Научная статья
УДК 343.4

КВАЛИФИЦИРУЮЩИЕ И ОСОБО КВАЛИФИЦИРУЮЩИЕ ПРИЗНАКИ СОСТАВА НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Георгий Фаризович Шипулин
Московский политехнический университет,
Москва, Россия, podumai_nad@mail.ru

Аннотация. В статье анализируется понимание квалифицирующих и особо квалифицирующих признаков неправомерного доступа к компьютерной информации (ч. ч. 2–4 ст. 272 Уголовного кодекса Российской Федерации (далее – УК РФ)) с учетом практики ее применения. Для исследования указанной тематики используются такие методы, как анализ, синтез, сравнение и аналогия. Указана актуальность исследуемой темы исследования, представлена обширная научная база данной тематики. В исследовании также используется актуальная нормативная база и статистические показатели. В статье раскрываются квалифицирующие и особо квалифицирующие признаки преступлений, предусмотренных ч.ч. 2–4 ст. 272 УК РФ. Данное исследование содержит актуальную судебную практику применения указанной нормы, проводится анализ судебных решений. В статье выявлены правовые пробелы в определении некоторых понятий, представлено предложение о решении данной проблемы. Рассмотрены отдельные особенности квалифицирующих признаков, на основе анализа указанных признаков сформулирован вывод о том, что большинство преступлений по статье 272 УК РФ осуществляется либо с корыстной заинтересованностью у преступника, либо с использованием должностного положения преступника и квалифицируется по ч.ч. 2 и 3 соответственно.

Ключевые слова: компьютерная информация, компьютерные сети, неправомерный доступ, квалифицирующие признаки, особо квалифицирующие признаки.

Для цитирования: Шипулин Г. Ф. Квалифицирующие и особо квалифицирующие признаки состава неправомерного доступа к компьютерной информации // Вестник Уфимского юридического института МВД России. 2023. № 3 (101). С. 126–130.

Original article

QUALIFYING AND ESPECIALLY QUALIFYING FEATURES OF THE COMPOSITION OF ILLEGAL ACCESS TO COMPUTER INFORMATION

Georgy F. Shipulin
Moscow Polytechnic University, Moscow, Russia, podumai_nad@mail.ru

Abstract. The article analyzes the understanding of qualifying and especially qualifying characteristics of illegal access to computer information (p. 2–4 art. 272 of the Criminal Code of the Russian Federation), taking into account the practice of its application. Analysis, synthesis, comparison and analogy were used to investigate the subject matter. The relevance of the investigated topic of research is indicated, an extensive scientific basis of the topic is presented. The up-to-date normative base and statistical indicators are also used in the research. The article reveals qualifying and especially qualifying features of the crimes stipulated by parts 2–4 of article 272 of the Criminal Code of the Russian Federation. The research contains the actual judicial practice of application of the mentioned norm; the analysis of the court decisions is carried out. The article reveals the legal gaps in the definition of certain concepts, presents a proposal for solving this problem. The separate features of qualifying signs are considered; on the basis of the analysis of the mentioned signs the conclusion

is formulated that the majority of crimes under the article 272 of the Criminal Code of the Russian Federation is committed either with selfish interest of a criminal, or with the use of official position of a criminal and is qualified under part 2 and 3 respectively.

Keywords: computer information, computer networks, illegal access, qualifying features, especially qualifying features.

For citation: Shipulin G. F. Qualifying and especially qualifying features of the composition of illegal access to computer information // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2023. No. 3 (101). P. 126–130. (In Russ.).

Сегодня одним из передовых направлений политики государства является внедрение инновационных технологий [1, с. 154; 2, с. 10; 3, с. 285; 4, с. 97; 5, с. 22], в результате чего количество преступлений, предусмотренных статьей 272 УК РФ, неуклонно растет, так как объем обрабатываемых данных увеличивается с каждым днем [6, с. 21]. При этом правоохранительные органы так и не создали оптимальных методов по раскрытию и пресечению данных видов преступлений.

Согласно данным статистической платформы «Достоевский», общее количество осужденных по статье 272 УК РФ за 2019–2021 годы составило 302 человека. По части 1 – 29 человек, по части 2 – 41, по части 3 – 225, по части 4 – всего двое осужденных.

Рассмотрим квалифицирующие признаки преступления, предусмотренного ст. 272 УК РФ. Преступление, совершенное по части 2 статьи 272 УК РФ, квалифицируется следующими признаками: нанесение материального ущерба на сумму свыше миллиона рублей, наличие стремления к получению материальной выгоды у лица, совершающего преступление. Как правило, ущерб пострадавшей стороны сопровождается сопутствующим ущербом для других лиц и квалифицируется уже по совокупности со статьей 159 УК РФ.

Так, например, гражданин Терентьев, имея корыстный умысел, с целью хищения чужих денежных средств с помощью информационно-коммуникационной сети Интернет посетил компьютерный салон, где арендовал персональный компьютер. Затем гражданин Терентьев купил идентификационные данные для входа в чужой аккаунт в социальной сети. Лицо, продавшее логин и пароль от чужого аккаунта, следствием не установлено. После этого гражданин Терентьев осуществил несанкционированный доступ к чужому аккаунту в социальной сети по ранее полученным идентификационным данным и совершил изменение компьютерной информации, находящейся в аккаунте социальной сети. Затем Терентьев, блокировав доступ к странице законного пользователя, с указанной электронной страницы осуществил отправку сообщений с просьбой одолжить денежные средства пользователям, находящихся в разделе «Друзья».

Получив указанное сообщение, введенный в заблуждение пользователь, предполагая, что сообщение ему отправлено его знакомым, по просьбе последнего перечислил со своей банковской карты на счет банковской карты, используемой Терентьевым, денежные средства. После получения денежных средств на счет указанной банковской карты Терентьев израсходовал их на личные нужды, причинив тем самым ущерб иным лицам.

Суд квалифицировал действия Терентьева по двум фактам по части 2 статьи 272 УК РФ как неправомерный доступ к охраняемой законом компьютерной информации, повлекший блокирование и модификацию компьютерной информации, совершенный из корыстной заинтересованности; и по двум фактам части 2 статьи 159 УК РФ как мошенничество, то есть хищение чужого имущества путем обмана и злоупотребления доверием, совершенное с причинением значительного ущерба гражданину[1].

[1] Обвинительный приговор Ленинского районного суда города Чебоксары от 22 сентября 2016 г. по уголовному делу № 1-346/2016 // Правосудие: государственная автоматизированная система. URL: https://bsr.sudrf.ru/bigs/portal.html (дата обращения: 06.11.2022).

Преступление, осуществляемое лицом по заказу другого лица, по наводке или распоряжению третьих лиц, может отражать корыстную заинтересованность правонарушителя.

Приведем еще один пример. Представители хакерской группировки Cobalt взломали рабочий компьютер сотрудника банка с помощью рассылки фейковых писем якобы от службы поддержки Microsoft. Закрепившись в сети, хакеры повысили свои привилегии до уровня администратора домена, подключились к банкоматам по RDP и с помощью вредоносного программного обеспечения отправляли команды на выдачу банкнот. Сбором денежных средств как раз и занимались представшие перед судом два брата. За работу они получили 10 % от похищенной суммы. В результате перед судом предстали низкоквалифицированные участники преступных групп. Настоящие организаторы оказались вне досягаемости правоохранителей[1].

В случае совершения преступления, предусмотренного статьей 272 УК РФ, группой лиц по предварительному сговору или преступным сообществом, или лицом с применением статуса служащего, оно квалифицируется по части 3 данной статьи. По общему правилу квалифицирующий признак совершения преступления группой лиц по предварительному сговору применяется при следующих условиях: в преступлении участвовало объединение из нескольких лиц, данное объединение лиц до осуществления преступления определило цели и задачи, каждый участник этой группы имеет статус соисполнителя. Если хотя бы один признак из вышеуказанных пунктов не отражен в правонарушении, тогда квалифицирующий признак совершения преступления группой лиц по предварительному сговору не применим.

Под преступным сообществом понимается организация преступной группы лиц с целью совершения тяжких преступлений. Стоит отметить, что с точки зрения уголовного права данный вид соучастия признается одним из опаснейших видов соучастия в преступлении. Организация преступного сообщества является отдельным видом преступной деятельности, за которую предусматривается уголовная ответственность согласно статье 210 УК РФ.

Применение статуса служащего предполагает возможность получения данных, которые могут относиться к разным категориям информации ограниченного доступа. В определении должностного лица можно опираться на трактовку понятия, изложенного в примечании 1 статьи 285 УК РФ [7, с. 36].

Например, гражданин Тихонов, осуществляя профессиональную деятельность системного администратора, поменял настройки служебного оборудования, а именно коммутатора. В результате этих изменений он получил возможность осуществлять доступ к коммуникатору со стороны внешнего контура с помощью информационно-коммуникационной сети «Интернет». Затем гражданин Тихонов, действуя с преступным умыслом, использовал известную ему уязвимость в служебном оборудовании, выполнил незаконный доступ к коммутатору и осуществил неправомерное изменение информации ограниченного доступа, поменяв содержимое загрузочного файла коммутатора. В результате указанных выше деяний гражданина Тихонова служебное оборудование отключилось, и информация ограниченного доступа, которая находилась на серверах, принадлежащих организации, уничтожилась. Сотрудники организации на определенный промежуток времени не смогли получать доступ к внутренним информационным системам организации. В результате несанкционированный доступ гражданина Тихонова к информации ограниченного доступа, повлекший удаление информации, привел к остановке рабочих процессов и причинил крупный ущерб организации[2].

---

[1] Евсиков В. Такие дела. Как и за что судили российских хакеров в 2019 году // Хакер. URL: https://xakep.ru/2020/06/23/criminal-cases-2019/ (дата обращения: 06.11.2022).

[2] Обвинительный приговор Ленинского районного суда города Чебоксары от 8 августа 2016 г. по уголовному делу № 1-356/2016 // Правосудие: государственная автоматизированная система. URL: https://bsr.sudrf.ru/bigs/portal.html (дата обращения: 06.11.2022).

Кроме того, стоит отметить, что нередки случаи, когда осуществление преступления по статье 272 УК РФ сопровождается совокупностью со статьей 273 УК РФ. Получение несанкционированного доступа к информации ограниченного доступа проводится посредством создания и использования вредоносных компьютерных программ. Например, совокупность статей 272 и 273 УК РФ имеет место в тех случаях, когда преступник осуществляет несанкционированный доступ с помощью вредоносного программного обеспечения, которое разработал самостоятельно или приобрел у иных лиц.

Например, граждане Баскаков и Гинда осуществляли деятельность по оказанию услуг неограниченному кругу лиц по организации доступа к спутниковому телевидению. Преступники проводили монтажные работы оборудования, с помощью которого осуществляется доступ к спутниковому телевидению. Заранее установив на данное оборудование вредоносный программный код, осуществляли незаконный доступ и копирование информации ограниченного доступа. Таким образом, в результате проведенного расследования суд признал вину Баскакова и Гинды по ч. 3 ст. 272 и ч.2 ст. 273 УК РФ[1].

В случае наступления тяжких последствий, к которым привел несанкционированный доступ к информации ограниченного доступа, данное деяние квалифицируется по части 4 статьи 272 УК РФ. Законодатель не дает определения термину «тяжкие последствия», поэтому определение тяжких последствий формируется судебной практикой и является оценочным [8, с. 16]. К ним могут относиться утрата трудоспособности, заболевание, инвалидность, вред здоровью, смерть человека, уничтожение или повреждение имущества.

Также квалифицироваться по части 4 статьи 272 УК РФ может ситуация, в которой тяжкие последствия имеют реальную угрозу наступления. Таким образом, установленные нарушения достаточно разнообразны по характеру [9, с. 252].

Подводя итог, отметим, что большинство преступлений по статье 272 УК РФ осуществляется либо с корыстной заинтересованностью у преступника, либо с использованием должностного положения преступника и квалифицируется по ч.ч. 2 и 3 соответственно. Преступления, осуществленные с использованием должностного положения, как правило, совершают лица, занимающие административные должности и обладающие специальными техническими знаниями. В основном все преступления квалифицируются исключительно по статье 272 УК РФ, однако имеют место случаи, когда действия преступников оцениваются по совокупности статей УК РФ. Превалирует совокупность преступлений по статьям 272 и 273 УК РФ.

Вид наказания за подобные преступления зависит от наличия квалификации преступления по иным статьям. В случае, если имеет место только статья 272 УК РФ, то чаще всего назначается штраф либо условное лишение свободы. Также следует отметить, что превалирующее количество дел сопровождается обстоятельствами, которые смягчают наказание.

СПИСОК ИСТОЧНИКОВ

1. Осокин Р. Б., Дикажев М. М. Электронный документооборот в правоохранительных органах: состояние и проблемы правовой регламентации // Юридические науки. 2020. № 6.

2. Трунцевский Ю. В., Ефремов А. А. Цифровая интеграция – путь в будущее // Международное публичное и частное право. 2018. № 1. С. 6–12.

[1] Обвинительный приговор Новоуренгойского городской суда Ямало-ненецкого автономного округа от 5 декабря 2016 г. по уголовному делу № 1-330/2016 // Правосудие: государственная автоматизированная система. URL: https://bsr.sudrf.ru/bigs/portal.html (дата обращения: 06.11.2022).

3. Влавацкая Е. А., Хохлова О. М. Проблемы квалификации неправомерного доступа к компьютерной информации // Молодой ученый. 2021. № 22 (364). С. 283–286.

4. Шаров А. В. К вопросу о классификации следов преступлений, совершенных с применением информационных технологий // Известия ТулГУ. Экономические и юридические науки. 2021. № 4.

5. Давыдов В. О., Тишутина И. В., Цифровые следы в расследовании дистанционного мошенничества // Известия ТулГУ. Экономические и юридические науки. 2020. № 3.

6. Трунцевский Ю. В. Цифровая (виртуальная) валюта и противодействие отмыванию денег: правовое регулирование // Банковское право. 2018. № 2. С. 18–28.

7. Бурмистрова А. А., Осокин Р. Б. Уголовно-правовая характеристика провокации взятки либо коммерческого подкупа // Юридические науки. 2021. № 1.

8. Расследование преступлений в сфере компьютерной информации, совершаемых против собственности: учебное пособие / А. В. Пузарин и др. М.: Московский университет МВД России имени В. Я. Кикотя, 2020. С. 14–18.

9. Осокин Р. Б. Деятельность прокуратуры Тамбовской области по надзору за соблюдением законодательства о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных муниципальных нужд // Юридические науки. 2017. № 2.

REFERENCES

1. Osokin R. B., Dikazhev M. M. Electronic document management in law enforcement agencies: state and problems of legal regulation // Legal Sciences. 2020. No. 6. (In Russ.)

2. Truntsevsky Yu. V., Efremov A. A. Digital integration – the way to the future // Public and private international law. 2018. No. 1. P. 6–12. (In Russ.)

3. Vlavatskaya E. A., Khokhlova O. M. Problems of qualification of illegal access to computer information // Young scientist. 2021. No. 22 (364). P. 283–286. (In Russ.)

4. Sharov A. V. On the classification of traces of crimes committed with the use of information technologies. Izvestiya TulGU. Economic and legal sciences. 2021. No. 4. (In Russ.)

5. Davydov V. O., Tishutina I. V., Digital traces in the investigation of remote fraud // Izvestiya TulGU. Economic and legal sciences. 2020. No. 3. (In Russ.)

6. Truntsevsky Yu. V. Digital (virtual) currency and counteraction to money laundering: legal regulation // Banking law. 2018. No. 2. P. 18–28. (In Russ.)

7. Burmistrova A. A., Osokin R. B. Criminal-legal characteristics of the provocation of a bribe or commercial bribery // Legal Sciences. 2021. No. 1. (In Russ.)

8. Investigation of crimes in the field of computer information committed against property: textbook / A. V. Puzarin et al. M.: Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot, 2020. P. 14–18. (In Russ.)

9. Osokin R. B. The activities of the prosecutor's office of Tambov region to supervise compliance with the legislation on the contract system in the field of procurement of goods, works, services to ensure state municipal needs // Legal Sciences. 2017. No. 2. (In Russ.)

Статья поступила в редакцию 16.05.2023; одобрена после рецензирования 18.05.2023; принята к публикации 15.09.2023.

The article was submitted 16.05.2023; approved after reviewing 18.05.2023; accepted for publication 15.09.2023.