Научная статья
УДК 343.3/.7

КВАЛИФИКАЦИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ БАЗ ДАННЫХ СОТРУДНИКАМИ ПРАВООХРАНИТЕЛЬНЫХ И СУДЕБНЫХ ОРГАНОВ

Марина Александровна Ефремова[1], Рамис Салихутдинович Бурганов[2],
[1, 2] Казанский филиал Российского государственного
университета правосудия им. В.М. Лебедева, Казань, Россия
[1] crimlaw16@gmail.com, [2] burganov.ramis@mail.ru

Аннотация

Введение: современная преступность претерпевает существенные качественные изменения. В последние годы наблюдается стремительный рост числа преступлений, связанных с использованием информационно-телекоммуникационных технологий. Подобного рода технологии используются и при совершении должностных преступлений, однако сегодня все еще не разработаны единые подходы к их квалификации. В статье рассматриваются особенности квалификации преступлений, совершаемых сотрудниками правоохранительных и судебных органов с использованием специальных баз данных.

Материалы и методы: основу исследования составили диалектический метод познания, формально-юридический метод, а также методы анализа, синтеза, индукции и дедукции. Объектом исследования выступили уголовно-правовые взгляды ученых и практиков относительно квалификации преступлений в сфере компьютерной информации и должностных преступлений. Предмет исследования составили нормы российского уголовного законодательства, устанавливающие ответственность за неправомерный доступ к компьютерной информации и должностные преступления, судебная практика их применения.

Результаты исследования: делается вывод об особенностях квалификации деяний по статье 272 УК РФ и статьям главы 30 УК РФ и возможности квалификации деяний по совокупности преступлений; обозначается несколько сформировавшихся подходов, сложившихся в современной правоприменительной практике.

Обсуждение и заключение: авторами подчеркивается сформировавшаяся потребность в выработке единого подхода к квалификации деяний, совершаемых сотрудниками правоохранительных и судебных органов с использованием баз данных, и предлагаются направления его реализации.

Ключевые слова: должностные преступления; компьютерная информация; базы данных; квалификация преступлений; неправомерный доступ к информации

Для цитирования: Ефремова М.А., Бурганов Р.С. Квалификация преступлений, связанных с использованием баз данных сотрудниками правоохранительных и судебных органов // Вестник Казанского юридического института МВД России. 2025. Т. 16. № 3 (61). С. 97 – 105.

Scientific article
UDC 343.3/.7

QUALIFICATION OF CRIMES RELATED TO THE USE OF DATABASES BY LAW ENFORCEMENT AND JUDICIAL OFFICERS

Marina Aleksandrovna Efremova[1], Ramis Salikhutdinovich Burganov[2],
[1, 2] Kazan Branch of the Russian State University
of Justice named after V.M. Lebedev, Kazan, Russia,
[1] crimlaw16@gmail.com, [2] burganov.ramis@mail.ru

Abstract

Introduction: Modern crime is undergoing significant qualitative changes. In recent years, there has been a rapid increase in the number of crimes related to the use of information and telecommunication technologies. Similar technologies are also used in the commission of official crimes, but today unified approaches to their qualification have not yet been developed. One of the aspects of this problem is the qualification of crimes committed by law enforcement and judicial officials using special databases.

Materials and Methods: the research based on the dialectical method of cognition, the formal legal method, as well as methods of analysis, synthesis, induction and deduction. The object of the research is the criminal law views of scientists and practitioners regarding the qualification of crimes in the field of computer information and official offenses. The subject of the study is the norms of Russian criminal legislation that establish liability for unlawful access to computer information and official offenses, as well as judicial practice of their application.

Results: a conclusion is drawn about the peculiarities of the qualification of acts under Article 272 of the Criminal Code and articles of Chapter 30 of the Criminal Code and the possibility of qualifying acts according to the totality of crimes, and several established approaches that have developed in modern law enforcement practice.

Discussion and Conclusions: The authors emphasize the emerging need to develop a unified approach to the qualification of acts committed by law enforcement and judicial officials using databases and suggest directions for its implementation.

Key words: official crimes; computer information; databases; qualification of crimes; unauthorized access to information

For citation: Efremova M.A., Burganov R.S. Qualification of Crimes Related to the Use of Databases by Law Enforcement and Judicial Officers. Bulletin of the Kazan Law Institute of MIA of Russia. 2025;16(3):97-105. (In Russ.).

Введение

В настоящее время мы можем наблюдать качественное изменение преступности. В последние несколько лет происходил стремительный рост преступлений, связанных с использованием информационно-телекоммуникационных технологий. При этом в некоторые годы рост доли таких преступлений составлял более 20%. Подобного рода преступления совершаются и сотрудниками правоохранительных и судебных органов. Однако до сих пор не выработаны общие подходы к квалификации преступлений в сфере компьютерной информации и должностных преступлений.

Одним из аспектов рассматриваемой проблемы является квалификация преступлений, совершаемых с использованием баз данных сотрудниками правоохранительных и судебных органов. Количество таких преступлений достаточно велико, что обусловливается наличием различных баз данных, а также постепенным переходом на электронное делопроизводство.

П. 16 постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «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»[1] содержит прямое указание на необходимость квалификации подобного рода деяний по совокупности со ст. 272 УК РФ. Однако проанализированные нами судебные акты не свидетельствуют об однозначности в этом вопросе.

[1] Бюллетень Верховного Суда Российской Федерации. 2023. № 3. СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

Другим аспектом рассматриваемой проблемы является квалификация доступа к компьютерной информации как неправомерного. Дело в том, что сотрудники правоохранительных и судебных органов пользуются базами данных для исполнения своих должностных обязанностей, то есть правомерно. Возникает закономерный вопрос о допустимости квалификации, например, незаконной модификации ими данных в базе по ст. 272 УК РФ, и если да, то не будет ли это двойной ответственностью за одно и то же преступление?

Сказанное выше обусловливает потребность в анализе квалификации деяний, связанных с преступным использованием сотрудниками правоохранительных и судебных органов баз данных, и выработке единого подхода к их квалификации.

Обзор литературы

Проблемам квалификации деяний, предусмотренных ст. 272 УК РФ, в том числе квалификации по совокупности с другими составами, посвящен ряд интересных исследований. Вопросы квалификации деяний, связанных с неправомерным доступом к компьютерной информации, рассматривались в трудах Е.А. Русскевича [1-4], в том числе в его докторской диссертации [5], В.Н. Винокурова и Е.А. Федоровой [6-7], К.Н. Евдокимова [8], И.О. Ткачева [9]. Вместе с тем вопросы квалификации деяний с использованием компьютерной техники и баз данных нельзя признать полностью решенными.

Исследование базируется на материалах судебной статистики Судебного департамента при Верховном Суде Российской Федерации, судебной практики по конкретным делам районных судов, судов субъектов Российской Федерации и кассационных судов общей юрисдикции, Верховного Суда Российской Федерации.

Материалы и методы

Методологической основой явилось комплексное применение философских, общенаучных и частнонаучных методов познания. Ключевыми инструментами анализа выступили методы анализа и синтеза, индукции и дедукции, формально-логический и структурно-функциональный подходы. Обоснованный выбор методологической базы позволил осуществить углубленное изучение вопросов, составляющих предмет исследования, и представить аргументированные авторские выводы и предложения. В качестве эмпирической базы исследования были использованы нормы уголовного и иных отраслей права, материалы судебно-следственной практики, а также фундаментальные и прикладные работы отечественных ученых, посвященные проблемам уголовной ответственности должностные преступления и преступления в сфере компьютерной информации.

Результаты исследования

По данным МВД России, 40% зарегистрированных в 2024 году преступлений были совершены с использованием информационно-телекоммуникационных технологий. Таких деяний зарегистрировано на 13,1% больше, чем в 2023 году. При этом количество зарегистрированных в Российской Федерации преступлений уменьшилось на 1,8%[1].

С другой стороны, доля сотрудников правоохранительных и судебных органов среди лиц, совершивших преступления в сфере компьютерной информации, в последнее время достаточно высока. Приведем статистические данные за 2024 год по ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». В соответствии с данными Судебного департамента при Верховном Суде Российской Федерации[2] в 2024 году всего осуждено 512 845 лиц, из них осуждено 2 308 лиц по категориям «Адвокаты, нотариусы, аудиторы», «Судьи, работника суда», «Прокуроры, следователи», «Иные сотрудники правоохранительных органов, в том числе органов прокуратуры» (далее по тексту – «Осужденные сотрудники правоохранительных и судебных органов»). То есть доля данных четырех категорий составляет 0,45% от общего числа осужденных. При этом осуждено по всем частям ст. 272 УК РФ всего 267 лиц, из них по перечисленным выше четырем категориям – 13 лиц. Таким образом, доля сотрудников правоохранительных и судебных органов среди осужденных по ст. 272 УК РФ составляет 4,86%. Это более, чем в 10 раз больше, чем среди общего числа осужденных.

Другой способ подсчета также свидетельствует о значительной доле осужденных по ст. 272 УК РФ сотрудников правоохранительных и судебных органов. Так, осужденные по ст. 272 УК РФ (267 лиц) составляют 0,052% от общего числа осужденных (512 845 лица). Доля осужденных по ст. 272 УК РФ сотрудников правоохранительных и судебных органов (13 лиц) составляет 0,56% от общего числа осужденных сотрудников правоохранительных и судебных органов (2308 лиц), то есть более чем в 10 раз. Можно сказать, что сотрудников правоохранительных и судебных органов в 10 раз чаще осуждают по ст. 272 УК РФ,

[1] Состояние преступности // Официальный сайт МВД России. URL: мвд.рф/reports/1/ (дата обращения: 26.02.2025).

[2] Судебный департамент при Верховном Суде Российской Федерации. URL: https://cdep.ru/index.php?id=79&item=8946 (дата обращения: 10.05.2025).

чем иных граждан. Вместе с тем необходимо отметить, что в 2021 и 2022 годах осужденных по ст. 272 УК РФ сотрудников правоохранительных органов было лишь по 1 лицу. В 2023 году их стало уже 10. Изменение ли это позиции правоприменителя, качественное изменение преступности и тренд, либо скачок в рамках дисперсии показателей – покажет время.

Кроме того, изучение статистики осужденных по различным частям ст. 272 УК РФ дает основание утверждать, что по части 3 данной статьи осуждено подавляющее большинство. В 2024 году по части 1 статьи 272 УК РФ осуждено 18 лиц, по части 2 – 47 лиц, по части 3 – 200 лиц (74,9%), по части 4 – 2 лица. Мы не можем внутри статистики по части 3 статьи 272 УК РФ разделить деяния, совершенные группой лиц по предварительному сговору или организованной группой, от совершенных лицом с использованием своего служебного положения. Но, например, по тем же данным среди всех 380 лиц, осуждённых по главе 28 УК РФ в 2024 году, 81 совершил преступления в группе. Методом исключения следует предположить, что доля осужденных, совершивших преступление с использованием своего служебного положения, составляет не менее половины.

Следует объяснить это тем, что все большее число государственных органов осуществляют делопроизводство и документооборот с помощью различных государственных автоматизированных систем, информационно-управляющих систем, программных продуктов, программных изделий, программных комплексов, баз данных и др. В данных программах сотрудники правоохранительных и судебных органов осуществляют весь цикл своей работы: вносят данные, получают справочную и статистическую информацию, готовят бланки документов и готовые документы, используют их для принятия разнообразных административных и управленческих решений.

Базы данных, системы управления базами данных, программные изделия, программные продукты в правоохранительных и судебных органах обладают рядом особенностей, которые отличают их от иных программных продуктов и предопределяют специфику работы с ними.

К названным особенностям можно отнести следующие:

- различные уровни доступа. Большинство баз данных доступны только сотрудникам этого правоохранительного или судебного органа. Вместе с тем зачастую существует контур для общего доступа и для служебного пользования, но он содержит более узкий объем информации;

- полномочиями на внесение данных в базу, получение информации из неё обладают, как правило, не все сотрудники. Возможно определение ролей пользователей, имеющих разный круг полномочий;

- у сотрудников, имеющих полномочия, есть учетные данные для доступа (логин, пароль), которые позволяют им войти в систему, а впоследствии установить, кто и когда внёс или получил какие-либо сведения;

- базы данных, как правило, содержат сведения, относящиеся к персональным данным, а для указанных работников – составляющих служебную тайну;

- внесение данных в базу может повлечь возникновение, изменение, прекращение прав и обязанностей лиц, информация о которых вносится.

Данные особенности предопределяют способ совершения преступлений, последствия совершаемых преступлений, особенности субъективной стороны, информированности соучастников и т.п.

Одна из сложностей при квалификации преступлений, совершенных сотрудниками правоохранительных и судебных органов с помощью баз данных, обусловлена тем, что сотрудники имеют легальный доступ к указанным базам, вытыкающий из служебных полномочий перечисленных субъектов.

Е.А. Русскевич в связи с этим отмечает, что «даже действие в рамках служебных или профессиональных полномочий отнюдь не исключает возможности признания доступа к компьютерной информации неправомерным. Это объясняется тем, что право лица на доступ к информационной базе данных не носит общий характер, а возникает только в связи со строго определенными (нормативно регламентированными) основаниями» [3, с. 46].

Вопрос о квалификации таких деяний разрешается по-разному. В специальной литературе неоднократно обращалось внимание на отсутствие единообразия в судебной практике по уголовным делам о преступлениях, где компьютерная техника выступает средством совершения преступления. Позиции судебных органов по одним и тем же вопросам порой кардинально противоположны. В частности, довольно распространены случаи, когда сходные деяния квалифицируются по-разному: одни суды квалифицируют их только по ст. 272 УК РФ, другие же – по совокупности с соответствующей статьей Особенной части УК РФ[10]. И с тех пор ситуация мало поменялась.

В настоящее время сформировалось три подхода к квалификации деяний, связанных с

доступом (законным или незаконным) к базе данных сотрудниками правоохранительных и судебных органов, и последующими уничтожением, блокированием, модификацией или копированием.

Согласно первому подходу, деяние квалифицируется по ч. 3. ст. 272 УК РФ. Так, приговором Октябрьского районного суда города Иваново В. был осужден за то, что, являясь старшим инспектором ДПС ГИБДД УМВД России по Ивановской области, из базы данных ФИС ГИБДД-М на планшетном компьютере, находившемся при нем, получил сведения о карточке операций с водительским удостоверением (персональных данных), выданных на имя третьего лица. Эти данные В. скопировал путем фотографирования на свой мобильный телефон и, используя мессенджер, отправил скопированную информацию заинтересованному лицу[1].

В данном случае неправомерный доступ к компьютерной информации повлек ее копирование вопреки требованиям закона. Интересно, что здесь суд использует фразу «имея доступ», то есть доступ у сотрудника был.

По другому делу произошла модификация компьютерной информации. З., являясь секретарем судебного заседания отдела обеспечения судопроизводства по гражданским делам апелляционной инстанции Московского областного суда, совершил 8 преступлений, предусмотренных ч. 3 ст. 272 УК РФ, с использованием своего служебного положения.

В частности, З. через свою учетную запись в ГАС «Правосудие» внес неправомерные изменения в карточке гражданского дела апелляционной инстанции, изменив назначенного в автоматическом режиме судью по гражданскому делу на другого судью, для чего при регистрации поступивших гражданских дел в ГАС «Правосудие» создавал фиктивные карточки дел. После этого зарегистрированные фиктивные дела совместно с другими делами распределялись помощником председателя Московского областного суда в «Модуле распределения дел» ГАС «Правосудие», которая была не осведомлена о преступных намерениях З. После этого З. осуществил неправомерную замену содержимого карточек дел, тем самым совершив неправомерный доступ к охраняемой законом компьютерной информации, неправомерно модифицировав сведения в ГАС «Правосудие» Московского областного суда, вследствие чего данные об указанном гражданском деле были внесены в ранее созданную фиктивную карточку дела[2].

Е.А. Русскевич, рассматривая возможность квалификации только по ч. 3 ст. 272 УК РФ, приводит следующий пример мотивации из судебной практики: «Суд, применив ч. 3 ст. 272 УК РФ, обоснованно указал, что наличие у виновного официального доступа к служебной базе данных само по себе не исключает возможности его осуждения по ст. 272 УК РФ, поскольку им совершены незаконные действия, связанные с неправомерным доступом к компьютерной информации, имевшие целью сокрытие ранее совершенного должностного преступления, а также направленные на избежание лицом, совершившим административное правонарушение, исполнения назначенного судебным решением наказания». И далее приходит к следующему: «Учитывая, что ч. 3 ст. 272 УК РФ точнее выражает направленность деяния, а также более полно описывает его признаки, следует, пожалуй, поддержать последний подход. При этом, полагаем, в силу ч. 1 ст. 17 УК РФ подобного рода действия должностных лиц полностью охватываются ч. 3 ст. 272 УК РФ и дополнительной квалификации по ст. 285 УК РФ не требуют» [1, с. 90-91].

Второй подход сводится к квалификации только по соответствующей статье главы 30 УК РФ**.** Здесь суды квалифицируют деяние в зависимости от существа преступления, которое хочет совершить лицо, невзирая на то, что оно использует для этого базу данных и специфичный способ. Доступ к базе данных рассматривается как способ совершения преступления.

Например, приговором Солнцевского районного суда города Москвы, оставленным без изменения судами апелляционной и кассационной инстанций, П. был признан виновным по ч. 1 ст. 292[1], ч. 1 ст. 286 УК РФ. П., будучи начальником отдела по вопросам миграции Отдела МВД России по району Солнцево г. Москвы, внес сведения в специальную базу данных ППО «Территория», произвел печать паспорта на имя В., являющегося гражданином иностранного государства, собственноручно поставил свою подпись и печать, а затем произвел выдачу паспорта гражданина Российской Федерации на имя В. гражданину В., не приобретшему в установленном порядке гражданства Российской Федерации. Также в результате аналогичных действий он произвел выдачу паспорта гражданина Российской Федерации на

[1] Приговор Октябрьского районного суда города Иваново от 28.12.2024 по делу № 1-308/2024. СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

[2] Приговор Красногорского городского суда Московской области от 11.04.2024 по делу № 1-268/2024. СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

имя А.А.Б. гражданину А.Г., находящемуся в розыске за вымогательство.

Интересно и то, что П. в судебном разбирательстве показал, что «у него, как у руководителя, был доступ ко всем базам данных. Он под своим паролем ни разу не работал, пароль находился в сейфе у него в кабинете, но он им не пользовался». «Из показаний допрошенного в судебном заседании свидетеля Ш., старшего оперуполномоченного ОСБ УВД по ЗАО, следует, что в ходе сбора материала установили IP компьютеров, с которых вносились сведения в базу данных. Было установлено, что сведения внесены под логином другой сотрудницы отдела – Ф., но все данные в формах были ложные, в том числе номер паспорта. Все сведения вносились сразу, с разницей в несколько секунд, т.е. вносило одно лицо, материала проверки на это лицо не было»[1].

Анализ иных материалов судебной практики показал, что такая квалификация деяний достаточно распространена.

Третий подход предполагает квалификацию по совокупности ст. 272 УК РФ и соответствующей статьи главы 30 УК РФ. Данная позиция высказана Пленумом Верховного Суда Российской Федерации, который в п. 16 постановления от 15.12.2022 № 37 разъяснил, что «если действия, предусмотренные статьями 272 – 274.1 УК РФ, выступали способом совершения иных преступлений, они подлежат квалификации по совокупности с преступлениями, предусмотренными соответствующими статьями Уголовного кодекса Российской Федерации»[2].

Например, И., будучи заместителем начальника МО МВД России «Кулундинский», имея допуск к работе по использованию сведений банков данных Госавтоинспекции МВД России, за взятку собрал содержащуюся в них информацию о персональных данных не менее 88 неустановленного круга лиц, транспортных средствах, скопировал и передал ее другому лицу посредством приложения «Телеграм». Осужден по ч. 3 ст. 290 и ч. 3 ст. 272 УК РФ[3].

По другому делу Д. осуждён по ч. 3 ст. 272, ч. 1 ст. 286 УК РФ. Д., замещая должность государственного инспектора дорожного надзора отделения ГИБДД в базовом ресурсе «Адмпрактика» в подсистеме «Административные правонарушения» федеральной информационной системы ГИБДД-М внес в электронную карточку административного материала в отношении Н., зарегистрированному в указанной информационной системе за уникальным номером сведения о прерывании течения срока лишения специального права Н. При этом Д. был наделен полномочиями по доступу к единой системе информационно-аналитического обеспечения деятельности МВД России, а также к ряду подсистем федеральной информационной системы ГИБДД-М, однако не обладал полномочиями по доступу к подсистеме «Административные правонарушения» указанной выше информационной системы, а соответственно, не обладал полномочиями по внесению каких-либо сведений в указанную подсистему[4].

В данном случае вопрос о неправомерности очень спорный, поскольку у Д. была возможность вносить изменения, наниматель ему эту возможность не заблокировал.

Имеются примеры совокупности ст. 272 УК РФ и должностных преступлений (статей 290, 286 УК РФ). По одному из дел таким должностным преступлением было злоупотребление должностными полномочиями. Например, Б. осуждён по ч. 4 ст. 272, ч. 6 ст. 290, ч. 3 ст. 285 УК РФ за то, что являясь начальником информационного обеспечения Информационного центра УВД по СЗАО ГУ МВД России по г. Москве, в составе организованной группы систематически предоставлял информацию из информационно-поисковых сервисов МВД России за вознаграждение. При этом преступление выражалось только в указанном и дополнительных эпизодов, преступлений ему не вменялось[5].

Оценивая такую квалификацию по совокупности, необходимо отметить, что ряд доводов в пользу такого варианта квалификации высказывает К.Н. Евдокимов, который пишет, что «неправомерный доступ к компьютерной информации достаточно редко встречается как самостоятельное

[1] Приговор Солнцевского районного суда города Москвы от 29.08.2023 по делу № 1-238/2023. СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

[2] 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 // Бюллетень Верховного Суда Российской Федерации. 2023. № 3.

[3] Приговор Бурлинского районного суда Алтайского края от 22.04.2024 по делу № 1-1/2024 (1-34/2023). СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

[4] Приговор Россошанского районного суда Воронежской области от 23.01.2023 по делу № 1-7/2023 (1-313/2022). СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

[5] Приговор Хорошевского районного суда № 1 – 348/23. URL: https://mos-gorsud.ru/rs/horoshevskij/cases/docs/content/bd375c10-0b5d-11ee-b0d0-997dd5e612d2 (дата обращения: 18.03.2025).

преступное, а чаще всего является способом для совершения других общественно опасных деяний и достижения иных преступных целей. Поэтому действия виновных следует квалифицировать по совокупности совершенных преступных деяний, где неправомерный доступ к компьютерной информации выступает только одним из преступлений» [8, с. 41].

Анализ приведенных выше подходов к квалификации свидетельствует о необходимости поиска разумного баланса между следующими доводами. С одной стороны, следует избегать возможности привлечения к уголовной ответственности дважды за одно преступление, а также привлечение к уголовной ответственности за способ совершения преступления в тех ситуациях, когда этот способ единственно возможный и без него совершить преступление невозможно.

С другой стороны, необходимо обеспечить неотвратимость наказания, привлечение к уголовной ответственности лиц, совершивших общественно опасные деяния, ни одно из них не должно остаться без заслуженного наказания. Кроме того, мы учитываем, что если способ совершения преступления влечет более строгую или равную ответственность с деянием, которое этим способом совершено, то он подлежит отдельной квалификации по совокупности с основным преступлением.

Обсуждение и заключение

Вышеизложенное позволяет сделать следующие выводы.

Во-первых, если доступ к компьютерной информации имел явно неправомерный характер (использование личных данных коллеги без его ведома, атака хакеров, подбор пароля, вход человеком, который таких полномочий не имеет и никогда не имел), то квалификация должна осуществляться по ст. 272 УК РФ. При этом неправомерность доступа должна быть мотивирована в приговоре. В исследованных нами приговорах мы такой мотивировки зачастую не видим.

Во-вторых, если доступ хотя и носил правомерный характер, а дальнейшие действия явились незаконными, то судебные органы рассматривают факт правомерного доступа с неправомерными целями (впоследствии реализованными в копировании, модификации и др.) как неправомерный. Хотя, как отмечалось выше, это происходит далеко не всегда. Нам представляется более обоснованным второй из выделенных нами подходов, то есть квалификация только по статье главы 30 УК РФ. Это объясняется тем, что совершение преступления с использованием базы данных является единственным возможным способом совершения преступления, антиобщественная направленность умысла лица не направлена на неправомерный доступ, а направлена на совершение должностного преступления (получение взятки, превышение должностных полномочий, служебный подлог и др.).

В-третьих, санкция ч. 3 ст. 272 УК РФ достаточно сурова (до 5 лет лишения свободы), а ч. 1 ст. 286 (до 4 лет лишения свободы), ч. 1 ст. 290 (до 3 лет лишения свободы) предполагают более мягкое наказание. Поэтому в настоящее время общие подходы к квалификации обязывают квалифицировать по совокупности статей главы 30 УК РФ и ч. 3 ст. 272 УК РФ как способ совершения преступления, более сурово наказуемый, чем само преступление.

Эти выводы касаются современного положения дел в законодательстве и судебной практике, которое, однако, на наш взгляд, должно быть изменено путем совершенствования законодательства и появлением новых разъяснений высших судебных органов.

СПИСОК ИСТОЧНИКОВ

1. Русскевич Е.А. О проблемах квалификации неправомерного доступа к компьютерной информации // Уголовное право. 2017. № 5. С. 85 – 91.

2. Русскевич Е.А. Неправомерный доступ к компьютерной информации: вопросы квалификации // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции. Москва, 2018. С. 630 – 633.

3. Русскевич Е.А. Неправомерный доступ к компьютерной информации: теория и судебная практика // Судья. 2018. № 10. С. 46 – 49.

4. Русскевич Е.А. О Постановлении Пленума Верховного Суда Российской Федерации по делам о преступлениях в сфере компьютерной информации и преступлениях, совершенных с использованием сети Интернет // Уголовное право: стратегия развития в 21 веке. 2023. № 3. С. 99 – 18.

5. Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации. Диссертация на соискание ученой степени доктора юридических наук. Москва. 2020.

6. Винокуров В.Н., Федорова Е.А. Пределы действия нормы, предусмотренной статьей 272 Уголовного кодекса РФ // Российский юридический журнал. 2021. № 4. С. 73 – 82.
7. Винокуров В.Н., Федорова Е.А. Предмет неправомерного доступа к компьютерной информации (ст. 272 УК) // Законность. 2021. № 5. С. 50 – 52.
8. Евдокимов К.Н. Некоторые особенности уголовно-правовой квалификации неправомерного доступа к компьютерной информации на стадии возбуждения уголовного дела // Российский следователь. 2017. № 4. С. 39 – 44.
9. Ткачев И.О. Использование информационно-телекоммуникационных сетей как квалифицирующий признак состава преступления // Уголовное право. 2024. № 10. С. 72-83.
10. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: монография. Москва: Юрлитинформ, 2018. 312 с.

REFERENCES

1. Russkevich E.A. O problemah kvalifikacii nepravomernogo dostupa k komp'yuternoj informacii // Ugolovnoe pravo. 2017. № 5. S. 85 – 91.
2. Russkevich E.A. Nepravomernyj dostup k komp'yuternoj informacii: voprosy kvalifikacii // Ugolovnoe pravo: strategiya razvitiya v XXI veke: materialy XV Mezhdunarodnoj nauchno-prakticheskoj konferencii. Moskva, 2018. S. 630 – 633.
3. Russkevich E.A. Nepravomernyj dostup k komp'yuternoj informacii: teoriya i sudebnaya praktika // Sud'ya. 2018. № 10. S. 46 – 49.
4. Russkevich E.A. O Postanovlenii Plenuma Verhovnogo Suda Rossijskoj Federacii po delam o prestupleniyah v sfere komp'yuternoj informacii i prestupleniyah, sovershennyh s ispol'zovaniem seti Internet // Ugolovnoe pravo: strategiya razvitiya v 21 veke. 2023. № 3. S. 99 – 18.
5. Russkevich E.A. Differenciaciya otvetstvennosti za prestupleniya, sovershaemye s ispol'zovaniem informacionno-kommunikacionnyh tekhnologij, i problemy ih kvalifikacii. Dissertaciya na soiskanie uchenoj stepeni doktora yuridicheskih nauk. Moskva. 2020.
6. Vinokurov V.N., Fedorova E.A. Predely dejstviya normy, predusmotrennoj stat'ej 272 Ugolovnogo kodeksa RF // Rossijskij yuridicheskij zhurnal. 2021. № 4. S. 73 – 82.
7. Vinokurov V.N., Fedorova E.A. Predmet nepravomernogo dostupa k komp'yuternoj informacii (st. 272 UK) // Zakonnost'. 2021. № 5. S. 50 – 52.
8. Evdokimov K.N. Nekotorye osobennosti ugolovno-pravovoj kvalifikacii nepravomernogo dostupa k komp'yuternoj informacii na stadii vozbuzhdeniya ugolovnogo dela // Rossijskij sledovatel'. 2017. № 4. S. 39 – 44.
9. Tkachev I.O. Ispol'zovanie informacionno-telekommunikacionnyh setej kak kvalificiruyushchij priznak sostava prestupleniya // Ugolovnoe pravo. 2024. № 10. C. 72-83.
10. Efremova M.A. Ugolovno-pravovaya ohrana informacionnoj bezopasnosti: monografiya. Moskva: Yurlitinform, 2018. 312 s.

Информация об авторах:
Ефремова Марина Александровна, доктор юридических наук, профессор, заведующий кафедрой уголовно-правовых дисциплин Казанского филиала Российского государственного университета правосудия им. В.М. Лебедева, e-mail: crimlaw16@gmail.com ORCID: 0000-0001-6037-6921
Бурганов Рамис Салихутдинович, кандидат юридических наук, доцент, доцент кафедры уголовно-правовых дисциплин Казанского филиала российского государственного университета правосудия им. В.М. Лебедева, e-mail: burganov.ramis@mail.ru ORCID: 0000-0003-0365-2146
Авторы прочитали и одобрили окончательный вариант рукописи.

Information about the authors:
Efremova Marina A., Doctor of Law (Doctor habilitatus), Professor, head of the Department of Criminal Law Disciplines Kazan Branch of the Russian State University of Justice named after V.M. Lebedev, e-mail: crimlaw16@gmail.com ORCID: 0000-0001-6037-6921
Burganov Ramis S., Candidate of Law (Research doctorate), Associate Professor, Associate Professor of the Department of Criminal Law Disciplines, Kazan Branch of the Russian State University of Justice named after V.M. Lebedev, e-mail: burganov.ramis@mail.ru ORCID: 0000-0003-0365-2146
The authors have read and approved the final version of the manuscript.

Заявленный вклад авторов:
Ефремова Марина Александровна – постановка проблемы, определение объекта и методов исследования, разработка обзора литературы, уточнение выводов и рекомендаций.
Бурганов Рамис Салихутдинович – анализ доктринально-прикладных данных, подготовка введения и результатов исследования, формирование заключения.

Статья получена: 10.05.2025.
Статья принята к публикации: 19.09.2025.
Статья опубликована онлайн: 19.09.2025.