психологической сути само деяние по небрежности, в результате которой нарушаются правила предосторожности, является мотивированным, целенаправленным, волевым и сознательным, что, однако, не в полной мере согласуется с принципом субъективного вменения. Для сглаживания проблемы преступную небрежность следует понимать как психологическую характеристику личности вообще. Примечателен тот факт, что большинство преступлений в сфере техники безопасности чаще совершаются по небрежности. Виновное лицо обязано соблюдать определенные правила и за их нарушение подлежит уголовной ответственности. Однако обязанность в данном случае имеет потенциальный характер. У виновного в момент совершения деяния обычно отсутствует психическое отношение к нарушаемой им обязанности.

Двойственность правовой природы нормы за небрежность предопределяется, с одной стороны, невозможностью ее обоснования в контексте общефилософского понимания вины, а с другой – необходимостью ее существования, поддержания стабильности правовой охраны общественных отношений. С учетом инновационного пути развития современного общества рост преступлений, вызываемых нарушением различных правил безопасности, неизбежен.

В теории уголовного права также все чаще звучит предложение о необходимости учета в вине факта осознания противоправности совершенного преступления, и особенно это актуально для преступлений, совершаемых по неосторожности. В одних анализируемых ситуациях пренебрежительное отношение к правилам может не повлечь причинения уголовно наказуемого преступления, в других случаях, наоборот, гораздо меньшая неосмотрительность виновного лица может стать основанием для его привлечения к уголовной ответственности. Указанная точка зрения имеет право на существование, так как в сфере безопасности государства действует великое множество нормативных правовых актов, в том числе ведомственных. Требовать от конкретного должностного лица безусловного познания всех их на уровне презумпции – значит, допускать объективное вменение, запрещенное уголовным законом. Положения, содержащиеся в указанных законодательных актах, далеко не всегда формулируют очевидные правила безопасности, иногда возникают ситуации, когда для того, чтобы понять конкретное правило поведения, необходимо ознакомиться со всем нормативным актом подробно. В случае совершения преступлений вышеуказанной группы необходимо вести речь об ответственности, которая базируется не на субъективном, а на объективном вменении.

Таким образом, субъективные элементы вины в составах преступлений, связанных с нарушением специальных правил безопасности, достаточно сложны для уголовно-правового анализа, и от системных алгоритмов в правильной квалификации по фактам преступных деяний, главной характеристикой которой является установление по уголовному делу всех элементов состава преступного деяния, напрямую зависит реализация принципа вины, а современная правоприменительная практика должна применять необходимые правовые инструменты, которые учитывают базовые положения теории уголовного права.

*Рогачев Д.Е.*

Научно-исследовательский институт Университета прокуратуры Российской Федерации (г. Москва)

## Борьба с преступностью в сфере компьютерной информации в Российской Федерации

На сегодняшний день компьютерные технологии стали неотъемлемой частью нашей повседневной жизни. Современному обществу как никогда свойственны интенсивный темп научно-технического прогресса, бурное развитие компьютерной техники и средств телекоммуникаций. В соответствии со Стратегией развития информационного общества в Российской Федерации на 2017-2030 годы развитие информационных и коммуникационных технологий, формирование информационного про-

странства и соответствующей инфраструктуры являются приоритетными направлениями внутренней политики государства[1]. Вместе с тем технологический прогресс сопровождается появлением новых видов преступлений, а их способы и формы постоянно совершенствуются.

Согласно действующему российскому законодательству к преступлениям в сфере компьютерной информации относятся: неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ); нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования (ст. 274.2 УК РФ).

Указанные статьи входят в главу 28 УК РФ, в которой в соответствии с примечанием к ст. 272 УК РФ под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. При этом определения многих других используемых в статьях данной главы УК РФ понятий закреплены в иных федеральных законах, например от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и др.

В отечественной науке преступления в сфере компьютерной информации часто именуют понятиями «компьютерные преступления», «информационные преступления» (деяния, совершаемые в информационно-телекоммуникационной сфере), «киберпреступления» (т.е. совершаемые с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, против компьютерной системы или сети)[2].

В формах федерального статистического наблюдения информация о результатах борьбы с данным видом преступности отражается вместе с данными о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Несмотря на то, что в структуре указанных преступлений деяния главы 28 УК РФ занимают незначительное место (в 2018 г. – 1,4%, в 2019 г. – 1%, в 2020 г. – 0,9%, в 2021 г. – 1,3%, в 2022 г. – 1,8%), количество зарегистрированных преступлений в сфере компьютерной информации в последние годы возрастает. Так, в 2018 г. правоохранительными органами было выявлено 2500 преступлений, предусмотренных статьями главы 28 УК РФ, в 2019 г. – 2883 (+15,3%), в 2020 г. – 4498 (+56,0%), в 2021 г. – 6869 (+52,7%), в 2022 г. – 10027 (+46%).

Рост уровня преступности в сфере компьютерной информации обусловливается несколькими факторами. Во-первых, злоумышленники стараются действовать на опережение и находятся на несколько шагов впереди тех, кто им противодействует. Законодательство в этом вопросе не поспевает за новыми угрозами в сфере высоких технологий и схемами их применения. Во-вторых, это легкомысленное поведение граждан в сфере информационных технологий. Сюда можно отнести легкие защитные пароли, передачу личных данных третьим лицам, посещение сомнительных сайтов, отсутствие антивирусных программ. В-третьих, это глобализация и возможность совершать рассматриваемые преступления из любой точки мира.

Одной из важнейших причин развития преступности в сфере компьютерной информации можно назвать обострение меж-

[1] О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы : Указ Президента Российской Федерации от 09.05.2017 № 203 // СПС «КонсультантПлюс».

[2] См.: Попов А.Н. Преступления в сфере компьютерной информации : учебное пособие. СПб.: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. 68 с.

дународной обстановки. Стратегия национальной безопасности Российской Федерации[1] прямо указывает, что в настоящий момент увеличивается количество компьютерных атак на российские информационные ресурсы. Большая часть таких атак осуществляется с территорий иностранных государств. Инициативы Российской Федерации в области обеспечения международной информационной безопасности встречают противодействие со стороны иностранных государств, стремящихся доминировать в глобальном информационном пространстве.

По данным Совета Безопасности Российской Федерации, ситуация в сфере информационной безопасности в течение 2022 г. характеризовалась существенным возрастанием масштаба и интенсивности деструктивного информационно-технического воздействия на информационную инфраструктуру Российской Федерации, осуществляемого специальными службами иностранных государств и международными преступными сообществами[2]. По итогам года количество выявленных случаев неправомерного доступа к компьютерной информации (ст. 272 УК РФ) возросло с 6392 до 9308, или на 45,6%, а количество случаев неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК РФ) в 3 раза превысило показатели предшествующего года (519 в 2022 г. против 159 в 2021 г.).

Так, по данным Лаборатории Касперского, в третьем квартале 2022 г., как и ранее, большинство управляющих ботнетами серверов находились в США (43,1%), Германии (10,2%), Нидерландах (9,3%)[3]. По словам IT-специалистов, представителей компаний, специализирующихся на информационной безопасности, в 2022 г. многократно возросло не только число подобных атак, но и их мощность, интенсивность. Так, по некоторым сведениям, число DDoS-атак на российские компании в первом полугодии 2022 г. выросло в 15 раз по сравнению с тем же периодом 2021 г., в том числе на государственный сектор – в 17 раз. При этом увеличилась длительность атак: если в конце 2021 г. атаки длились в среднем три часа, то в начале 2022 г. – семь часов, а некоторые атаки длятся неделями. По мнению экспертов, рост количества DDoS-атак связан прежде всего с нестабильной политической ситуацией в России и во всем мире и, как следствие, активизацией «хактивистов», целью которых является нанесение вреда экономике и социальной сфере России[4].

Следует отметить, что в ходе надзорной деятельности прокурорами в течение 2022 г. выявлялись нарушения требований законов в сфере информационной безопасности, представляющие собой серьезный криминогенный фактор. Так, в ряде регионов к работе со средствами криптографической защиты информации допускались должностные лица, не прошедшие соответствующее обучение, использовалось несертифицированное программное обеспечение, государственные информационные системы эксплуатировались без надлежащего оформления прав на них, установлены случаи несвоевременного обновления антивирусных баз, неисполнения планов мероприятий по защите информации и реагированию на компьютерные инциденты[5].

В связи с обострением угроз в информационной сфере в 2022 г. были приняты организационные меры, направленные на усиление борьбы с преступлениями в сфере компьютерной информации: в структуре центрального аппарата МВД России обра-

[1] О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 02.07.2021 № 400 // СПС «КонсультантПлюс».

[2] Состоялось заседание Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности // Совет Безопасности Российской Федерации : сайт. URL: http://www.scrf.gov.ru/news/allnews/3410/ (дата обращения: 20.01.2023).

[3] См.: Отчет «DDoS-атаки в третьем квартале 2022 г.» // Лаборатория Касперского. URL: https://securelist.ru/ddos-report-q3-2022/106012/ (дата обращения: 15.02.2023).

[4] Число DDoS-атак на российские компании в I полугодии 2022 года выросло в 15 раз // ТАСС. URL: https://tass.ru/ekonomika/15211801 (дата обращения: 15.02.2023).

[5] Генпрокуратурой России проанализирована практика надзора в сфере противодействия компьютерным атакам на информационные ресурсы Российской Федерации // Генеральная Прокуратура Российской Федерации : сайт. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=84090509 (дата обращения: 15.02.2023).

зовано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий[1], на которое возложено осуществление предупреждения, выявления, пресечения и раскрытия преступлений и иных правонарушений в сфере IT-технологий, а также координация этой деятельности в системе МВД России, аналогичные структуры появятся и в территориальных органах[2]. Кроме того, в целях повышения скорости межведомственного взаимодействия внесены изменения в законодательство, касающееся вопросов информационного обмена между Банком России и МВД России[3].

Развивалось и отечественное уголовное законодательство. Так, в 2022 г. глава 28 УК РФ была дополнена ст. 274[2] «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования»[4]. Такое решение принято на фоне ужесточения санкций против Российской Федерации и увеличения кибератак на государственные сайты.

Кроме того, в конце 2022 г. Верховным Судом Российской Федерации приняты меры, направленные на совершенствование правоприменительной практики борьбы с преступностью рассматриваемого вида. В связи с многочисленными вопросами, возникающими у судов, и в целях обеспечения единообразного применения ими законодательства об уголовной ответственности за преступления в сфере компьютерной информации, предусмотренные ст. 272, 273, 274 и 274[1] УК РФ, а также за иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет, Пленум Верховного Суда Российской Федерации дал судам соответствующие разъяснения[5].

Таким образом, борьба с преступлениями в сфере компьютерной информации является одной из наиболее актуальных проблем не только в России, но и во всем мире. Многие сферы общественных отношений перешли в интернет-пространство и нуждаются в надежной защите от преступных посягательств. Специфика рассматриваемых преступлений обусловлена использованием при их совершении различных новейших технологических достижений, необходимостью обладания определенным уровнем специальных познаний, а также наличием специального инструментария, что с учетом высокой латентности подобных общественно опасных деяний затрудняет их выявление и фиксацию, а также их пресечение и предупреждение. В связи с этим особое значение имеет создание соответствующих механизмов нормативно-правового, информационного, организационного, методологического обеспечения этого вида деятельности.

[1] Указ Президента Российской Федерации от 30.09.2022 № 688 «О внесении изменений в некоторые акты Президента Российской Федерации» // СПС «КонсультантПлюс».

[2] Выступление Министра внутренних дел Российской Федерации генерала полиции Российской Федерации В.А. Колокольцева на заседании Государственной Думы Федерального Собрания Российской Федерации в рамках «правительственного часа» // Официальный сайт МВД России. URL: https://мвд.рф/document/33200763 (дата обращения: 17.02.2023).

[3] О внесении изменений в статью 26 Федерального закона «О банках и банковской деятельности» и статью 27 Федерального закона «О национальной платежной системе» : Федеральный закон от 20.10.2022 № 408-ФЗ.

[4] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 14.07.2022 № 260-ФЗ.

[5] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37.