареста на территории России относится к числу основных наказаний, который предусматривает содержание осужденного в условиях строгой изоляции от общества сроком от 1 до 6 месяцев, об этом говорится в ст. 54 Уголовного кодекса Российской Федерации (далее – УК РФ). В литературе главной целью такого вида наказания служит частная превенция [1], которая основывается на идее «шокового воздействия» на осужденного. Если обратиться к нормам Уголовно-исполнительного кодекса Российской Федерации (далее – УИК РФ), то, можно говорить о том, что это специализированные учреждения, в которых исполняется данное наказание и данными учреждениями являются арестные дома. Как правило, срок ареста осужденный отбывает в одном учреждении.

Прежде чем обозначить проблемы создания арестных домов, хотелось бы вспомнить историю их появления. Впервые арест как наказание в отношении граждан появился в Своде учреждений и уставов о содержащихся под стражею и о ссыльных 1832 г. Он упоминался в пяти статьях и не имел какого-либо четкого регулирования [4]. Со временем арест стал одним из самых распространенных видов уголовных наказаний. Условия отбывания зависели от сословного положения осужденного.

Арест был закреплен во всех дореволюционных нормативных правовых актах даже до Уголовного уложения 1903 г. В советский период арест был исключен из системы уголовных наказаний и применялся в большей степени в рамках административного и уголовно-

процессуального законодательства. И вот спустя почти столетие арест снова появился среди уголовных наказаний. Изначально нормы, которые регламентируют исполнение ареста, должны были вступить в силу не позднее 2001 г., но в связи с отсутствием арестных домов указанный срок был перенесен на 1 января 2006 г. До сегодняшнего момента дата создания арестных домов остается неизвестной.

С момента вступления в силу Уголовного кодекса Российской Федерации, арест как вид уголовного наказания не был введен в действие. Мы полагаем, что эта мера государственного принуждения не будет реализована, так как это объясняется огромными материальными проблемами в государстве, что связано с их исполнением. Поэтому мы предлагаем исключить из системы уголовных наказаний арест. Этот вывод можно подтвердить регулированием отношений в обществе, которые фактически складываются при исполнении уголовных наказаний.

Так, из этого следует, что на сегодняшнее состояние уголовно-исполнительного права оказывают значительное влияние экономические факторы, что является первой проблемой создания арестных домов. Существующие экономические отношения объясняют ряд проблем, которые связаны с исполнением ареста как вида уголовного наказания. Проблемы обновления и создания новых учреждений и органов, исполняющих уголовные наказания и иные меры уголовно-правового характера, имеют также не законодательный, а экономический аспект. Указанный фактор учитывался учеными при разработке научно-теоретической модели Уголовно-исполнительного кодекса Российской Федерации, где предложен отказ от данного вида уголовного наказания [5].

В качестве главного недостатка ареста как вида наказания называется его чрезмерное карательное воздействие на осужденного. По мнению исследователей, осужденные, совершившие преступления небольшой или средней тяжести, претерпевают лишения и ограничения, схожие с теми, которым подвергаются осужденные за тяжкие и особо тяжкие преступления. Нужно не забывать, что арест должен применяться к лицам, впервые совершившим преступления небольшой или средней тяжести. Однако данный тезис вступает в противоречие с ч. 1 ст. 69 УИК РФ, из формулировки которой следует, что в арестных домах могут также содержаться лица, ранее отбывавшие наказание в местах лишения свободы и имеющие судимость. Учитывая короткий период данного вида наказания, вряд ли можно говорить о том, что арест способен произвести какой-то огромный эффект. Поэтому мы считаем, что из ч. 1 ст. 69 УИК РФ нужно исключить формулировку «а также осужденные, ранее отбывавшие наказание в исправительных учреждениях и имеющие судимость».

Если мы обратимся к зарубежному опыту, то такие страны, как Армения, Беларусь, Бельгия, Германия, Испания, Италия, Китай, Украина, Финляндия применяют арест в качестве вида уголовного наказания. А вот Франция придерживается такого мнения, что бессмысленно применять арест в системе уголовных наказаний.

Статья 37 Уголовного кодекса Испании устанавливает, что осужденный отбывает арест только в выходные дни, при этом срок наказания составляет от 2 до 24 выходных дней. Так же стоит отметить, что время отбывания ареста в субботу и воскресенье не должно превышать 36 часов, а в зачет наказания идут все два дня [7]. Арест в Испании отбывается в исправительном учреждении, которое располагается максимально близко к месту жительства осужденного. В Бельгии же осужденный отбывает арест с 14 часов в субботу до 6 часов утра в понедельник. Действует он как эксперимент в отношении осужденных к аресту. Такой вариант отбывания наказания возможен только с согласия осужденного лица, при этом срок ареста не должен превышать двух месяцев. В Бельгии имеются арестные дома. Целью данного эксперимента является исправление осужденного без утраты его социальных связей. В Эстонии, в статье 23.2 Уголовного кодекса арест может быть назначен на срок до 3 месяцев [8]. Несовершеннолетнему лицу арест может назначаться на срок до 1 месяца, а его отбытие должно осуществляться в

свободное от учебы и работы время с определением количества дней ареста, отбываемых осужденным в календарном месяце.

Из этого можно сделать небольшой вывод касательно применения краткосрочного тюремного заключения за рубежом. В зарубежных странах очень активно используют арест, который используется в правоприменительной практике. Стоит отметить, данный вид наказания является наказанием, связанным с кратковременной изоляцией осужденного от общества, и назначается за совершение преступлений небольшой тяжести. Арест как вид уголовного наказания имеет достаточно продолжительную историю применения за рубежом и имеется в уголовных законах многих стран, причем порядок и основания его назначения, условия отбывания отличаются огромным разнообразием, который касается практически всех сторон применения этого наказания.

Продолжая обозначать проблемы создания арестных домов в России, поступает такой вопрос «а нужен ли вообще данный вид наказания?». Ученые высказывают противоположные позиции касательного данного вопроса. Нормы об аресте при принятии УК РФ и УИК РФ обосновывались необходимостью иметь альтернативу лишению свободы. С другой стороны, трудно дать научное объяснение установлению наказания в виде ареста, поскольку фактически условия отбывания наказания при аресте более строгие, чем в тюрьме, где отбывают наказание лица, совершившие наиболее тяжкие преступления осужденные к лишению свободы. В научной литературе подчеркивается несоответствие принципу справедливости, условий отбывания в арестных домах лицами, совершившими значительно менее опасные преступления, по сравнению с лицами, отбывающими наказания в тюрьмах [3]. Некоторые авторы обосновывают, что законодатель может и вовсе относительно отказаться от введения наказания в виде ареста.

Первоначально, арест планировалось исполнять на базе следственных изоляторов и тюрем, однако вследствие перегруженности последних от этой идеи пришлось отказаться. В УИК РФ закреплено, что арест исполняют арестные дома и гауптвахты. В качестве решения проблемы ученые предлагают сделать арест специальным видом уголовного наказания, применяемым исключительно в отношении военнослужащих [2]. Предложенный вариант является наиболее простым и повлечет незначительные изменения норм УК РФ и УИК РФ, регламентирующих исполнение наказания в виде ареста.

В научной литературе представлены различные модели создания арестных домов: от перепрофилизация некоторых видов исправительных учреждений, расположенных в городах, до создания арестных домов на новом фундаменте [6]. Поэтому мы предлагаем выделить три основные модели создания арестных домов: создание арестного дома как самостоятельного учреждения уголовно-исполнительной системы; возложение обязанности исполнения ареста на действующие исправительные учреждения; арестный дом как изолированный участок на территории исправительного учреждения.

Выделяя следующую проблему, хотелось бы отметить, что введение ареста противоречит программным установкам государства. В течение последнего десятилетия количество осужденных и подследственных лиц, содержащихся в учреждениях ФСИН России, стремительно сокращается. Это было связано с либерализацией уголовно-исполнительной политики: увеличилось количество осужденных, отбывающих наказания, не связанные с изоляцией от общества, суды стали активнее отправлять подследственных не в камеры следственных изоляторов, а под домашний арест, заработали ранее не применяемые меры пресечения – залог и ограничение определенных действий. Также снизилось количество подследственных, содержащихся в следственных изоляторах и помещениях, функционирующих в режиме следственного изолятора.

Подводя итоги, можно сказать о том, что, изучая федеральную целевую программу «Развитие уголовно-исполнительной системы (2018–2026 годы)», строительство арестных домов в ней не запланировано. Приоритетными задачами указанной программы являются реконструкция и строительство следственных изоляторов, исправительных, лечебных

исправительных, лечебно-профилактических учреждений в соответствии с международными стандартами и российским законодательством, а также создание дополнительных рабочих мест для осужденных к лишению свободы. Арест задумывался как альтернатива лишению свободы на непродолжительный срок. Однако минимальный срок лишения свободы в настоящее время составляет два месяца. Поэтому необходимость в существовании ареста попросту отсутствует.

На наш взгляд в современных условиях следует предусмотреть исполнение наказания в виде ареста в следственных изоляторах. Это обусловлено тем, что переполненность следственных изоляторов, которая была ранее, в настоящее время отсутствует. Кроме этого, данное решение является менее затратным, так как режим содержания в следственном изоляторе предусматривает покамерное размещение подследственных лиц.

Таким образом, на данный момент одними из важных аспектов, способствующих формированию системы наказаний, следует экономические условия государства. Именно эти условия коснулись такого наказания, как арест. По мнению подавляющего большинства исследователей, для создания арестных домов потребуются существенные финансовые вложения, и применение наказания в виде ареста отсрочено по причине того, что в стране сложилась нестабильная экономическая ситуация.

Однако исключать арест из системы уголовных наказаний нецелесообразно, так как, во-первых, сегодня он исполняется в отношении военнослужащих, во-вторых, рано или поздно появятся финансовые ресурсы на строительство арестных домов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Головастова, Ю. А. Уголовно-исполнительное право как отрасль российского права. Современный взгляд: монография / Ю. А. Головастова; под редакцией В. И. Селиверстов. – Москва : Юриспруденция, 2017.
2. Добряков Д. А. К вопросу о неприменимых видах наказаний в уголовном законодательстве Российской Федерации // Евразийская адвокатура. 2017. № 5. С. 93–97.
3. Подройкина И. А. О перспективе ареста как уголовного наказания // Академический вестник Ростовского филиала Российской таможенной академии. 2015. № 3 (20). С. 65–69.
4. Свод учреждений и уставов о содержащихся под стражею и о ссыльных 1832 г. URL: http://www.rus-sky. com/history/library/vol.14/vol.14.4.htm
5. Степашин В. М. Арест как вид уголовного наказания // Вестник Омского университета. 2011. № 4 (29). С. 130–134.
6. Стромов В.Ю. Эффективность отечественной системы наказаний: проблемы уголовно-правовой теории и правоприменительной практики // Вестник Тамбовского университета. 2014. № 6 (134). С. 199–204.
7. Уголовный кодекс Испании. URL: http:// artlibrary2007.narod.ru/kodeks/ispanii_uk.doc
8. Уголовный кодекс Эстонии. URL: http:// okpravo.ru/zarubezhnoe-pravo/ugolovnoe-pravozarubezhnyh-stran.html

Крепышева В.В.
студент 4 курса юридического факультета Нижегородского государственного университета им. Н.И. Лобачевского

Krepysheva V.V.,
4th year student of the Faculty of Law of the Nizhny Novgorod State University named after N.I. Lobachevsky

ВЛИЯНИЕ ПАНДЕМИИ КОРОНАВИРУСА COVID-19 НА КИБЕРПРЕСТУПНОСТЬ

IMPACT OF THE COVID-19 PANDEMIC ON CYBERCRIME

Аннотация: Во время пандемии COVID-19 люди и общество оказались в чрезвычайно уязвимом положении. Во время этого кризиса общество все больше, чем когда-либо, полагается на компьютерные системы, мобильные устройства и Интернет во время работы, общения, совершения покупок.

Ключевые слова: киберпреступность, COVID-19, фишинговые компании, социальное дистанцирование.

Abstract: During the COVID-19 pandemic, people and society were in an extremely vulnerable position. During this crisis, society relies more than ever on computer systems, mobile devices and the Internet for work, communication and shopping.

Key words: cybercrime, COVID-19, phishing companies, social distancing.

В конце 2019 года весь мир узнал о распространение коронавирусной инфекции COVID-19 в КНР. Эта инфекция, являясь опасным заболеванием, вызываемым вирусом SARS-CoV-2, впервые была обнаружена в городе Ухань. Сразу после этого стало известно о новых вспышках заболевания в США, Бразилии, Франции, Великобритании и ряде других государств. С этого момента все страны, с целью предотвращения дальнейшего распространения вируса, стали вводить ограничения, которые, безусловно, повлияли практически на все сферы жизнедеятельности человека.

В Российской Федерации органы государственной власти так же предприняли ряд мер, направленных на ограничение распространения вируса, в частности:

05.03.2020 Мэром Москвы был издан указ №12-УМ «О введении мер повышенной готовности».

Указом от 25.03.2020 №206 Президент РФ Владимир Владимирович Путин объявил нерабочими днями период с 30.03.2020 г. по 03.04.2020 г.

В ответ на ухудшающуюся эпидемиологическую ситуацию в стране органы государственной власти Российской Федерации фактически ввели «режим самоизоляции», вынуждая большую часть населения оставаться в пределах своих домов, а работодателей – перевести практически всех своих работников на удаленный режим работы.

Глубоко повлияв на все общественные процессы, пандемия не обошла стороной и различные криминальные явления. Особенно значительно влияние пандемии коронавируса на киберпреступность.

С увеличением числа людей, проводящих больше времени в интернете, киберпреступность возросла. Из-за увеличения объема работы из дома все преступники могут получить доступ к большему объему корпоративных данных, которые хранятся на домашних компьютерах, которые, не так защищены, как офисные компьютерные системы [1].

Начиная с 21 века, когда крупные и мелкие компании начали в целом наращивать меры безопасности своих ИТ-систем, киберпреступные группы постепенно меняли тактику атак, используя человеческую уязвимость для кражи пользовательских данных.

В первые месяцы 2020 года количество атак резко возросло из-за страха перед COVID-19 и усугубляется снижением уровня безопасности в некоторых компаниях. Так же все чаще происходят кибератаки на правительственные инфраструктуры или международные организации. Так, например, количество кибератак на компьютерные системы Всемирной организации здравоохранения (ВОЗ) во время пандемии коронавируса выросло в пять раз. В апреле 2020 года произошла утечка 450 электронных адресов и паролей ВОЗ. После этого Всемирная организация здравоохранения опубликовала уведомление о кибербезопасности, предупреждающее людей о мошенниках, имитирующих сотрудников ВОЗ [2].

На протяжении всей пандемии наблюдается всплеск фишинговых атак, мошенники распространяют вредоносные программы через электронные письма, содержащие информацию или советы по COVID-19, заражая компьютеров и извлекая учетные данные пользователей.

Программы-вымогатели – программное обеспечение, использующее приложения, которые предоставляют «подлинную» информацию о COVID-19, вымогая у пользователя деньги.

Преступники активно пользуются схемами мошенничества, при которых людей обманом заставляют покупать такие товары, как маски, дезинфицирующие средства для рук, а также поддельные лекарства, утверждающие, что они предотвращают или лечат от SARS-CoV-2.

Пытаясь извлечь выгоду из опасений по поводу коронавируса, мошенники запускают новые фишинговые кампании с ложными советами против вируса для распространения своего вредоносного ПО среди жертв или кражи их личной информации.

Пожилые люди с ограниченными знаниями о цифровом мире особенно уязвимы для интернет-мошенничества. Частота атак заметно возросла во время социального дистанцирования COVID-19, когда хакеры пользуются резким увеличением времени пользователя в сети и уязвимостью определенных групп людей.

Дезинформация или фейковые новости распространяются троллями и фальшивыми аккаунтами в СМИ, чтобы вызвать панику, социальную нестабильность и недоверие к правительствам или мерам, принимаемым органами здравоохранения [3].

Правонарушители получают доступ к системам компаний и организаций, взламывая компьютеры сотрудников, работающих удаленно.

Для того чтобы минимизировать риск ущерба от новых кибератак в период пандемии, компании, которые перевели своих сотрудников на удаленную работу могут:

1. выработать и утвердить политику безопасности при удаленной работе,
2. повышать уровень киберграмотности сотрудников
3. обеспечить сотрудников всем необходимым для работы защищенным корпоративным оборудованием с доступом в корпоративную сеть.
4. обеспечить защиту каналов для безопасного обмена информацией,
5. проводить непрерывный мониторинг периметра сети и инфраструктуры, во время выявлять и устранять уязвимости и ошибки в системе.

Безусловно, приведенный выше механизм не является абсолютной панацеей. Но соблюдение вышеперечисленных действий может значительно помочь организациям в предотвращении кибератак.

Стоит отметить, что компании, которые ранее пользовались возможностями безопасной удаленной работы, были лучше подготовлены к переводу на удаленную работу. А компании, которые были застигнуты врасплох, не смогли быстро оценить свою подверженность киберугрозам.

Пандемия SARS COV-2 сделала очевидными проблемы кибербезопасности, связанные с:

1. Увеличением финансовых потерь от кибератак;
2. Низким уровнем грамотности населения в цифровой среде;
3. Повышенной уязвимостью из-за «более простой и крупной цели и поверхности атаки», вызванная социальным дистанцированием;

4. Усилением киберпреступности против уязвимых предприятий, компаний и частных лиц;

5. Слабым, как международным, так и российским законодательством в области кибербезопасности.

Эти проблемы необходимо решать на уровне федеральной власти. Отдельное внимание следует уделить улучшению нормативно-правовой базы нашей страны в области кибербезопасности. На сегодняшний день практически отсутствует официально закрепленный целостный подход к данной национальной проблеме. Действующая Доктрина информационной безопасности изжила себя и требует серьезных изменений [4].

Необходимо обновление политики в области цифровых технологий, касающиеся кибербезопасности, цифровой торговли, пользования интернетом и конфиденциальности в интернете.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Орцханова Т. М., Попов М.Д. «Кибермошенничество» как угроза безопасности: краткий обзор ситуации в условиях пандемии. // Тамбовские правовые чтения имени Ф. Н. Плевако. Материалы IV международной научно-практической конференции. В двух томах. Тамбов, 2020. С. 332-337.

2. Торшхоев С. А., Иванов Ф. К. Кибермошенничество как угроза экономической безопасности в контексте пандемии SARS COV-2 // Актуальные исследования. 2021. №19 (46). С. 51-54. URL: https://apni.ru/article/2413-kibermoshennichestvo-kak-ugroza-ekonomichesk

3. Номоконов В.А. Киберпреступность, как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология. Вчера. Сегодня. Завтра. – 2012. – №1 (24). – С. 47.

4. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение. // Власть. №8. 2014. С. 46-50.

Кутин П.М.
курсант 3 курса прокурорско-следственного факультета
Военного университета МО РФ

Kutin P.M.,
3rd year cadet of the
Prosecutor's and Investigative Faculty
Military University of the Ministryof Defense of the Russian Federation

Наливайко В.О.
курсант 3 курса прокурорско-следственного факультета
Военного университета МО РФ

Nalivayko V.O.
3rd year cadet of the
Prosecutor's and Investigative Faculty
Military University of the Ministryof Defense of the Russian Federation

УГОЛОВНО-ПРАВОВАЯ ЗАЩИТА ГРАЖДАН РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

CRIMINAL LEGAL PROTECTION OF CITIZENS OF THE RUSSIAN FEDERATION IN THE SPHERE OF INFORMATION SECURITY

Аннотация. В статье рассматриваются вопросы информационной безопасности граждан в Российской Федерации, которые в современных реалиях начали набирать обороты, ведь развивающаяся киберпреступность ставит под угрозу целостность и сохранность государства. В исследовании анализируется статистика преступлений в сфере информационных технологий, а также в статье определены основные проблемы реализации и правоприменения статей Уголовного кодекса Российской Федерации, связанных с преступлениями против собственности, и рассматриваются подходы к улучшению ситуации в сфере информационной безопасности.

Annotation. The article discusses the issues of information security of citizens in the field of the Russian Federation, which in modern realities have begun to gain momentum, because the developing cybercrime threatens the integrity and safety of the state, analyzes the statistics of crimes in the field of information technology. The article also identifies the main problems of the implementation by the law enforcement officer of articles related to crimes against property, and discusses approaches to improving the situation in the field of information security.

Ключевые слова: информационная безопасность, киберпреступность, уголовно-правовая защита, мошенничество, персональные данные.

Keywords: information security, cybercrime, criminal defense, fraud, personal data.

В соответствии со статьей 2 Конституции Российской Федерации (далее – РФ) человек, его права и свободы являются высшей ценностью государства [1]. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства. Гражданин РФ обладает всеми правами и свободами и несет равные обязанности, предусмотренные Конституцией Российской Федерации.

На сегодняшний день тенденции глобализации особенно проявляются в информационной сфере, обеспечивая диалог культур и цивилизаций во всех направлениях жизнедеятельности человечества. Российская Федерация занимает важное место в процессе информатизации

общества и формирования единого мирового информационного рынка. Информационный фактор играет значительную роль в современном государстве.

Особое место в мире занимают проблемы правового обеспечения информационной безопасности. Процесс развития технологий обработки, хранения и передачи информации в России приводит к повышенному вниманию к вопросам правового регулирования информационной безопасности, так как играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации. Незаконное и несанкционированное использование информационных ресурсов приводит к серьезным проблемам как у отдельного гражданина, так и у всего государства в целом. В современной России уже сформированы правовые инструменты защиты информации на государственном уровне, однако они требуют оперативного совершенствования и развития. Уголовное законодательство направлено на предупреждение и пресечение незаконных преступных посягательств на конституционные права и свободы человека и гражданина.

Преступления в сфере информационных технологий отражены в Уголовном кодексе Российской Федерации (далее – УК РФ) [2]. В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства [3, С. 55–59]. Ответственность за совершение указанных преступлений предусмотрена главой 28 Уголовного кодекса Российской Федерации.

По Уголовному кодексу Российской Федерации преступлениями в сфере компьютерной информации являются:

1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ),
2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ),
3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и распространение порнографии (ст. 274 УК РФ).

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации.

Постановление Пленума Верховного суда РФ № 48от 30 ноября 2017 г. «О судебной практике по делам о мошенничестве, присвоении и растрате» подробно обозревает правоприменительную практику по квалификации преступлений в информационной сфере, а именно говорит о том, что в статье 159.6 УК РФ (мошенничество в сфере компьютерной информации) под вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации признается целенаправленное воздействие программных средств на серверы, средства вычислительной техники, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него[4].

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ.

По данным МВД России в период пандемии COVID-19 резко возросло количество преступлений в информационной сфере, а именно деяний, подпадающих под статью 272 УК РФ (неправомерный доступ к компьютерной информации). Начальник пресс-службы московского ГУ МВД Владимир Васенин сообщил, что полиция ежедневно фиксирует по 10-15 обращений, в

основном жертвами становятся пожилые люди. Количество обращений также выросло за последний месяц на фоне пандемии. Активизировалось мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации, так как ограничительные меры, вводимые в связи с пандемией, привели к развитию технологических решений, как например, перевод ряда услуг в онлайн-сферу [5].

О росте преступности сообщает также Департамент региональной безопасности и противодействия коррупции города Москвы [6]. По его сообщениям, на фоне пандемии COVID-19 отмечается повышение активности мошенников, использующих тему коронавирусной инфекции, а именно участились случаи массовой рассылки сообщений под видом государственных органов и должностных лиц с целью получения денежных средств. Проблема неправомерного доступа к компьютерной информации является одной из самых приоритетных на сегодняшний день в информационную эру, так как базы данных с номерами и данными граждан РФ попадают к лицам, которые осуществляют свой преступный умысел, используя полученную ими информацию в качестве орудия совершения преступления. База данных номеров граждан РФ незаконно размещается в информационный сети «Интернет», лицо, осуществляющее преступный умысел, использует эти данные для совершения другого преступления, тем самым создают угрозы безопасности граждан РФ.

Примером может послужить случай с появлением в теневом секторе интернета данных более 500 тысяч россиян из московского региона, которые покупали поддельные справки о вакцинации и ПЦР [7]. Данный факт в дальнейшем опровергла пресс-служба Департамента информационных технологий города Москвы [8]. Однако сама тенденция информационной незащищенности уже давно прослеживается в Российской Федерации. Уголовная ответственность за данные преступления против конституционных прав граждан РФ крайне мала, что приводит к тому, что лицо, совершающее преступление, между материальной выгодой и риском уголовного наказания выбирает первое. Тем самым совершает преступление, предусмотренное статьей 272 (неправомерный доступ к компьютерной информации) и статьей 159.6 (мошенничество в сфере компьютерной информации), санкцией которого предусмотрен штраф или минимальное лишение свободы.

В последнее время в нашей стране все чаще стали происходить преступления, связанные с размещением данных граждан РФ в свободном доступе, преступники просто продают эти базы данных, тем самым, нарушая законное право на защиту персональных данных. Механизмы и инструменты защиты персональных данных раскрыты в Федеральном закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» [9].

По данным МВД России замедлился рост количества зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Если в первом квартале 2021 года их число увеличилось на 33,7%, то за 8 месяцев 2021 года – на 12,7%. Однако проблема заключается в том, что рост данных преступлений продолжается, многие деяния остаются незамеченными правоохранительными органами РФ, тем самым создается практика, когда человек остается один на один с мошенниками, не имя действенных правовых инструментов и способов защиты своих прав.

Согласно статистике, предоставленной МВД России, Генеральной прокуратурой РФ, удельный вес преступлений в сфере IT среди их общего количества увеличился на 5% за пять месяцев [10]. 21 июня МВД опубликовало статистику по преступлениям за январь – май 2021 года. Число преступлений против личности сократилось, но общее количество зарегистрированных преступлений выросло на 1,6% за счет цифровой преступности. В то же время IT-преступность продолжает расти. В январе – мае 2021 года количество таких преступлений выросло на 25,7% в сравнении с аналогичным периодом 2020 года. Увеличивается и доля киберпреступности в общем объеме преступлений – год назад она составлял 21,7%, а сейчас – уже 26,8%, то есть более четверти от их общего количества. В том числе на 48,4%

выросло количество преступлений, совершенных при помощи интернета. На 40,1% увеличилось число преступлений с использованием компьютерной техники [11].

Примером работы судов при рассмотрении преступлений в данной сфере служит дело №22-993/2019, которое прошло две судебные инстанции. Гражданин Ербягин А.Е. совершал переводы денежных средств от имени потерпевшей. Вследствие чего суд вынес приговор, по которому данный гражданин был осужден по п. «г» ч.3 ст.158 УК РФ к 2 годам лишения свободы, но суд назначил наказание условным с испытательным сроком 2 года.

В свою очередь суд апелляционной инстанции пересмотрев обстоятельства дела, выявил нарушение в части назначения наказания. Поэтому действия Ербягин А.Е. с п. «г» ч.3 ст.158 УК РФ переквалифицировали на п. «в» ч.2 ст.158 УК РФ – кражу, то есть тайное хищение чужого имущества с причинением значительного ущерба гражданину. В итоге по п. «в» ч.2 ст.158 УК РФ Ербягину А.Е. назначено наказание в виде 1 (одного) года исправительных работ с удержанием в доход государства 10% его заработной платы, однако также условно с испытательным сроком 1 год [12].

Данное решение суда свидетельствует о том, что одной из причин растущего количества киберпреступлений в России является чересчур легкое наказание по отношению к лицам, совершающих данную категорию преступлений. Судам необходимо пересмотреть подход к решению данных дел, чтобы небольшое наказание не вызывало чувства безнаказанности.

Тем самым, перед правоприменителем встает проблема правильной квалификации деяния, которое подпадает под два состава преступления. Для решения данной проблемы необходимо более конкретно определить границы преступлений, предусмотренных ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации) и ст.158 УК РФ (Кража). Законодателю необходимо увеличить санкцию по данным составам преступления, так как только решительная уголовная политика государства способна побороть рост киберпреступности.

Резюмируя вышеизложенное, необходимо отметить, что в Российской Федерации ведется активная борьба с киберпреступностью, но ввиду новизны данных преступлений, отсутствия разъяснений Верховного суда РФ и трудности выявлений и расследования данных общественного опасных деяний виновные лица уходят от уголовного наказания или получают незначительные, часто условные, сроки. Для решения данной проблемы и снижение темпов развития преступлений в информационной сфере необходимо провести соответствующую подготовку правоприменителей, это исключит возможность виновным уйти от справедливого и соразмерного наказания. Так же следует ожесточить ответственность за совершения преступления по ст.159.6 УК РФ (мошенничество в сфере компьютерной информации), так как именно из-за низкого уровня наказания, преступники не боятся совершать данные преступные деяния. Политика информационной безопасности должна иметь многосторонний характер. Ее главными составляющими являются: регулирование информационных отношений в целях обеспечения национальной безопасности, территориальной целостности и общественного порядка, поддержания законности; регулирования информационных отношений в целях обеспечения прав и свобод граждан, здоровья и нравственности; регулирования информационных отношений в сфере коммерческой информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)// Собрание законодательства РФ. 2020. № 27. Ст. 4196.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 295

3. Уголовное право России. Части общая и особенная: Учебник. 3-е издание. / Под ред. А.В. Бриллиантова. – 2021.

4. Постановление Пленума Верховного суда Российской Федерации № 48 от 30 ноября 2017 г. «О судебной практике по делам о мошенничестве, присвоении и растрате» (с изменениями, внесенными постановлением Пленума ВС РФ от 29 июня 2021 г. № 22)// СПС КонсультантПлюс (дата обращения 20.11.2021)

5. О состоянии преступности в Российской Федерации в 1-м квартале 2020 года [Электронный ресурс] URL: https://мвд.рф/news/item/19986723/(дата обращения 24.11.2021)

6. Предупреждение о новых способах мошенничества с использованием темы коронавируса [Электронный ресурс] URL: https://www.mos.ru/news/item/72309073(дата обращения 19.11.2021)

7. О размещении данных граждан РФ [Электронный ресурс] URL: https://rg.ru/2021/11/12/smi-v-set-slity-dannye-500-tysiach-kupivshih-poddelnye-sertifikaty-rossiian.html(дата обращения 22.11.2021)

8. Заявление органов власти Москвы [Электронный ресурс] URL: https://tass.ru/obschestvo/11803637(дата обращения 20.11.2021)

9. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ // СПС КонсультантПлюс (дата обращения 20.11.2021)

10. Состояние преступности в России (форма федерального статистического наблюдения № 4-ЕГС и ведомственного отчета МВД России формы 1-А.) [Электронный ресурс] URL: https://epp.genproc.gov.ru/web/gprf, https://epp.genproc.gov.ru/(дата обращения 18.11.2021)

11. МВД России публикует данные о состоянии преступности по итогам пяти месяцев 2021 года [Электронный ресурс] URL: https://мвд.рф/news/item/24738876(дата обращения 22.11.2021)

12. Судебное решение [Электронный ресурс] URL: https://sudact.ru/vsrf/doc/?vsrf-txt=&vsrf-case_doc=%E2%84%9622-993%2F2019(дата обращения 21.11.2021)

13. Чучаев А.И. Уголовное право. Особенная часть. Учебник для бакалавров. – 2019.

14. Шаньгин В. Ф. Информационная безопасность и защита информации. – 2017.

Лагунова Е.С.
курсант 3 курса Московского университета МВД России имени В.Я.Кикотя,

Lagunova E.S.
third-year cadet of the V.Y. Kikotyan Moscow University of the Ministry of Internal Affairs of Russia,

ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРОТИВОДЕЙСТВИЯ ЭКОНОМИЧЕСКИМ ПРЕСТУПЛЕНИЯМ В ИНФОРМАЦИОННУЮ ЭРУ

PROSPECTS FOR THE DEVELOPMENT OF COUNTERACTION TO ECONOMIC CRIME IN THE INFORMATION AGE

Аннотация: В настоящей статье рассмотрены наиболее актуальные механизмы и способы преодоления информационных угроз на государственном уровне. В связи с этим, целью данной научной статьи является анализ проводимой государством и правоохранительными органами работы по модернизации системы противодействия экономическим преступлениям в информационном пространстве. Актуальность работы, в свою очередь, определяется нарастающими оборотами технологического прогресса, результаты которого зачастую становятся оружием в руках правонарушителей. Так, качественный анализ сферы противодействия таким правонарушениям позволит выявить необходимые направления для дальнейшей оптимизированной и максимально эффективной работы. Изучаемые в данной статье реформы и проекты преобразования сферы информационной безопасности позволяют оценить уровень заинтересованности государства в данном вопросе и степень значимости проводимой им работы.

Abstract: This article examines the most relevant mechanisms and ways of overcoming information threats at the state level. In this connection, the purpose of this scientific article is to analyze the work carried out by the state and law enforcement agencies to modernize the system of countering economic crimes in the information space. The relevance of the work, in turn, is determined by the increasing turnover of technological progress, the results of which often become a weapon in the hands of offenders. Thus, qualitative analysis of the sphere of counteraction to such offences will allow to reveal necessary directions for further optimized and maximally effective work. Reforms and projects of transformation of the sphere of information security studied in this article allow us to evaluate the level of interest of the state in this issue and the degree of significance of the work it carries out.

Ключевые слова: информационная сфера, кибератака, государство, экономика, правоохранительные органы.

Key words: information sphere, cyber-attack, state, economy, law enforcement.

Современный этап развития отечественного инновационного сектора позволяет говорить о том, что Россия стремительно приближается к постиндустриальному типу общества. Передовые технологии находят свое применение во всех сферах жизнедеятельности. Однако не редки случаи, когда современные технологии становятся инструментом приобретения экономических благ, полученных преступным путем. Проблема противодействия экономическим преступлениям, совершаемым в информационной сфере, обретает особую актуальность на сегодняшний день. В первую очередь это связано со значительным ростом данных правонарушений за последние годы. Об этом свидетельствуют статистические данные, предоставляемые Министерством внутренних дел РФ. Так, за первые 7 месяцев 2021 года наблюдалось общее повышение числа зарегистрированных преступлений в It-сфере на 15,7% по сравнению с аналогичным периодом прошлого года. Стоит учитывать, что данное повышение сопровождается уменьшением числа иных совершаемых уголовно наказуемых преступлений:

количество убийств и покушений на убийство снизилось на 8,4 %, умышленного причинения тяжкого вреда здоровью – на 12,4%, а случаев совершения разбоев и грабежа на 19,5% и 20,4% соответственно. Данная тенденция подтверждает, что преступная деятельность все активнее переходит в информационное пространство, что требует от правоохранительных органов.

Одним из самых продуктивных подразделений МВД, осуществляющих борьбу с информационными преступлениями, является Управление «К». Данное подразделение занимается выявлением и пресечением ряда преступлений, совершаемых в информационной сфере, в том числе связанных с неправомерным получением доступа к компьютерной информации, незаконным использованием объектов авторских и смежных прав и совершением махинаций в сети Интернет, социальных сетях и банковских системах. Благодаря работе Управления ежегодно предотвращается значительное количество преступлений, способных нанести экономический ущерб как государству, так и отдельным хозяйствующим субъектам. Однако в современных условиях правонарушители находят все больше способов совершения экономических преступлений в информационном пространстве, не всегда попадающих под компетентность Управления «К». В связи с этим государство активно принимает меры по реформированию существующей системы противодействия экономическим преступлениям. Так, в сентябре 2020 года Генеральной прокуратурой РФ была создана межведомственная группа, координирующая свои действия в борьбе с киберпреступностью. Кроме того, официальные лица МИДа, МВД, ФСБ, Следственного комитета и Министерства юстиции, вошедшие в данную группу, уполномочены представлять российскую позицию в проекте международной конвенции ООН по противодействию использования информационно-коммуникационных технологий в преступных целях. Примечательно, что этим не ограничивается международное сотрудничество России в вопросе модернизации системы противодействия преступлениям в it-сфере. Еще в 2018 году председателем Правительства, Михаилом Мишустиным было подписано постановление об одобрении Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий. А в начале текущего 2021 года на российско-американском саммите в Женеве был поднят вопрос о сотрудничестве США и России как в части снижения уровня атак, совершаемых на территории США, так и в части взаимной договоренности о запрете на совершение атак по определенным секторам инфраструктуры.

Безусловно, говорить об эффективности такого взаимодействия рано, однако заинтересованность Российской Федерации в международном сотрудничестве в вопросе противодействия информационным преступления имеет перспективу положительного влияния на модернизацию данной сферы.

Кроме того, правоохранители понимают, что работа в данном направлении должна вестись не только благодаря поддержки других государств, но и за счет максимальной вовлеченности внутригосударственных ведомств. Так, МВД совместно с Банком России уже начало разработку единой статистической базы киберпреступлений. Данный сервис будет предназначен для сбора статистических сведений о зарегистрированных преступлениях в информационном пространстве, анализ которых поможет правоохранителям определить основные направления дальнейшей работы. Стоит отметить, что при разработке такой системы, правоохранители могут столкнуться с рядом практических проблем, например, трудностью организации работы системы, которая сможет одновременно хранить и обрабатывать большое количество данных. Решением такой проблемы может стать применение BigData в качестве структурного компонента будущей системы. BigData представляет собой автоматизированный инструмент, способный обрабатывать большое количество информации и выдавать результат своего анализа. Поэтому внедрение механизма BigData сможет значительно ускорить и улучить работу создаваемой базы по информационным преступлениям. Потенциально возможное применение такой технологии в деятельности правоохранительных органов говорит о том, что работа по обеспечению безопасности в информационным пространстве должна проводиться

совместными усилиями правоохранительных органов и граждан, в лице организаций, способных оказать качественное воздействие в данной сфере. Так, концерн «Автоматика», АО НИК и ООО «Ти Хантер» планируют создать систему для борьбы с киберпреступлениями. Сервис будет работать автоматизировано и находиться в открытом доступе для правоохранителей. Как сообщают официальные представители, следователь сможет загрузить в систему e-mail или номер телефона подозреваемого, а программный комплекс, используя этот фрагмент, сопоставит с ним массивы данных.

Кроме того, всестороннее воздействие на решение изучаемой проблемы может оказать содействие граждан, а именно соблюдение ими мер по предотвращению кибератак. Речь идет о популяризации среди населения использования многофакторной аутентификации. Для ее установки существует множество сервисов и приложений, которые делают качественную защиту персональных данных доступной и простой в использовании. Также актуальность в настоящее время обретает искусственный интеллект, который все чаще применяется организациями как инструмент дополнительной защиты от кибератак. Это позволяет снизить потери: пострадавшие от утечки данных организации, у которых была полностью развернута технология искусственного интеллекта, сэкономили в среднем 3,58 миллиона долларов в 2020 году.

Подводя итог, можно отметить высокий уровень заинтересованности государства и правоохранительных органов в обеспечении достойного уровня информационной безопасности государства и иных хозяйствующих субъектов. Анализ проводимой работы, позволяет говорить о необходимости дальнейшей модернизации системы выявления и предотвращения кибератак на государственном уровне. Продолжив работать в данном направлении, Российская Федерация сможет создать уникальную систему противодействия информационным преступлениям, способную отражать внешние и внутренние угрозы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. 1. Гаврилин Ю. В. Противодействие цифровой трансформации преступности (по итогам Всероссийского онлайн-семинара) // Труды Академии управления МВД России. 2020. (56).
2. Пырчев С. В. Тенденции организованной преступности в развивающемся цифровом мире // Труды Академии управления МВД России. 2020. № 2 (54).
3. Positive Technologies: Актуальные угрозы – 2018: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018rus.pdf.
4. Жиронкин, Д. С. Влияние цифровой экономики на киберпреступность / Д. С. Жиронкин. – Текст : непосредственный // Молодой ученый. – 2019. – № 30 (268). – С. 88-92. – URL: https://moluch.ru/archive/268/61757/ (дата обращения: 28.11.2021).
5. Tsepelev V.F., Borisov A.V., Vlasov A.V., Drozdova E.A. Corruption and legal limits of anticorruption enforcement // International Journal of Economics and Business Administration. 2019. Т. 7. № S1. С. 204–208

Люсина П.А.
курсант 3 курса 191 учебного взвода
Московский областной филиал Московского университета
МВД России имени В.Я. Кикотя,

Lyusina P.A.
3st year cadet of the group 191
of the Moscow region brunch of the Moscow University
of the MIA of Russia named after V. Ya. Kikot',

АКТУАЛЬНЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ СКЛОНЕНИЮ НЕСОВЕРШЕННОЛЕТНИХ К СУИЦИДУ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ "ИНТЕРНЕТ")

CURRENT COUNTERACTION ISSUES PREVENTION OF MINORS TO SUICIDE USING INFORMATION AND TELECOMMUNICATION NETWORKS (INCLUDING THE "INTERNET" NETWORK).

Аннотация: В статье анализируется проблема склонения несовершеннолетних к суициду с использованием информационно-телекоммуникационных сетей включая сеть Интернет. Актуальность рассмотрения проблемы обусловлена активным развитием сферы совершения суицида несовершеннолетних при условии недостаточного обеспечения безопасности несовершеннолетних и их защита от преступных посягательств.

Abstract: The article analyzes the problem of persuading minors to commit suicide using information and telecommunication networks. The urgency of considering the problem is due to the active development of the sphere of committing suicide of minors, provided that the safety of minors is insufficient and their protection from criminal encroachments.

Ключевые слова: Склонение несовершеннолетнего, суицид, преступная деятельность, задания, сообщество, сеть «Интернет», побуждение.

Keywords: Declination of a minor, suicide, criminal activity, assignments, community «Internet», motivation.

В соответствии с ч. 4 ст. 67.1 Конституции РФ, дети являются важнейшим приоритетом развития России, а на государство возложена обязанность создать всесторонние условия для их развития. Безусловно, что одним из наиболее значимых факторов такого развития является обеспечение безопасности несовершеннолетних и их защита от преступных посягательств.

К сожалению, новым и весьма угрожающим явлением в XXI веке стало не только возросшее число самоубийств среди людей несовершеннолетнего возраста, но и целенаправленное распространение, особенно в виртуальном мире, идеологии суицида, призывов к нему, а также, предоставления советов по совершению самоубийств.

Учитывая высокую общественную опасность данных деяний, их направленность, в основном, против жизни и здоровья несовершеннолетних лиц, законодатель с 2017 г. криминализовал как склонение к самоубийству конкретного лица (ст. 110.1 Уголовного кодекса Российской Федерации (Далее – УК РФ), так и организацию деятельности, направленной на побуждение к самоубийству (ст. 110.2 УК РФ) в том числе с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»).

Для того, чтобы оценить достаточность и полноту данных уголовно-правовых норм, необходимо проанализировать их, исходя из общей теории уголовного права. При этом, криминологический анализ феномена деятельности, направленной на побуждение других лиц к

самоубийству, крайне важен для выработки на государственном уровне стратегии противодействия данной деструктивной преступной деятельности. Сказанное подтверждает актуальность названной темы.

Современный мир сложно представить без развития информационных технологий, позволяющих человеку достаточно свободно обмениваться информацией с другими людьми, независимо от места его нахождения, для чего достаточно лишь доступа в сеть «Интернет». Однако, к сожалению, данные технические достижения активно используются и в противоправных целях – при помощи «Интернета» могут совершаться преступные деяния, посягающие на самые разные общественные отношения, в том числе, способные повлечь за собой смерть человека.

Дети и молодежь являются одной из самых уязвимых категорий населения для преступлений, совершаемых в «Интернете». Это связано с различными обстоятельствами сформировавшуюся психику, подверженные категоричным эмоциональным решениям и действиям в своей жизни, могут попадать под деструктивное влияние.

Названные причины, в определенной степени, облегчают преступную деятельность, направленную на молодежную среду. Примерно с 2015 г., широкий общественный резонанс приобрела деятельность так называемых «групп смерти» в социальных сетях, основной аудиторией которых являются подростки.

Как отмечает Н. Е. Крылова, деятельность организаторов «групп смерти» заключается в вовлечении их подписчиков в, своего рода, интерактивную игру, в которой подросткам даются задания, так или иначе связанные с тематикой суицида [1, с. 52].

Однако, можно отметить, что деятельность таких деструктивных сообществ, независимо от того, используют ли они формат игры, в любом случае, подчинена формированию у его участников мнения о том, что самоубийство является выходом из сложной ситуации.

Для этих целей, в тех же группах могут размещаться фотографии, видео, другие материалы, которые направлены на пропаганду культа смерти, создания у подростков общего депрессивного настроя.

М. Ю. Пучнина делит деятельность таких групп на несколько стадий [2, с. 361]:

Первая стадия – вовлечение несовершеннолетнего в деструктивное сообщество. На данном этапе так называемые «кураторы» находят подростков, интересующихся всем, что связано с суицидом, по кодовым словам, размещенным ими на своих страницах в социальных сетях или участию в группах с соответствующими названиями («Синий кит», «Море китов» и т.п.).

Как отмечают в этой связи А. Е. Шалагин и А. Д. Идиятулов, интерес преступников направлен, прежде всего, на детей и подростков, находящихся в кризисной ситуации из-за проблем в учебе, отношениях с родителями и сверстниками, предлагают «решение» всех данных проблем в обмен на обязанность выполнять предлагаемые задания и никому не сообщать об участии в сообществе [2, с. 361].

Вторая стадия заключается в непосредственном участии несовершеннолетнего в деятельности деструктивной группы, с наиболее возможным отрывом его от реальной жизни.

На этой стадии «куратор» может давать ему различные задания, которые изначально не связаны напрямую с причинением вреда себе – например, просмотр различных материалов, направленных на убеждение в привлекательности смерти, ее эстетичности, и оправданности суицида.

Третья стадия уже наиболее опасна, поскольку «кураторы» предлагают подросткам выполнить задания, связанные с нанесением себе порезов и других увечий, с фиксацией этого процесса на фото или видео.

Это рассматривается, как определенное «посвящение», после которого задания становятся приближенными к непосредственному совершению суицида, и завершаются им. Не случайно, в связи с этим, задания, даваемые «куратором» деструктивных сообществ, должны выполняться

несовершеннолетним глубокой ночью, что отрицательно сказывается на возможности адекватно воспринимать действительность.

Сложность в выявлении деятельности по склонению несовершеннолетних к самоубийству заключается также в том, что лицо, ее осуществляет, может длительный период не попадать в поле зрения правоохранительных органов.

Для сравнения, можно отметить, что если иная преступная деятельность может требовать, например, приобретения запрещенных к гражданскому обороту предметов (наркотических средств, оружия и т. п.), то для того, чтобы дистанционно побуждать других лиц к совершению самоубийства, достаточным является лишь приобретение необходимых технических средств для выхода в «Интернет».

Кроме того, если лица, объединяющиеся в организованную группу или преступное сообщество, либо банду, с целью совершения других преступных деяний, нередко имеют неоднократную судимость, в отношении создателей и кураторов «групп смерти» таких лиц практически нет.

Указанное обстоятельство представляется возможным подтвердить судебной практикой. Так, например, в 2017 г. В., пользуясь общедоступной социальной сетью «Вконтакте», создал собственное сообщество, размещая в нем материалы, оправдывающие суицид несовершеннолетних и призывающие к нему.

Ведя переписку с участниками данного сообщества, посредством указанной выше социальной сети, он давал лицам, которых считал несовершеннолетними, находящимися в тяжелой жизненной ситуации, указания, связанные с причинением вреда их здоровью – призывал нанести порезы на различные части тела, фотографироваться различных опасных для жизни местах, а также, побуждал их совершить самоубийство различными способами.

Рассматривая уголовное дело в отношении В., суд установил, что основным мотивом данных действий с его стороны было самоутверждение себя как человека способного руководить действиями других лиц, при этом, ранее судим В. не был, на учете у врача-нарколога и психиатра не состоял [3].

В 2018 г. Б., также используя мобильный телефон и планшетный компьютер, вступала в переписку с несовершеннолетними лицами, с использованием различных психологических приемов, склонила несовершеннолетнюю Ф. к совершению суицида, предлагая ей выполнить задания, которые связаны с нанесением порезов и других повреждений на теле и руках, а также, с рядом других опасных для жизни и здоровья действий.

Б. также не использовала для своей преступной деятельности запрещенные к обороту предметы и ранее не была судима, при этом, совершенные ей деяния были выявлены случайно, когда родители несовершеннолетней Ф. обнаружили переписку дочери с Б., имеющую соответствующее содержание [4].

Из материалов другого уголовного дела следует, что Г., также пользуясь социальной сетью «Вконтакте», получила информацию о тяжелом психоэмоциональном состоянии П., и склоняла ее к совершению самоубийства, путем демонстрации ей фотоматериалов суицидального характера, а также, давала советы по поводу различных способов самоубийства.

Как и в ранее указанном деле, Г. прежде не была судима, не находилась в поле зрения правоохранительных органов и каким-либо иным образом [5].

Данные обстоятельства значительно усложняют выявление и пресечение деятельности, которая направлена на склонение несовершеннолетних к самоубийству, и, в то же время, подтверждают необходимость активного использования современных технологий и сети «Интернет» для противодействия данным преступным проявлениям.

В целом, исходя из изложенного выше, можно сделать следующие выводы:

1.Деятельность по склонению несовершеннолетних к совершению самоубийства имеет высокую общественную опасность, поскольку совершается лицами, использующими приемы

психологического воздействия на подростков, как правило, находящихся в состоянии депрессии и не имеющих достаточного взаимопонимания в семье и в кругу друзей;

2.Характерным признаком действий, целью которых является склонить несовершеннолетнее лицо к суициду, представляется возможным считать, как правило, дистанционный характер этих действий, поскольку они совершаются через сеть «Интернет», лицами, скрывающими свои данные, и использующими методы конспирации (закрытые группы в социальных сетях, использование кодовых слов, псевдонимов и т.п.), при этом, преступник может иметь существенную территориальную удаленность от места жительства потерпевших;

3.Фактором, усложняющим выявление и пресечение действий, направленных на побуждение несовершеннолетних к суициду, является использование ими легальных технических средств (персональные компьютеры, мобильные телефоны, ноутбуки и т. п.) и популярных социальных сетей, при этом, за пределами сети «Интернет» могут не проявлять преступного поведения.

В целях корректной организации профилактической работы с несовершеннолетними необходимо в первую очередь проработать возможности психологической поддержки, включаю короткие памятки для классных руководителей и родителей с учетом базовых положений [6, с. 142].

Кроме того, необходимо ориентировать родителей и классных руководителей на проведение регулярного мониторинга социальных сетей ребенка на предмет выявления наиболее распространенных индикаторов «групп смерти».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Крылова Н.Е. «Группы смерти» и подростковый суицид: уголовно-правовые, психологические и психиатрические аспекты // Психическое здоровье человека и общества. – 2017.– № 3.– С. 52.
2. Шалагин А.Е., Идиятуллов А.Д. О мотивации преступного и суицидального поведения // Вестник Казанского юридического института МВД России. – 2019. – №3 (37). – С. 361.
3. Приговор Звериноголовский районный суд Курганской области от 10.01.2019 г. по делу № 1-3/2019 [электронный ресурс] – URL: http://zverinogolovsky.krg.sudrf.ru/(дата обращения: 15.10.2021 г.)
4. Приговор Татарского районного суда Новосибирской области от 04.04.2018 г. по уголовному делу № 1-46/2018 [электронный ресурс] – URL: http://tatarsky.nsk.sudrf.ru/modules.php?name=press_dep&op=4&did=51 (дата обращения: 15.10.2021 г.)
5. Приговор Судакского районного суда Республики Крым от 7 мая 2018 г. по делу № 1-25/2018[электронный ресурс] – URL: http://sudak.krm.sudrf.ru/ (дата обращения: 15.10.2021 г.)
6. Раненкова Е.А., Осипова Д.А. Актуальные вопросы профилактической работы по предотвращению вовлечения несовершеннолетних в «группы смерти» В сборнике: Уголовное судопроизводство по делам несовершеннолетних и ювенальная юстиция: проблемы и перспективы развития (правовые, социальные и психолого-педагогические аспекты). Сборник статей научно-представительских мероприятий. Коллектив авторов. 2021. С. 139-142.

Максимов М.М.
Курсант 3 курса прокурорско-следственного факультета Военного Университета Министерства Обороны

Maksimov M. M.,
3st year cadet of the Faculty of Law of the prosecution and investigation of the Military University of the Ministry of Defense

ПРОБЛЕМЫ ОТЕЧЕСТВЕННОГО УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА И ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ В СФЕРЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В ТЕНЕВОЙ СЕТИ (ДАРКНЕТ)

PROBLEMS OF DOMESTIC CRIMINAL LEGISLATION AND LAW ENFORCEMENT PRACTICE IN THE FIELD OF CRIMES COMMITTED IN THE SHADOW NETWORK (DARKNET)

Аннотация: В статье рассмотрена ретроспектива зарождения и развития сети «интернет», послужившая отправной точкой для образования субсети «даркнет». Определены необходимые векторы упорядочения сферы общественных отношений в инфокоммуникационной сети, сделаны определенные выводы и предложения по оптимизации отрасли в целом. Детальному изучению подвергнута субсеть всемирной сети интернет «даркнет». Также рассмотрены основные проблемы уголовного законодательства и правоприменительной практики РФ в сфере преступлений, совершаемых в теневой сети (даркнет).

Abstract: The article considers a retrospective of the origin and development of the Internet network, which served as a starting point for the formation of the Darknet subnetwork. The necessary vectors for the development of the ordering of the sphere of public relations in the infocommunication network are determined, certain conclusions and proposals for optimizing the industry as a whole are made. A detailed study has been made of the "darknet" sub-network of the world Wide Web, the contents of which have been subjected to empirical research in the form of content analysis. The main problems of criminal legislation and law enforcement practice of the Russian Federation in the field of crimes committed in the shadow network (darknet) are also considered.

Ключевые слова: интернет, даркнет, преступность, преступления, киберпреступники, наркотики, правовое регулирование, уголовное законодательство

Keywords: Internet, darknet, crime, crimes, cybercriminals, drugs, legal regulation, criminal legislation

Продвижение научно-технического прогресса позволяет повысить уровень безопасности в обществе, однако преступность непрерывно развивается и подстраивается под новые реалии. Так, после появления банкоматов преступники сразу изобрели устройство для считывания информации с банковских карт, которое устанавливалось на приемниках этих средств платежа. Сотрудники служб безопасности обратили внимание на участившиеся случаи хищений и узнали о существования данных устройств. Чтобы предотвратить кражи денежных средств, было принято решение устанавливать прозрачный пластик на приемники карт. Банкоматы были усовершенствованы, но при совершенствовании различных методов предупреждения преступлений одновременно происходит и обновление способов совершения этих деяний.

Теневой Интернет – это скрытая группа веб-сайтов, которая доступна только через специализированные браузеры [2]. Они используются для сохранения анонимности и конфиденциальности онлайн-деятельности, как законной, так и незаконной. В то время как одни пользователи используют эти браузеры для посещения заблокированных государством интернет-ресурсов, другие, в свою очередь, занимаются деятельностью, которую нельзя назвать законной.

«Первые русскоязычные сайты в теневом интернете появились еще в 2012 году, что было связано с распространением в России такого браузера, как Tor. По данным TOR Metrics с начала 2018 года Российская Федерация заняла четвертое место в мире по числу пользователей теневой паутины, более 250 тысяч жителей нашей страны ежедневно выходят в теневой Интернет, на которых приходится около 10% общемирового числа пользователей данной сетью» [3].

Теневой Интернет заработал репутацию платформы для преступной деятельности и размещения незаконного контента, а также торговли услугами и запрещенными товарами. Тем не менее, законопослушные граждане также могут воспользоваться теневой паутиной.

В теневом Интернете есть как положительные, так и отрицательные стороны. Если более детально разобраться, то теневая паутина действует как рай для демократии и борьбы с коррупцией. Здесь пользователи могут сообщать прессе о неправомерных действиях корпораций и правительства, не опасаясь возмездия, рассекречивать коррупционные действия, скрытые от общественности. Эта сеть имеет полную свободу слова и информации. Теневая сеть – это также место, где люди из репрессивных стран или религий могут найти единомышленников и даже получить помощь [8]. И, конечно же, теневая паутина – это место для журналистов и людей с очень нестандартным образом жизни, позволяющее общаться в сети и не бояться репрессий.

DeepWeb («глубокая паутина», «глубокая сеть», «глубокий Интернет») – область Интернета, которая скрыта от общественности и не индексируется поисковыми машинами. Данная часть Интернета содержит около 96% всей информации в сети. В ней содержатся базы данных, служебные части сайтов, просто скрытые страницы и т.д. Несмотря на то, что содержащиеся в этой части Интернет данные не индексируются поисковыми машинами, к большинству из них можно получить доступ без каких-либо специальных средств, используя обычный браузер и пройдя процедуру аутентификации.

Отдельной частью DeepWeb является так называемая DarkWeb («темная сеть»), которая преднамеренно и надежно скрыта от глаз обычных пользователей, в которой решающее значение имеет анонимность. Для обозначения данной части сети Интернет также достаточно часто используется название «Даркнет» (от англ. DarkNet – темная сеть, темный Интернет). Именно под этим названием данный сегмент Интернет наиболее широко известен российским пользователям.

Пир (от английского «peer» равноправный, исходящий от членов своей группы) – это участник сети. При использовании программного обеспечения участники сети тотчас же становятся «пирами». Число пиров отображает общее количество раздающих и загружающих файлообменников. Данные в анонимной сети передаются между собой посредством виртуальных каналов в зашифрованном виде.

Темный интернет по многим аспектам схож с общедоступным Интернетом: он имеет собственные поисковые системы, интернет-магазины, новостные сайты и социальные сети. Однако его существенной особенностью является то, что большинство расположенных в нем сайтов занимается нелегальной деятельностью [1].

Прежде всего, сайты в темном интернете используются для незаконного оборота наркотиков. Ежегодно на таких сайтах проводятся десятки и даже сотни тысяч таких транзакций, оплата производится в биткоинах [1]. Далее товары доставляются по указанному адресу как обычные товары, купленные на Amazon или Ebay. Единственное отличие в том, что в этом случае все происходит анонимно. Россия на данный момент занимает второе место в мире по количеству пользователей даркнета с точки зрения оборота психоактивных веществ [5]. В теневой паутине свободно возможно купить оружие, а также всевозможные нелегальные услуги: например, там можно арендовать сетевых ботов или заказать кибератаку у профессиональных хакеров. Желающий может купить компьютерные вирусы, «черви», «трояны» и тому подобное. «В России оружие через теневой интернет приобретается не так часто. На одних из самых крупных форумов можно найти всего пару сайтов с каталогами оружия и номерами продавцов. Приобретается оно обычно по 50 или 100% предоплате через криптовалюту или фейковые платежные аккаунты, а

получить оружие можно через «закладку» или курьером, в таком случае оно обычно пересылается отдельными частями» [2].

Помимо всего прочего «в даркнете можно обнаружить объявления о таких услугах, как слежка, поджог дома или машины, ограбление и избиение человека, фальсификация уголовных дел. Также можно наткнуться на такие услуги, как обмен и вывод денежных средств, финансовое мошенничество. Обычно за определенный процент от суммы, чаще всего это около 10%, могут перевести деньги из криптовалюты в российские рубли, а также по желанию в доллары или евро» [3].

В теневом интернете «встречаются» и другие противозаконные действия, которые уголовно наказуемы в Российской Федерации, такие как: «распространение детской порнографии и объявления об услугах сексуального характера, продажа и приобретение поддельных паспортов и других документов, а также фальшивых купюр и медицинских препаратов. На просторах даркнета наряду со всем можно найти услуги по взлому аккаунтов в соцсетях» [4].

Даркнет не является в полной мере негативным явлением социума, а скорее детерминантом преступности, то есть одним из конкретных факторов порождающих киберпреступность, обусловливают ее существование в некоторых аспектах. Для того, чтобы доказать это, необходимо обратиться к краткой истории появления и развития теневой сети [3].

Если представить подводную часть айсберга, то там находится «глубинный интернет» (deepweb от английского deep – глубокий и web – сеть). По мнению журналиста и исследователя из Берлина Альбрехта Уде, через поисковики можно найти лишь около 4% информации, тогда как оставшиеся 96% – подводная часть айсберга – это данные из скрытого глубинного интернета. Чтобы получить к ним доступ нужно иметь верифицированный аккаунт. К ним относится информация из социальных сетей, закрытых форумов, запароленных сайтов и миллионов баз данных. Глубинная сеть похожа на теневой интернет, хотя информация в ней не индексируются поисковыми системами, но хранится в открытом доступе при соблюдении определенных условий.

Исследования статистики пользователей браузера Tor показали, что что 11 июля 2019 года более 600 тысяч российских пользователей воспользовались данной сетью, это стало историческим рекордом по количеству интернет-посетителей. В этот день Россия, обойдя США и Иран, заняла первое место по количеству пользователей.

Использование новых технологий всегда влияет на преступность. Так, на общий объем и раскрываемость преступлений в стране повлиял рост количества преступных посягательств, совершаемых с использованием информационно-телекоммуникационных (IT) технологий. На выступлении в Совете Федерации глава МВД РФ – Владимир Колокольцев, сообщил, что доля киберпреступлений в общем числе преступлений увеличилась и достигла 23%, это почти 25% от общего числа совершаемых преступлений в России: «В целом на деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, по-прежнему приходится одно из четырех регистрируемых в текущем году преступлений (461,2 тыс.). Двумя годами ранее удельный вес таких деяний был втрое меньше». Однако темп роста совершаемых киберпреступлений во второй половине 2020 года немного замедлился с 91,7% до 76,6%.

Современные технологии позволили упростить процесс совершения преступлений, а также предоставили новые инструменты для противоправных деяний. Сегодня преступники уже освоили различные виртуальные платформы, Telegram-каналы, мессенджеры, и вебсайты в Даркнете, устройства бесконтактной оплаты NFC. FATF (международная межправительственная организация, группа разработки финансовых мер борьбы с отмыванием денег) определяет, что современные условия обеспечивают возможности для активного использования виртуальных технологий для функционирования преступной деятельности, в Интернете, особенно в Даркнете,

появляются открытые призывы к анонимному сбору средств на террористическую деятельность с помощью переводов электронных денег и криптовалюты.

В России для борьбы с распространением запрещенного контента не так давно был создан «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», далее черный список. Если какой-либо Интернет-ресурс находится в этом списке, то все российские Интернет-провайдеры обязаны заблокировать к нему доступ для своих клиентов, но так как блокировка работает только в пределах Российской Федерации, пользователь по-прежнему может доступ к заблокированному Интернет-ресурсу, например, с помощью прокси-сервера или VPN.

Если мы говорим о продаже персональных данных, то нормативно-правовую базу, регламентирующую порядок обработки и защиты в целом, составляют Конституция Российской Федерации, ФЗ «О персональных данных», ФЗ «Об информации, информационных технологиях и о защите информации». Они действуют как в общедоступной части интернета, так и в Даркнете, а также в локальных сетях, доступных узкому кругу пользователей.

Наиболее распространенным мнением относительно квалификации деяний, совершаемых с использованием информационных технологий, является их отнесение к компьютерным преступлениям, или киберпреступлениям [6], под которыми понимается совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству [8].

Вместе с тем с данным утверждениями можно поспорить, учитывая тот факт, что компьютерная информация является предметом преступления только в гл. 28 Уголовного кодекса Российской Федерации (УК РФ) «Преступления в сфере компьютерной информации». В составах преступлений, связанных с распространением порнографических материалов с помощью сети Интернет (п. «б» ч. 3 ст. 242 УК РФ, п. «г» ч. 2 ст. 242.1, п. «г» ч. 2 ст. 242.2 УК РФ), использование информационно-телекоммуникационных сетей является квалифицирующим признаком, а в ст. 132 УК РФ (насильственные действия сексуального характера) и ст. 135 УК РФ (развратные действия) использование информационно-телекоммуникационных сетей представляет собой один из способов совершения преступления, хотя и не является квалифицирующим признаком в соответствии с уголовным законодательством [5].

Подходы к государственному контролю и правовому регулированию Даркнета можно разделить на 3 группы:

1.государственная позиция, согласно которой Даркнет должен быть запрещен, поскольку он используется в криминальных целях и не позволяет идентифицировать правонарушителей;

2.позиция сторонников свободного интернета, выступающих против любого вмешательства и контроля со стороны государства;

3.подход, учитывающий невозможность запрета Даркнета и нейтральность оценки самой анонимной технологии социальной коммуникации. При этом в рамках последнего подхода отмечается необходимость как технического, так и правового ответа на угрозы, которые несет Даркнет.

Полагаем, что третья позиция наиболее сбалансирована, поскольку в ней Даркнет предстает как инструмент, который приобретает общественную опасность в связи с преступными целями пользователей, а не сам по себе. Кроме того, текущий уровень развития не позволяет государствам блокировать использование Даркнета. Вместе с тем необходимо вырабатывать правовые и технические средства борьбы с его опасными проявлениями.

Законодательным и правоприменительным органам в ближайшем будущем надлежит уделить особое внимание выпавшей на наш взгляд из правового поля и административного поля субсети «даркнет», в рамках чего необходимо поставить вопросы о:

- оперативном упорядочении пользования сетью «даркнет»;

- разработке административно-правовых методик ограничения использования TOR-браузеров на территории Российской Федерации;

- качественной методико-технической подготовке специалистов, непосредственно занимающихся деятельность по выявлению противоправных деликтов в рассматриваемой среде.

Таким образом, сложившаяся ситуация требует от государства принятия комплекса мер, направленных на противодействие преступности в Даркнете. Представляется, что помимо опережающего нормативного регулирования соответствующий комплекс мер должен обусловливаться и современными техническими решениями, позволяющими выйти на качественно новый уровень международного сотрудничества оперативно-технических подразделений компетентных органов. Так, МВД России объявило закрытый конкурс на выполнение научно-исследовательской работы по исследованию возможностей получения данных о пользователях анонимной интернет-сети TOR. Заказчиком проекта выступило научно-производственное объединение «Специальная техника и связь» МВД России [3].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Иванцов С.В. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С.В. Иванцов, Э.Л. 288 Сидоренко, Б.А. Спасенников, Ю.М. Березкин, Я.А. Суходолов // Всероссийский криминологический журнал. – 2019. – Т. 13, № 1. – С. 85–93.

2. Ларина Е. Криптовалюта: свет и тени / Е. Ларина, В. Овчинский // Наш современник. – 2018. – № 8. – С. 214–224.

3. Мазур А.А. Актуальные проблемы предупреждения преступности в социальной сети Даркнет /А.А. Мазур// Вестник Российского института кооперации. – 2018. – № 3 – С. 125–129.

4. Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты / В.А. Перов. – М.: Юрлитинформ, 2017. – 200 с.

5. Романова Л.И., Дремлюга Р.И. Преступный мир DarkNet // Юридическая наука и практика. – 2018. – Т.14, №1. – С. 52-60.

6.Сидоренко Э.Л. Наркопреступность в сети «Интернет»: современные криминологические тренды / Э.Л. Сидоренко // Наркоконтроль. – 2018. – № 4. – С. 13–18.

7. Секреты Даркнета. Ищем полезное в скрытых сервисах Tor [Электронный ресурс]. – Режим доступа: https://www.cena5.ru/sekrety-darkneta-ishchem-poleznoe-v-skrytyh-servisah-tor-krome-oruzhiya-i.html (15.11.2021).

8. Что такое тор браузер? Анонимная луковичная программа и как его скачать? [Электронный ресурс]. – Режим доступа: https://yandex.ru/turbo?text=https%3A%2F%2Fwww.iqmonitor.ru%2Fanonim%2Ftor-brauser.html (15.11.2021).

Меерсон В.Р.
адъюнкт факультета подготовки научно-педагогических и научных кадров,
Московский университет МВД России имени В.Я. Кикотя /
Академия МВД Республики Беларусь

Meerson V. R.,
postgraduate student of the
Faculty of Preparation of Scientific and Pedagogical staff
V.Ya. Kikot' Moscow University of the
Ministry of Internal Affairsof the Russian Federation /
Academy of the Ministry of Internal Affairs of the Republic of Belarus

О НЕКОТОРЫХ, АКТУАЛЬНЫХ В НАСТОЯЩЕЕ ВРЕМЯ, ОСОБЕННОСТЯХ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ФУНКЦИОНИРОВАНИЯ УЧРЕЖДЕНИЯ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

ABOUT SOME, CURRENTLY RELEVANT, FEATURES OF THE CRIMINAL LEGAL PROTECTION OF THE FUNCTIONING OF THE ESTABLISHMENT OF THE CRIMINAL EXECUTIVE SYSTEM

Аннотация. Рассмотрены некоторые вопросы, касающиеся норм действующего уголовного законодательства Российской Федерации и Республики Беларусь, предусматривающие ответственность за действия, дезорганизующие функционирование учреждений уголовно-исполнительной системы.

Annotation. Some issues regarding the norms of the current criminal legislation of the Russian Federation and the Republic of Belarus are considered, providing for responsibility for actions that disorganize the functioning of the penitentiary system.

Ключевые слова: дезорганизация деятельности пенитенциарных учреждений, уголовное право, ст. 321 УК Российской Федерации, ст. 410 УК Республики Беларусь**.**

Keywords: disorganization of the activities of prisons, criminal law, Art. 321 of the Criminal Code of the Russian Federation, Art. 410 of the Criminal Code of the Republic of Belarus.

В настоящее время внедрение в различные сферы жизнедеятельности информационных технологий играет особую роль и в процессе развития современной уголовной политики любого государства, влияет на процесс сотрудничества с целью борьбы с преступностью между странами. Не обошел этот процесс мимо двустороннее взаимодействие между Российской Федерацией и Республикой Беларусь. Наступившая информационная эра детерминирует возможность чрезвычайно быстрого обмена сведениями о совершенных преступлениях, передовым правоприменительным опытом, новеллами в законодательстве не только внутри одной страны, но и за ее пределами. Указанное обстоятельство является достаточно позитивным в силу продолжающихся интеграционных процессов в рамках Союзного государства Республики Беларусь и Российской Федерации, которые на данный момент получили новый виток в своем развитии.

Обмен опытом, двустороннее сотрудничество, немаловажны для качественного противодействия преступности, в том числе и в сфере функционирования пенитенциарных учреждений. Несмотря на особенности близкого взаимодействия двух стран и взаимного стремления к гармонизации законодательств, до настоящего времени нет единства в подходах к пониманию различного рода уголовно-правовых институтов. Прежде всего следует обратить внимание на расхождение в регламентации и содержании в Уголовных кодексах двух стран такого преступления, как дезорганизации функционирования исправительных учреждений (мест

содержания под стражей). Актуальность указанного вопроса обуславливается достаточно важной сферой деятельности государства, которой является обеспечение исполнения судебных решений, в частности реализация назначаемых судами наказаний, а также поддержания на должном уровне функционирования соответствующей системы органов и учреждений. Безусловно, без эффективной работы уголовно-исполнительной системы, ее отдельных звеньев, сложно представить оконченным поступательный механизм борьбы с преступностью в любом государстве, вне зависимости от исторической эпохи и общественно-экономической формации. В этой связи особое значение приобретают устанавливаемые уголовно-правовые запреты, направленные на определенное общественно опасное поведение лиц, содержащихся в местах изоляции от общества.

Сравнительно-правовое исследование уголовно-правовых норм, направленных на противодействие преступлениям, дезорганизующим деятельность исправительных учреждений, в настоящее время обладает особой актуальностью. В частности, научный интерес представляет рассмотрение ст. 321 УК Российской Федерации [1] и ст. 410 УК Республики Беларусь [2], выделение специфики объективных и субъективных признаков составов соответствующих преступлений. Указанные преступления характеризуются высоким уровнем латентности, многие деяния, содержащие признаки анализируемых составов, могут расцениваться администрацией пенитенциарных учреждений как дисциплинарные правонарушения. Вместе с тем, высокая превентивная направленность данных норм, необходимость принятия решений о правильной квалификации подобного рода деяний, отсутствие современных исследований, касающихся данной тематики (в особенности в уголовно-правовой науке Республики Беларусь), обуславливают необходимость в достаточно детальном изучении и рассмотрении указанного преступления.

В правоприменительной практике и науке уголовного права Российской Федерации и Республики Беларусь в связи с применением исследуемой нормы усматриваются множество проблем. Например, нет единства в понимании объекта, субъекта рассматриваемого преступления, вызванного различиями в подходах национальных законодателей; в современной судебной практике отсутствуют толкования важных дефиниций, что влечет проблемы при квалификации. Законодателем не учитывается современное состояние, структура, тенденции развития органов уголовно-исполнительной системы (мест содержания под стражей). В частности, дискуссионным является подход белорусского законодателя к повышенной уголовной ответственности лиц, осужденных за тяжкие (особо тяжкие) преступления, в случае совершения ими действий, дезорганизующих функционирования учреждений уголовно-исполнительной системы. Использование подобного квалифицирующего признака выглядит не совсем оправданным, так как в данном случае «презюмируется с одной стороны, что совершенное посягательство имеет большую общественную опасность исходя из субъекта, совершающего его, с другой стороны благодаря данному квалифицирующему признаку количество лиц, осужденных по ч. 2 ст. 410 УК Республики Беларусь, значительно превышает (в 2,4 раза), число лиц, привлекаемых по основному составу исследуемого преступления» [3, с. 84]. Представляется, что личность виновного, его характеристика, должны рассматриваться не как инструмент криминализации, а как средство дифференциации или индивидуализации наказания.

Таким образом, существующие в настоящее время в Российской Федерации и Республике Беларусь конструкции статей, предусматривающих уголовную ответственность за действия, дезорганизующие функционирование учреждений уголовно-исполнительной системы, требуют детального анализа, а также определенной редакции в целях гармонизации. Представляется целесообразным рассмотреть вопрос об исключении квалифицирующих признаков из ст. 410 УК Республики Беларусь и рассмотреть возможность использования опыта российского законодателя в рамках совершенствования конструкции данной статьи. Вместе с тем имеет место быть и позитивные решения белорусского законодателя в рамках определения субъекта, объекта

и потерпевших в рассматриваемом преступлении, что также может быть использовано при совершенствовании ст. 321 УК Российской Федерации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (в ред. от 01.07.2021 № 292-ФЗ). URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891 (дата обращения: 30.11.2021).

2. Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З (в ред. от 26.05.2021 № 112-З). URL: https://pravo.by/document/?guid=3871&p0=hk9900275 (дата обращения: 30.11.2021).

3. Меерсон, В. Р. О квалифицирующих признаках действий, дезорганизующих работу исправительных учреждений (по уголовному законодательству Республики Беларусь) / В. Р. Меерсон, С. Ю. Мельников // Актуальные вопросы права, образования и психологии: Сборник научных трудов. – Могилев: Учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь», 2021. – С. 80-85.

Молчанова С.М.
Студентка 1-го курса магистратуры
Международного юридического института

Molchanova S.M.
1st year student of the International Law Institute

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРИВЛЕЧЕНИЯ К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ДЕТОУБИЙСТВО

CURRENT PROBLEMS OF LEGAL REGULATION OF CRIMINAL RESPONSIBILITY FOR CHILD MURDER

Аннотация. Автором статьи рассматриваются основные проблемы правового регулирования привлечения к уголовной ответственности за детоубийство (статья 106 УК РФ «Убийство матерью новорожденного ребенка») и пути их решения. Автор приходит к выводу, что законодатель не в полной мере продумал пункт «в» части 2 статьи 105 Уголовного кодекса Российской Федерации и не закрепил признак, который положен в основу смягчения наказания за совершение детоубийства.

Annotation. The author of the article examines the main problems of legal regulation of Article 106 of the Criminal Code of the Russian Federation "Murder of a newborn child by a mother" and ways to solve them. The author comes to the conclusion that the legislator did not fully think over paragraph "c" of part 2 of Article 105 of the Criminal Code of the Russian Federation and did not consolidate the feature that underlies the mitigation of punishment for committing infanticide.

Ключевые слова. Убийство, решение, дети, право, закон, проблемы, законодательство, уголовное право, криминология.

Keywords. Murder, decision, children, law, law, problems, legislation, criminal law, criminology.

Насильственная преступность составляет достаточно объемный пласт над процентом преступности в России, самое ужасное состоит в том, что противоправные деяния касаются права на жизнь ребенка. Каждое государство ставит себе за цель увеличение рождаемости, так как новое поколение (дети) – ее основное наследие, гарантия перспективы функционирования и также формирования. Убийства детей отрицательно сказываются в единой демографической ситуации в государстве, подрывают концепцию ее общегосударственной защищенности, поэтому охрана существования любого из детей обязана быть главной ценностью уголовно-правовой политики страны.

В научной доктрине уголовного права термин «детоубийство», зачастую применяется к убийству матерью новорожденного ребенка, в то время как должен употребляться в более широком значении, параллельно охватывая собой и убийство малолетнего. Применение термина «детоубийство» как для привилегированного и квалифицированного составов преступления, содержащих санкцию для действий, направленных на лишение жизни детей, вполне обоснованно, так как это позволяет провести детальный анализ актуальных проблем уголовно-правовой регламентации ответственности за детоубийство.

В российском уголовном законодательстве, ответственность за убийство детей установлена в пункте «в» ч. 2 ст. 105 Уголовного кодекса Российской Федерации (УК РФ), где сказано: «малолетнего или иного лица, заведомо для виновного находящегося в беспомощном состоянии, а равно сопряженное с похищением человека», данный пункт регулирует ответственность за убийство малолетнего в рамках квалифицированного состава преступления, а ст. 106 УК РФ «Убийство матерью новорожденного ребенка» – в рамках привилегированного

состава, где выделяется специальный субъект преступления-это мать новорожденного ребенка, которого умертвили. Как утверждают в своем труде ученые: «Самостоятельное значение закон придает наличию психотравмирующей ситуации, в которой оказывается роженица. Эта ситуация может возникнуть как в непосредственной связи с процессом родов, так и быть обусловленной иными причинами (в частности, отказом отца ребенка признать его своим, травлей женщины родственниками)» [1, с. 231].

Помимо этого, не будет лишним отметить тот факт, что пунктом «в» ст. 105 УК РФ, помимо ответственности за убийство малолетних, предусмотрена ответственность за убийство лица, заведомо для виновного, находящегося в состоянии беспомощности, в связи с этим, дифференцировать по статистике эти преступления не представляется возможным. Вышеперечисленное обстоятельство определяет потребность выделения убийства малолетнего в самостоятельный квалифицирующий признак ч. 2 ст. 105 УК РФ. Данное законодательное решение даст возможность создать систему уголовных противоправных деяний, регламентирующих ответственность за детоубийство, а также реализовывать статистическую градацию, по учету количества убийств малолетних детей, совершенных на территории Российской Федерации.

Придание узкого обхвата дефиниции «детоубийство», влечет за собой и сложность конструкций норм в Уголовном кодексе Российской Федерации. Если рассматривать основополагающую для назначения ответственности за убийство ребенка, статью «Убийство матерью новорожденного ребенка», то можно заметить, что она предусматривает три вида убийства: убийство матерью новорожденного ребенка во время или сразу же после родов; убийство матерью новорожденного ребенка в условиях психотравмирующей ситуации; убийство матерью новорожденного ребенка в состоянии психического расстройства [2, с. 209].

Для квалификации основное значение имеет время: во время или сразу же после родов. Начало и окончание родов дается в статье 53 Федерального закона от 21.11.2011 № 323– ФЗ [3].

Термин «новорожденный» законодательно закреплен в «Охране репродуктивного здоровья работников. Основные термины и понятия» [4].

Помимо этого, отсутствие законодательного закрепления признака, который был положен в основу для смягчения наказания за совершенное деяние, является все еще актуальной проблемой правового регулирования детоубийства, которая требует урегулирования.

Если рассматривать диспозицию пункта «в» части 2 статьи 105 УК РФ, то можно также заметить, что понятие «малолетний» тоже не определено никакой законодательной базой, даже Постановление Пленума Верховного Суда Российской Федерации [5] не содержит в себе ответа на этот вопрос.

Ко всему этому добавляется проблематика отсутствия ссылки на заведомую осознанность виновным малолетнего возраста жертвы убийства.

Таким образом, анализируя вышеперечисленное, следует прийти к выводу, что недоработка норм в части правового регулирования несет за собой трудности не только в научном толковании, но и провоцирует проблемы их правильного практического применения, посредством несовершенства юридических конструкций статей.

Рассмотрев актуальные вопросы правового регулирования детоубийства, возникает необходимость предложения путей решения сложившихся проблем. Следует закрепить термин «малолетний» как ребенок, не достигший возраста четырнадцати лет, поскольку употребление в конструкциях различных уголовно-правовых норм различных дефиниций как «малолетний», «ребенок» и т. д. не способствует цельному толкованию и практическому применению уголовного законодательства. Данный термин можно включить в постановление Пленума Верховного Суда РФ от 01.02.2011 N 1[6].Выделение в самостоятельный квалифицирующий признак убийство малолетнего, будет способствовать вычленение его из общего числа статистических данных, предусмотренных п. «в» ч.2 ст.105 УК РФ и приведет к объективному пониманию состояния преступности в указанной сфере.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Журавлев М.П., Наумов А.В., Никулин С.И., Понятовская Т.Г., Рарог А.И., Яненко Б.В. Уголовное право России. Части Общая и Особенная (учебник; под ред. заслуженного деятеля науки РФ, д.ю.н., проф. А.И. Рарога; издание 10-е, перераб. и доп.). – "Проспект", 2018 г. 613 с.;

2. Уголовное право России. Общая и Особенная части: учебник/под ред. В. Ю. Голубовского. – Москва: Проспект, 2020. – 736 с.;

3. Федеральный закон от 21.11.2011 N 323-ФЗ (ред. от 02.07.2021) "Об основах охраны здоровья граждан в Российской Федерации" (с изм. и доп., вступ. в силу с 01.10.2021) // URL: http://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения: 08.11.2021).

4. Охрана репродуктивного здоровья работников. Основные термины и понятия (утв. Минздравом РФ 02.10.2003 N 11-8/13-09) (с изм. и доп.) // URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=366297#MJZLymSucr74ufDP (дата обращения: 26.10.2021);

5. Постановление Пленума Верховного Суда РФ от 27.01.1999 N 1 (ред. от 03.03.2015) "О судебной практике по делам об убийстве (ст. 105 УК РФ)" (с изм. и доп.) // URL: http://www.consultant.ru/document/cons_doc_LAW_21893/ (дата обращения:26.10.2021).

6. Постановление Пленума Верховного Суда РФ от 01.02.2011 N 1 (ред. от 28.10.2021) "О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних"//URL: http://www.consultant.ru/document/cons_doc_LAW_110315/ (дата обращения: 08.11.2021).

Патлань Е.С.
курсант 5 курса прокурорско-следственного факультета
Военного университета Министерства обороны Российской Федерации

Patlan E.S.
Fifth-year cadet of prosecuting and investigating faculty
of the Military University of the Russian Defense Ministry

Трунов Н.Ю.
курсант 5 курса прокурорско-следственного факультета
Военного университета Министерства обороны Российской Федерации

Trunov N.Y.
Fifth-year cadet of prosecuting and investigating faculty
of the Military University of the Russian Defense Ministry

ПРОБЛЕМНЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ СРЕДСТВ ОБЕСПЕЧЕНИЯ ПРАВОПРИМЕНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ВОЕННЫХ СЛЕДСТВЕННЫХ ОРГАНАХ

PROBLEMATIC ISSUES OF THE USE OF MEANS TO ENSURE LAW ENFORCEMENT ACTIVITIES IN MILITARY INVESTIGATIVE BODIES

Аннотация: В статье рассматриваются проблемы эффективности применения средств обеспечения, в том числе технико-криминалистических средств военными следственными органами Следственного комитета Российской Федерации при предупреждении, пресечении, раскрытии и расследовании преступлений.

Annotation: The article deals with the problems of effective use of security tools, including technical and forensic tools by military investigative bodies of the Investigative Committee of the Russian Federation in the prevention, suppression, detection and investigation of crimes.

Ключевые слова: следователь; военные следственные органы; следственные действий; технико-криминалистические средства.

Keywords: investigator; military investigative agencies; investigative actions; technical and forensic means.

Как показывает практика, в современных условиях эффективность работы следователей в значительной степени зависит от их оснащения современными научно-техническими средствами криминалистики. Данное направление деятельности может успешно развиваться лишь при достижении определенного компромисса между руководством Следственного комитета Российской Федерации и Главного военного следственного управления.

В частности, в 2012 году приняты меры по реализации Минобороны России, иными федеральными органами исполнительной власти, в которых законом предусмотрена военная служба, положений приказа «О нормах обеспечения криминалистической и специальной техникой Следственного комитета Российской Федерации» (далее – приказ СК России от 27.12.2011 № 159) [1].

В результате достигнутого соглашения в Росгвардии и ФСБ России изданы соответствующие организационно-распорядительные документы, касающиеся обеспечения военных следственных органов, содержащихся за счет штатной численности войск национальной гвардии Российской Федерации и ФСБ России, технико-криминалистическими средствами.

С Минобороны России эта работа продолжается.

Принимаются меры к улучшению качественных характеристик научно-технических средств. Систематически проводится их мониторинг, по мере возможности обновляется комплектация средств криминалистики.

В настоящее время обеспеченность военных следственных органов криминалистической и специальной техникой составляет: подвижными криминалистическими лабораториями – 67% (здесь и далее от положенного количества по нормам, установленным приказом СК России от 27.12.2011 № 159), универсальными криминалистическими комплектами – 60%, специализированными комплектами – от 43 до 79%.

Наиболее проблемным является обеспечение следователей современными средствами видео- и аудиозаписи и воспроизведения, в т.ч. цифровыми видеокамерами – 10%, видеомагнитофонами (видеоплеерами) – 2%, магнитофонами, комбинированными с аудиосистемой – 2%, магнитофонами-траскрайберами – 0%, цифровыми малогабаритными диктофонами – 11%, микрофонами направленными для диктофона – 1%, телевизорами (в т.ч. с видеоплеером) – 2%, DVD – проигрывателями – 3%, видеопроекторами – 11%.

Не поступили к настоящему времени на оснащение следственных подразделений системы бескраскового дактилоскопирования, комплекты для охраны места происшествия с возможностями аудио- и видеозаписи, универсальные геолокаторы (георадары), тепловизоры и т. д., предусмотренные приказом СК России от 27.12.2011 № 159.

В целом же в настоящее время технико-криминалистическая оснащенность военных следственных органов СК России обеспечивает минимально необходимую потребность для надлежащей организации работы следователей при раскрытии и расследовании преступлений.

Проведенным анализом установлено, что сотрудниками военных следственных органов наиболее часто в 2021 году применялась судебная фотография.

Так, при производстве следственных действий (доследственных проверок) фототехника использовалась в 9429 случаях, в том числе при осмотре мест происшествий – 2155, осмотре предметов и документов – 1824, допросах, очных ставках – 25, обысках, выемках – 258, проверках показаний на месте, следственных экспериментах – 4912, получении образцов для сравнительного исследования – 255. В 8622 случаях (91,4% от общего количества) фотосъемка производилась следователями военных следственных органов, в остальных – специалистами, экспертами, сотрудниками иных правоохранительных органов (8,6%).

Достаточно активно использовалась в работе следователей видеосъемка – 455 раз, в том числе при осмотре мест происшествий – 45, допросах, очных ставках – 260, обысках, выемках – 13, проверках показаний на месте, следственных экспериментах – 128, получении образцов для сравнительного исследования – 9. В 432 случаях (94,9% от общего количества) видеосъемка производилась следователями военных следственных органов, в остальных – иными лицами (5,1%).

Звукозапись (помимо видеозаписи) применялась в 106 случаях, в том числе при осмотре мест происшествий – 3, осмотре предметов и документов – 9, допросах, очных ставках – 56, проверках показаний на месте, следственных экспериментах – 8, получении образцов для сравнительного исследования – 30. В 91 случае (85,8% от общего количества) звукозапись производилась следователями военных следственных органов, в остальных – иными лицами (14,2%).

Из принадлежностей, входящих в комплектацию криминалистических комплектов, в текущем году наиболее часто использовались измерительные средства, в т.ч. линейки, рулетки, транспортиры – 2093 раза, лазерные дальномеры – 318.

Поисковые приборы применялись в 58 случаях (металлоискатели – 41, магнитные подъемники – 15, газоанализаторы – 2), УФ и ИК облучатели – 60, осветительные приборы – 283, оптические приборы, в т.ч. микроскопы, лупы, бинокли – 202, следокопировальные пленки – 71,

дактилоскопические порошки – 264, комплекты для дактилоскопирования – 151, приборы для отбора запаховых следов – 1.

Средства экспресс-анализа использовались: на наличие следов взрывчатых веществ – в 6 случаях, на наличие следов спермы – 12, на наличие следов крови – 6.

В большинстве случаев применение технико-криминалистических средств осуществлялось следователями военных следственных органов самостоятельно (от 80 до 95%).

Одним из важнейших результатом использования при раскрытии и расследовании преступлений технико-криминалистических средств является получение доказательств материального характера, позволяющих установить и изобличить лицо, его совершившее.

Следы рук человека традиционно занимают важное место в группе следов-отображений и используются в процессе доказывания.

Так, по уголовному делу в отношении Сенчукова С.П. и Русина В.А. (ВСУ СК России по ЮВО), обвиняемых в совершении преступления, предусмотренного п. «а» и «б» ч. 2 ст. 158 УК РФ, в качестве доказательств их виновности использовались обнаруженные и изъятые следователем на месте происшествия отпечатки пальцев указанных выше лиц [2].

Грамотная работа со следами пальцев рук, обнаруженных следователем на пакетах, служащих упаковкой для различных наркотических и психотропных веществ, позволили изобличить военнослужащего войсковой части 75943 старшего прапорщика Сатаева И.М. в совершении трех преступлений, предусмотренных п. «а» и «г» ч. 3 ст. 228^1 УК РФ (ВСУ СК России по ЮВО) [3].

По мере реализации приказа СК России от 27.12.2011 № 159 в военные следственные органы в ближайший период времени начнут поступать современные технико-криминалистические средства, многие из которых потребуют получения дополнительных навыков и специального обучения для их эффективного использования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Приказа Следственного комитета Российской Федерации от 27.12.2011 № 159 «О нормах обеспечения криминалистической и специальной техникой Следственного комитета Российской Федерации»

2. Уголовное дело №14/26/0027-19.

3. Уголовное дело №20/01/0156-20.

Сейтова А.К.
студент 2 курса образовательной программы «Право» Казахско-Русского международного университета (Республика Казахстан, г. Актобе)

Seytova A.K.,
2nd year student of the educational program «Law» of the Kazakh-Russian International University (Republic of Kazakhstan, Aktobe)

ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРОФИЛАКТИКИ ПОДРОСТКОВОЙ ПРЕСТУПНОСТИ

WAYS TO IMPROVE THE EFFECTIVENESS OF PREVENTION OF JUVENILE DELINQUENCY

Аннотация: В научной статье рассмотрены основные причины и условия, способствующие совершению уголовных правонарушений несовершеннолетними, а также некоторые аспекты особенностей профилактики правонарушений в подростковой среде. Особое внимание уделяется вопросам выработки эффективного комплекса мероприятий, способных оказать положительное влияние на состояние подростковой преступности, а также устранению предпосылок к совершению уголовных правонарушений несовершеннолетними.

Abstract: The scientific article discusses the main reasons and conditions conducive to the commission of criminal offenses by minors, as well as some aspects of the peculiarities of the prevention of offenses in adolescents. Special attention is paid to the development of an effective set of measures that can have a positive impact on the state of juvenile delinquency, as well as the elimination of prerequisites for the commission of criminal offenses by minors.

Ключевые слова: подростковая преступность, профилактика, полиция, нулевая терпимость, несовершеннолетний.

Key words:juvenile delinquency, prevention, police, zero tolerance, minor.

С 1 октября 2020 года на базе Казахско-Русского Международного университета проводится научно-исследовательская работа по теме «Пути повышения эффективности профилактики подростковой преступности в деятельности ювенальной полиции и школьных психологов». В рамках научного проекта, наравне с выявлением причин и условий преступности несовершеннолетних и молодежи, студенты образовательных программ «Право» и «Психология» разрабатывают пути решения существующих проблемных вопросов в сфере профилактики подростковой преступности в деятельности как подразделений местной полицейской службы, так и службы школьных психологов.

В ходе проектной работы мы пришли к выводу, что из причин и предпосылок подростковой преступности, среди множества различных факторов необходимо особо выделить случаи насилия в семье; асоциальное поведение братьев, сестер, родителей; морально-психологический климат в семье, в организациях образования; всевозможные конфликты, возникающие в процессе учебы; влияние окружения, в т. ч. и виртуального в сети Интернет и социальных сетях. Кроме того, следует отметить и имеющуюся тенденцию популяризации насилия, жестокости и «криминальной романтики» в средствах массовой информации, кино, «бульварной» литературе, в социальных сетях.

Проведенный анализ публикаций в средствах массовой информации о резонансных преступлениях, совершенных несовершеннолетними вызвал большую тревогу, указав на то, что современная подростковая преступность приобретает массовость и становится некой нормой поведения в среде несовершеннолетних. Преступления, совершаемые учащимися школ и колледжей, становятся все более жестокими и циничными. Последние несколько лет

казахстанские средства массовой информации ежемесячно публикуют материалы о криминальных происшествиях, главными отрицательными героями которых являются подростки в возрасте 14-17 лет. Ежемесячно по республике регистрируются факты применения несовершеннолетними оружия, в т. ч. и огнестрельного.

Так, в ноябре 2014 года в поселке Жибек жолы Сарыагашского района ЮКО конфликт между школьниками закончился перестрелкой, где один десятиклассник застрелил другого из обреза охотничьего ружья. В феврале 2015 года в одной из школ Актау конфликт учеников завершился перестрелкой. В апреле 2015 года перестрелка между учащимися случилась в городе Алматы. В сентябре 2015 года в больницу города Арыси в тяжелом состоянии с огнестрельными ранениями доставлено трое подростков 16-17 лет, участников групповой драки. В январе 2019 года в Шалкарском районе Актюбинской области между школьниками произошла потасовка, в результате которой один из подростков получил ножевое ранение. В феврале 2019 года в одной из школ города Каркаралы Карагандинской области, на перемене девятиклассник нанес ножевое ранение своему сверстнику. В сентябре 2019 года в городе Шымкенте патрульными нарядами пресечена массовая драка, в ходе которой телесные повреждения получил 16-летний подросток. У задержанных изъяты нож, обрез охотничьего ружья и травматический пистолет. В сентябре 2019 года в городе Алматы в результате конфликта, возникшего между представителями двух групп, 15-летний подросток нанес ножевое ранение гр. С., 1995 года рождения, который спустя несколько часов скончался. В ноябре 2019 года в городе Актобе в драке между подростками был убит 15-летний парень, еще двое получили ножевые ранения. В ноябре 2019 года в городе Кандыагаш Актюбинской области два ученика 10 класса выясняли отношения на ножах, причинив ножевые ранения. В ноябре 2019 года в городе Павлодар школьный конфликт перерос в драку, где один подросток получил ножевое ранение. В декабре 2019 года в поселке Жетысай Туркестанской области между учащимися десятого класса двух различных школ произошел конфликт, в ходе которого один из школьников ударил ножом в голову своего оппонента-ровесника. Колотая проникающая рана составила порядка 7 сантиметров в область головы. В январе 2020 года в городе Шалкаре Актюбинской области старшеклассники одной из школ учинили массовую драку, в ходе которой один несовершеннолетний получил ножевое ранение. В январе 2020 года в городе Арысе на одной из улиц между подростками произошла ссора, которая переросла в потасовку. В результате один из них нанес пять проникающих ножевых ранений своему сверстнику. В январе 2020 года в городе Нур-Султан между двумя одноклассниками одной из столичных школ произошла драка, в ходе которой один из подростков достал складной нож и нанес ранение однокласснику, а также по неосторожности порезал себе руку. В феврале 2020 года в городе Актобе за общежитием АРГУ имени К. Жубанова произошла драка между студентами. В результате ножевое ранение получил 19-летний студент вуза, который был госпитализирован в больницу. 01 июня 2020 года в г. Шымкенте скончался 17-летний подросток, впавший в кому после массовой драки, имевшей место 23 мая 2020 года. [1, с. 19].

Наибольшую тревогу и озабоченность вызывает и увеличение регистрации фактов совершения относительно нового вида массовых убийств – «schoolshooting», что в переводе с английского буквально означает стрельбу в школах. Так, 11 мая 2021 года в столице Республики Татарстан Российской Федерации девятнадцатилетний юноша, вооруженный гладкоствольным ружьем Hatsan Escort PS, ворвался в казанскую гимназию № 175 и совершил массовое убийство учащихся и сотрудников гимназии, где погибли 9 человек и 32 – пострадали. В ходе расследования стало известно, что подозреваемый Г. весной 2021 года прошел шестичасовые курсы по безопасному обращению с оружием, имея требуемые медицинские справки, а также билет охотника, без труда смог приобрести полуавтоматическое гладкоствольное ружье Hatsan Escort PS и патроны к нему, впоследствии ставшем орудием преступления[2].17 октября 2018 года в Керченском политехническом колледже произошло аналогичное массовое убийство учащихся и сотрудников колледжа, где в результате взрыва и стрельбы погиб 21 человек и 67 –

пострадало. Подозреваемый восемнадцатилетний студент колледжа Р. погиб на месте преступления, покончив с жизнью самоубийством. В ходе расследования стало известно, что подозреваемый Р. 13 октября 2018 года законно приобрел помповое ружье Hatsan Escort и 150 патронов с картечью, предварительно получив необходимое разрешение [3].

Изучение в ходе проектной работы судебно-следственной практики показало, что многие преступления совершаются несовершеннолетними с целью самоутверждения и демонстрации значимости в своем окружении. Кроме того, в последнее время через телевидение, Интернет и социальные сети активно идет популяризация идей криминального мира, а также пропаганда жестокости и насилия. Полагаем, что именно в этих условиях особую роль в профилактике подростковой преступности должна играть политика нулевой терпимости к правонарушениям.

Анализируя возможные предпосылки перечисленных трагических событий, нами было высказано предположение о том, что причины кроятся не только в психологических особенностях подростков, а в большей части, в пассивном отношении и отсутствии реакции общества на такое социальное явление, как проявление негативных форм девиантного поведения несовершеннолетних. В этой связи большинство насильственных преступлений можно было предотвратить, если бы общество отреагировало на развитие подростковых конфликтов элементарным своевременным сообщением в правоохранительные органы о намечающихся драках, «разборках» и т. д.

Не следует сбрасывать со счетов и фактическое отсутствие либо неправильную организацию досуга несовершеннолетних. Ни для кого не секрет, что в большинстве своем, родители по причине своей загруженности зачастую не имеют физической возможности в полной мере контролировать своих детей. В свою очередь, работники организаций образования также не в состоянии обеспечить всесторонний контроль деятельности учащихся, тем более, вне учебного времени. В результате, подростки, наиболее подверженные влиянию асоциальной среды, проводят все свое свободное время в дворовых компаниях, бесцельно слоняются по улицам либо сидят в компьютерных клубах, постепенно приобщаясь к употреблению спиртных напитков, сигарет и наркотиков. Для них характерна беспричинная конфликтность, вспыльчивость и несдержанность в поступках.

В качестве еще одной острой проблемы профилактики подростковой преступности следует отметить и имеющуюся практику замалчивания администрацией организаций образования фактов агрессивного и прокриминального поведения несовершеннолетних. Можно предположить, что причина сокрытия подобных фактов кроется, как бы это банально не звучало, в погоне за рейтингами, нежелании нести ответственность и становиться центром негативного внимания. Соответственно, школьник, ощущая относительную безнаказанность, продолжает свою асоциальную деятельность, что в итоге приводит к совершению преступлений, в т. ч. насильственного характера. Хотя, если с подобными «трудными» подростками своевременно и качественно проводить воспитательную, психологическую и профилактическую работу, то многих преступлений можно было бы избежать.

Здесь хотелось бы особо выделить роль сотрудников ювенальной полиции и службы школьных психологов, которые в интересах всей системы профилактики правонарушений среди несовершеннолетних ни в коем случае не должны идти «на поводу» у администрации организаций образования и закрывать глаза на факты правонарушений, совершаемые учащимися. Наоборот, к воспитанию несовершеннолетних необходимо подходить совместными усилиями и комплексно, где целями такой работы должны стать поиск правильных подходов к каждому подростку индивидуально, в зависимости от конкретной ситуации, а также обучение родителей правильной методике воспитания своих детей.

Также считаем, что положительное влияние на снижение уровня подростковой преступности могут оказать следующие мероприятия:

Во-первых, в целях исключения фактов совершения правонарушений, совершаемых как подростками, так и в отношении последних, конечно же, необходимо полное оснащение объектов

организаций образования, прилегающей к ним территории и максимально приближенных путей подхода освещением и качественной системой видеонаблюдения, исключая наличие «слепых» зон. Подобное техническое оснащение безусловно окажет благоприятное действие на предупреждение, своевременное пресечение и раскрытие возможных преступлений. А также следует проработать вопросы усиления контрольно-пропускной системы организаций образования, с отказом от привычных всем вахтерш и привлечением (аутсорсинг) для данных целей сотрудников специализированных охранных служб.

Во-вторых, для направления подростков в «правильное русло» необходимо организовать качественный досуг несовершеннолетних, вывести на новый уровень патриотическое, нравственное и, в некотором роде, идеологическое воспитание молодежи. Для этого следует наладить деятельность и увеличить количество бесплатных дворовых клубов, специализированных спортивных и творческих школ, пришкольных спортивных секций и творческих кружков, бесплатных центров языковой подготовки, летних лагерей отдыха, в т. ч. спортивных и трудовых. Кроме того, есть смысл возродить детские и юношеские организации по подобию пионерии, комсомола, скаутских движений и т. п.

В-третьих, целесообразно уделять пристальное внимание к результатам реализации администрацией, кураторским звеном, службой школьных психологов, а также сотрудниками ювенальной полиции принципа «нулевой терпимости» к мелким правонарушениям в организациях образования и внешкольных учреждениях, что положительно скажется на профилактике буллинга, хулиганства и прочих противоправных проявлений.

Таким образом, перед государством и казахстанским обществом стоят важные и серьезные задачи по незамедлительному пересмотру существующей системы профилактики правонарушений среди несовершеннолетних. И в этой связи, органам государственной власти следует взять за правило требование Главы государства: «Недостаточно просто слышать и видеть проблемы граждан, главное – правильно и объективно реагировать на них» [4].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Галым Ф.Г. О некоторых проблемах профилактики преступности в подростковой среде. //Роль общественности и взаимодействие с правоохранительными органами в предупреждении и профилактике правонарушений (к 25-летию Конституции и Ассамблеи народа Казахстана). Материалы международной научно-практической конференции, 15 мая 2020 г. / Под ред. М.Ж. Кайбжанова. Актобе, 2020. С. 158.

2. Серков Д. Эксперты назвали казанского стрелка террористом-одиночкой. //РБК. URL: https://www.rbc.ru/society/11/05/2021/609a54249a794720634de06a (дата обращения 10 ноября 2021 года).

3. Жилин И. Керченский колумбайн? //Новая газета. URL: https://novayagazeta.ru/articles/2018/10/17/78234-kerchenskiy-kolumbayn (дата обращения 10 ноября 2021 года).

4. Послание Главы государства Касым-Жомарта Токаева народу Казахстана. 1 сентября 2020 г.Казахстан в новой реальности: время действий. URL: https://www.akorda.kz/ru/addresses/addresses_of_president/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-1-sentyabrya-2020-g (дата обращения 10 ноября 2021 года).