УДК 343.34
Рубрика: Уголовное право и особенности квалификации преступлений

Совершенствование уголовно-правового противодействия неправомерному доступу к компьютерной информации

ВЕКЛЕНКО СЕРГЕЙ ВЛАДИМИРОВИЧ
доктор юридических наук, профессор, Заслуженный работник высшей школы Российской Федерации, профессор кафедры уголовного права Санкт-Петербургского университета МВД России, veklenkosv@mail.ru
ORCID ID: 0000-0002-8625-8656
Veklenko Sergey Vladimirovich, Doctor of Law, Professor, Honored Worker of the Higher School of the Russian Federation, Professorof the Department of Criminal Law of the Saint-Petersburg University of the MIA of Russia.
veklenkosv@mail.ru ORCID ID: 0000-0002-8625-8656

ЛОКНОВ АЛЕКСЕЙ ИГОРЕВИЧ,
кандидат технических наук, доцент, доцент кафедры информационной безопасности Санкт-Петербургского университета МВД России, info_for_aleksey@mail.ru
ORCID ID: 0000-0003-4425-1939
Loknov Aleksey Igorevich, Candidate of Technical Sciences, associate Professor, Associate Professor of the Department of Information Security of the Saint-Petersburg University of the MIA of Russia.
info_for_aleksey@mail.ru. ORCID ID: 0000-0003-4425-1939

Аннотация:

Введение. Актуальность исследования продиктована необходимостью анализа норм уголовного закона о преступлениях, связанных с неправомерным доступом к компьютерной информации, объективных и

субъективных признаков состава данного преступления, уголовной ответственности и необходимостью формулировки предложений по совершенствованию уголовно-правового противодействия такого вида деяниям. В статье анализируются особенности квалификации преступления, предусмотренного ст. 272 Уголовного кодекса Российской Федерации. Подчеркивается высокий уровень неопределённости трактовки понятий, связанных с неправомерным доступом к компьютерной информации, что вполне закономерно обуславливает отсутствие единообразной судебно-следственной практики применения данной статьи. Проведён анализ объективных и субъективных признаков этого преступления. Обосновываются предложения по внесению изменений в действующее законодательство.

Методы. Методологическую основу исследования составляют общие научные (анализ, синтез, индукция, дедукция, классификация, сопоставление, сравнение) и частные научные методы юридического исследования (историко-юридический, сравнительно-правовой, формально-логический, системный).

Результаты. Проведённое исследование показывает, что, несмотря на активную разработку вопросов практического применения положений ст. 272 Уголовного кодекса Российской Федерации в отечественной науке, следует констатировать, что многие аспекты квалификации данного посягательства на сегодняшний день носят спорный и нормативно неразрешённый характер. Авторами предложено дополнение, которое позволит правоприменителям более точно определять и квалифицировать преступления, связанные с незаконным доступом к компьютерной информации.

Ключевые слова: неправомерный доступ, компьютерные преступления, компьютерная информация.

Improvement of criminal law counteraction to illegal access to computer information

Abstract:

Introduction. The relevance of the study is dictated by the need to analyze the norms of the criminal law on crimes related to unlawful access to computer information, objective and subjective signs of the composition of this crime, criminal liability and the need to formulate proposals to improve criminal law counteraction to this type of acts. The article analyzes the specifics of the qualification of the crime provided for in Article 272 of the Criminal Code of the Russian Federation. The high level of uncertainty in the interpretation of concepts related to illegal access to computer information is emphasized, which quite naturally causes the lack of uniform judicial and investigative practice in the application of this article. The analysis of objective and subjective signs of such a crime is carried out. The proposals on amendments to the current legislation are substantiated.

Methods. The methodological basis of the research is made up of general scientific (analysis, synthesis, induction, deduction, classification, comparison, comparison) and private scientific methods of legal research (historical-legal, comparative legal, formal-logical, systemic).

Results. The conducted research shows that despite the active development of issues of practical application of the provisions of Art. 272 of the Criminal Code of the Russian Federation in domestic science, it should be noted that many aspects of the qualification of this attack are currently unresolved. The authors have proposed an addition that will allow law enforcement officers to more accurately define and qualify crimes related to illegal access to computer information.

Keywords: unauthorized access, computer crimes, computer information.

Введение

В современном обществе информационные технологии и цифровизация играют весьма существенную роль, проникая в различные сферы жизни людей. Всевозможные коммуникация, повседневное общение, быстрое и целенаправленное планирование рабочих задач и полный незабываемых впечатлений досуг – неразрывно связаны с компьютерной информацией. В процессе своей жизнедеятельности люди постоянно сталкиваются с фотографированием, аудиозаписью, способностями быстро и многократно обмениваться в различных программах-мессенджерах текстовыми и голосовыми сообщениями, документами, графическими изображениями, возможностью осуществлять мгновенное управление финансами и осуществлять денежные переводы. Наличие такого информационного пространства подразумевает использование компьютерной информации, безусловно, в благих целях, но вместе с тем активизирует противоправную деятельность ряда недобросовестных личностей и социальных групп.

Методы исследования

Авторами при исследовании применялись общие научные (анализ, синтез, индукция, дедукция, классификация, сопоставление, сравнение) и частные научные методы юридического исследования (историко-юридический, сравнительно-правовой, формально-логический, системный).

Результаты

Неправомерный доступ к компьютерной информации – общественно опасное деяние, непосредственно связанное с тем, что современные технологии – телефоны, компьютеры и другие технические устройства различного назначения (кассовые аппараты, смартфоны, планшеты, терминалы по приёму платежей), а также информация, которую они передают и хранят, не только затрагивают все сферы деятельности нашего общества, но и являются очень социально значимым благом, посягательство на которое должно преследоваться уголовным законом. Окончательная законность операций с данными, включая компьютерную информацию, а также работу

компьютеров, их систем и сетей, в первую очередь, зависит от наличия согласия и одобрения со стороны оператора или владельца данной информации, или техники; во вторую очередь, от соблюдения требований по обработке и передаче данных и правил эксплуатации.

Проникновение и незаконное ознакомление с компьютерной информацией может подорвать выполнение банковских операций, нашу оборонную способность, социальное обеспечение, транспортную инфраструктуру и, в конечном итоге, национальную безопасность[1]. Именно поэтому уголовное законодательство, наряду с законами из других отраслей права, защищает законные процессы по сбору, хранению, поиску, обработке и передаче информации.

Законодатель не определяет содержание видового объекта, указывая лишь сферу охраняемых отношений. Проведя анализ структуры УК РФ, можно сделать вывод о том, что родовым объектом состава преступления, предусмотренного ст. 272 УК РФ, являются общественные отношения по поводу общественной безопасности и общественного порядка [1, с. 174].

Под непосредственным объектом неправомерного доступа к компьютерной информации понимаются общественные отношения, обеспечивающие право обладателя компьютерной информации на ее безопасное создание, хранение, использование и передачу.

Дополнительный объект неправомерного доступа к компьютерной информации факультативен, его наличие зависит от вида вреда, причиненного правам и законным интересам потерпевшего.

Дополнительный объект – это общественные отношения, заслуживающие самостоятельной защиты применительно к целям и задачам издания конкретной нормы, которые охраняются законом лишь попутно, так как они неизбежно ставятся в опасность причинения вреда при посягательстве на основной объект [2, с. 84]. Он повышает степень

[1] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации от 5 июля 2021 г. № 27 (часть II) ст. 5351;

общественной опасности исследуемого преступления. Им могут выступать отношения в области права собственности, в области авторского права, личные права и свободы граждан, неприкосновенность частной жизни.

Большой научный и практический интерес вызывает вопрос определения предмета неправомерного доступа к охраняемой законом компьютерной информации. Под предметом преступления в отечественной уголовно-правовой науке обычно понимается элемент нормального правомерного общественного отношения, воздействуя на который, лицо нарушает (пытается нарушить) охраняемое законом общественное отношение [3, с. 41]. В последнее время в предмет преступления ученые включает не только материальные объекты, но и объекты нематериального мира. Например, Колмаков П.А., Воробьёв В.В. учитывая специфичность и многообразность преступлений в сфере компьютерной информации считают, что необходим более широкий подход к определению предмета преступления. В зависимости от вида этих преступлений в качестве предметов следует считать не только охраняемую законом компьютерную информацию, но и иную компьютерную информацию, а также аппаратно-технический комплекс ЭВМ, системы ЭВМ или их сети [4, с. 68]. Мицкевич А.Ф., Суслопаров А.В. считают предметом рассматриваемых составов «данные» [5, с. 206]. В.Б. Вехов считает, что предметом такого рода преступлений является машинная информация, компьютер, компьютерная система или компьютерная сеть [6, с. 79].

Не смотря на то, что статья 272 УК РФ, предусматривающая уголовную ответственность за неправомерный доступ к компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, согласно официальной статистике[2], является наиболее востребованным и применимым составом преступления из

[2] Судебная статистика РФ [Электронный ресурс] – Режим доступа: https://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17?ysclid=ln60fdhccm646861487 (дата обращения 10.11.2023).

всех уголовно-правовых запретов главы 28 УК РФ, проблемы с ее правоприменением у практиков остаются.

Как показывает практика, законодательство не поспевает за все вновь возникающими новыми технологиями и формами преступности [7, с. 78], такими как мошенничество с использованием электронной почты или сети «Интернет», кража «цифровой личности», кража данных платежных карт и другой финансовой информации, хищение и перепродажа корпоративных данных, кибершантаж, атаки с использованием программ-вымогателей, криптоджекинг (майнинг криптовалют с использованием чужих информационных ресурсов).

Одна из распространенных трудностей, имеющая место при квалификации общественно опасных деяний, ответственность за которые предусмотрена ст. 272 УК РФ, связана с неоднозначной трактовкой понятия «неправомерный доступ к компьютерной информации» [8, с. 201].

Следует отметить, что в понимании терминов «информация», «сведения», «сообщения», «данные» есть определенные различия. В то время как данные представляют собой объективные факты или сведения, информация возникает только у субъекта, который анализирует и сопоставляет эти данные с своими знаниями об объекте. То есть информация используется субъектом для принятия управленческих решений. С учетом этого, применение термина «информация» в данном контексте, с точки зрения науки информатики, может считаться несколько некорректным, однако в примечании к статье 272 УК РФ, законодатель между этими терминами фактически поставил знак равенства.

Легитимно неразрешенным остался вопрос правильного толкования термина «охраняемая законом информация», что вполне закономерно обуславливает отсутствие единообразной судебно-следственной практики применения ст. 272 УК РФ. Отдельные суды, придерживаясь рекомендаций Генеральной прокуратуры РФ, указывают, что неправомерные манипуляции с

открытой (общедоступной) информацией не подпадают под действие данной статьи [9, с. 302].

Вместе с тем все большее распространение стала получать позиция, согласно которой под охраняемой законом информацией следует понимать так называемую закрытую информацию, к которой относятся государственная, служебная, коммерческая, банковская, врачебная, нотариальная, адвокатская тайна, персональные данные и другие виды тайн [10, с. 85].

По мнению А. Ю. Карамнова и М. Ю. Дворецкого пробелы законодательства способствуют безнаказанному созданию и распространению программ-вирусов [11, с. 169].

В Методических рекомендациях Генеральной прокуратуры Российской Федерации, в частности, указано, что по смыслу ст. 272 УК РФ охраняемой законом информацией являются лишь сведения, в отношении которых установлен специальный режим правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные)[3].

Так, отменяя обвинительный приговор, вышестоящий суд указал: «По смыслу закона под охраняемой законом понимается информация, для которой установлен специальный режим ее правовой защиты... то есть информация ограниченного доступа... При этом судом сделаны выводы, что указанная информация (новости, советы логопеда, психолога и т.п.) охраняется законом - статьей 6 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» ... Однако данные выводы противоречат содержанию вышеуказанных законодательных актов Российской Федерации... Информация на сайте, в редактировании и удалении которой признана виновной К., является общедоступной информацией, к которой относятся общеизвестные сведения и для которой отсутствует

[3] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс]: утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «Гарант» - Режим доступа: https://www.garant.ru/products/ipo/prime/doc/70542118/;

необходимость установления специального режима ее правовой защиты. Указанное закреплено и в пунктах 1.7 и 3.2 Положения о сайте МБДОУ "1", утвержденного Приказом заведующей учреждением, согласно которому информационный ресурс сайта является открытым и общедоступным, информация на сайте является открытой и общедоступной, если иное не определено специальными документами. При этом таковых в материалах уголовного дела не имеется»[4].

Компьютерная информация доступна только законным пользователям, то есть тем, кто имеет право использовать компьютерные системы. Это разрешение может быть предоставлено администратором базы данных.

Момент начала выполнения объективной стороны неправомерного доступа к охраняемой законом компьютерной информации А.Ю. Решетников и Е.А. Русскевич определяют «осуществление лицом действий, которые направлены на преодоление средств защиты информации и их нейтрализацию» [12, с. 87].

К стадиям совершения неправомерного доступа относятся приготовление к преступлению (такие действия как получение логинов и паролей, планирование технической стороны совершения преступления, подыскание специализированных программ для доступа) и покушение (действия, непосредственно направленные на получение доступа, ввод паролей, использование программ для получения доступа к информации). Начало деяния связано с совершением данных действий.

Обязательный элемент объективной стороны данного состава – последствия. Общественно-опасное последствие – это такое вредное изменение в объекте уголовно-правовой охраны, которое предусмотрено УК РФ, и наступает или может наступить в результате совершения преступления.

---

[4]Приговор № 22-1054/2015 от 03.06.2015 Верховного Суда Чувашской Республики (Чувашская Республика): [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru

Статья 272 УК РФ устанавливает ответственность за незаконное получение доступа к информации, охраняемой в компьютерных системах. Само по себе проникновение в машинные носители (например, для ознакомления с информацией путем прочтения), не является достаточным для применения данной статьи. Согласно выстраиванию объективной стороны преступления в соответствии со статьей 272 УК РФ, совершение определенного деяния или наступление последствий, непосредственно предусмотренных законом, является обязательным. Это означает, что необходимо не только считывать информацию, но и незаконно обрабатывать ее, чтобы совершать незаконные действия, такие как уничтожение, блокирование, изменение и копирование информации.

Следует заметить, что согласно ч. 1 ст. 272 УК РФ уголовная ответственность возникает только при неправомерном доступе к компьютерной информации, который обязательно сопровождается блокированием, уничтожением, копированием или модификацией информации.

Уничтожение информации заключается в удалении файла (поименованной области на диске или другом машинном носителе) без технической возможности восстановления. «Формы уничтожения также могут быть разнообразными. Главный признак уничтожения - информацию невозможно восстановить» [13, с. 102]. У.В. Зинина полагает, что если есть возможность восстановить информацию, то такое деяние должно признаваться покушением на преступление, предусмотренное ст. 272 УК РФ[5]. А.А. Гребеньков считает, что при уничтожении информации преступление считается оконченным, если данная информация восстановлению не подлежит [14, с. 26].

Блокирование информации – это мера, направленная на ограничение доступа к конкретным данным без их удаления. В отличие от полного

[5]Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: Дис. ... канд. юрид. наук: 12.00.08 / Зинина Ульяна Викторовна; – Москва, 2007. - 33 с.

стирания, блокировка позволяет сохранить информацию, но делает ее недоступной для определенного пользователя или группы пользователей. Для этого могут использоваться различные методы, такие как установка паролей или перевод программы на специфичный для программирования язык, непонятный для неавторизованных лиц.

По мнению А.Г. Антонова и Д.В. Крюкова проявление общественной опасности такого деяния более очевидно в случае наступления последствий, отражённых в квалифицирующих признаках, установленных ч. 2-4 ст. 272 УК РФ [15, с. 168].

Под модификацией понимается изменение программы или базы данных с целью оптимизации ее поведения на конкретном оборудовании пользователя или под управлением конкретной программы. Во время модификации программный код может быть изменен, могут быть добавлены новые функции, исправлены ошибки и улучшены рабочие параметры. Однако изменения должны быть необходимыми и не мешать работе программы или базы данных.

Использование «взломанной» или модифицированной программы, без наличия других преступных действий, не является составом преступления по статье 272 УК РФ. Для образования состава данного преступления необходимо наличие незаконного доступа к компьютерной информации и ее модификации или копирования.

Декомпиляция программы для компьютеров или базы данных является отдельным процессом, отличным от модификации. Декомпиляция включает преобразование машинного кода в исходный текст программы с целью изучения ее структуры и кодирования. Машинный код представляет собой исходный текст, который был скомпилирован в символы, понятные компьютеру, в то время как исходный текст представляет алгоритм для обработки данных или управления ими, описанный на языке программирования.

Под копированием информации следует понимать процесс дублирования файла или системной области на диск.

Согласно действующей редакции ч. 1 ст. 272 УК РФ простое ознакомление или чтение информации без согласия владельца информации не является преступлением и не преследуется по уголовному законодательству, то есть не образует состава преступления.

Однако, речь идет зачастую не о фактах незаконного любопытства и проявления безразличия к собственности других, что уже само по себе является неприемлемым в современном обществе, а о фактах грубого вмешательства в частную жизнь, способных привести к серьезным негативным последствиям, как для индивидуальных лиц, так и для общества в целом. Необходимо четко понимать, что существуют определенные ситуации, когда действия человека представляют угрозу обществу, являются общественно опасными, но при этом неправомерный доступ к компьютерной информации был осуществлен исключительно для ознакомления с определенной информацией.

Учитывая вышеизложенное, предлагается в ч. 1 ст. 272 УК РФ внести изменения, а именно после слова «повлекло», следует дополнить следующими словами: «несанкционированное ознакомление» и далее по тексту:

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло несанкционированное ознакомление, уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

Такое дополнение позволит правоприменителям более точно определить и квалифицировать преступления, связанные с незаконным доступом к компьютерной информации. Понятие «несанкционированное ознакомление» охватывает как случаи, когда лицо получает доступ к данным без согласия их владельца, так и случаи, когда доступ был предоставлен, но был совершен с иной целью, чем предполагалось изначально.

Заключение

Таким образом, авторы приходят к выводу о том, что несмотря на активную разработку вопросов практического применения положений ст. 272 Уголовного кодекса Российской Федерации в отечественной науке, следует констатировать, что многие аспекты квалификации данного посягательства на сегодняшний день носят неразрешённый характер.

Причинно-следственная связь является ключевым элементом при привлечении лиц к ответственности за несанкционированный доступ к компьютерной информации. Доказательства должны подтверждать, что действия виновного лица напрямую привели к наступившим последствиям, указанным в законе. Для этого часто требуется проведение тщательного технического анализа компьютерных систем и сетей, а также сбор и анализ цифровых доказательств. Это позволяет установить не только факт несанкционированного доступа, но и связать его с конкретным лицом или группой лиц. Иными словами, должно быть установлено, что несанкционированный доступ привел к указанным последствиям, что поведение виновного реально могло привести к этим последствиям и что это поведение явилось основной причиной наступления последствий в виде уничтожения, вмешательства, изменения или копирования информации.

Принятие предложенного дополнения частично поможет устранить давно назревшую необходимость внесения соответствующих изменений в действующее законодательство. Однако оно не решит все имеющиеся проблемы правового и организационного характера. Отдельные положения законодательных и иных нормативных правовых актов необходимо усовершенствовать и привести в соответствие, исключая существующие противоречия между ними, и вызывающие неоднозначное толкование не только правоприменителями, но и отдельными учёными.

Библиографический список

1. Клещева, А. С. Особенности объекта и предмета преступлений в сфере компьютерной информации // Материалы национальной научно-практической конференции, 8 декабря 2017 года, Чита: Забайкальский государственный университет, 2018. – С. 173-177.

2. Ораздурдыев, А. М. Характеристика объекта составного преступления // Вестник Волжского университета им. В.Н. Татищева. – 2011. – № 75. – С. 80-85.

3. Динека, В. И., Жабский, В. А., Денисенко, М. В. Предмет преступления в уголовном праве // Ученые труды Российской академии адвокатуры и нотариата. – 2022. – № 1(64). – С. 40-47.

4. Колмаков, П. А. К вопросу о содержании и объеме предмета преступлений в сфере компьютерной информации / П. А. Колмаков, В. В. Воробьев // Вестник Оренбургского государственного университета. – 2011. – № 3(122). – С. 66-69.

5. Мицкевич А.Ф., Суслопаров А.В., 5.3. Понятие компьютерной информации по российскому и зарубежному уголовному праву/Пробелы в Российском законодательстве. // Издательский дом «Юр-ВАК». – 2010. – № 2. – с. 206-209.

6. Вехов В.Б. Преступления, связанные с неправомерным использованием баз данных и содержащейся в них компьютерной информации/Защита информации. Инсайд. //ООО Издательский дом «Афина». – 2008. – № 2 (20). С. 78-81.

7. Зайцева, С. Е. Исследование и анализ уголовной ответственности за преступления в сфере компьютерной информации в Российской Федерации и зарубежных странах / С. Е. Зайцева, С. Р. Сосновская // Актуальные проблемы современной науки : сборник статей международной научной конференции, Санкт-Петербург, 21 апреля 2023 года. – Санкт-Петербург:

Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ», 2023. – С. 78-83;
8. Зайцев В.С., Горбань, В.С. Проблемы квалификации преступления, предусмотренного ст. 272 УК РФ / В.С. Зайцев, В.С. Горбань // Научное и образовательное пространство: перспективы развития. Сборник материалов III Международной научно-практической конференции: в 2-х томах. Том 2. - 2016 – С. 200-204.
9. Демин, Д. В. Проблемы квалификации неправомерного доступа к компьютерной информации / Д. В. Демин // E-Scio. – 2022. – № 8(71). – С. 301-305.
10. Русскевич, Е. А. О проблемах квалификации неправомерного доступа к компьютерной информации / Е. А. Русскевич // Уголовное право. – 2017. – № 5. – С. 85-91.
11. Карамнов, А. Ю. Уголовная ответственность за преступления в сфере компьютерной информации в России и зарубежных государствах / А. Ю. Карамнов, М. Ю. Дворецкий // Вестник Воронежского института МВД России. – 2011. – № 2. – С. 165-169;
12. Решетников, А. Ю., Русскевич, Е. А. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации // Уголовное право. – 2018. – № 2. – С. 86-95;
13. Халиуллин, А. И. Уголовно-правовой аспект неправомерного уничтожения компьютерной информации // Вестник Самарской гуманитарной академии. Серия: Право. – 2013. – № 2(14). – С. 100-105.
14. Гребеньков, А.А. Уничтожение компьютерной информации как информационное преступление // Апробация. – 2016. – № 7(46). – С. 26-27.
15. Антонов А.Г., Крюков Д.В. К вопросу об общественной опасности неправомерного доступа к компьютерной информации, повлекшего ее блокирование // Ленинградский юридический журнал. 2021. № 2(64). С. 168–179.

Bibliograficheskij spisok

1. Kleshcheva, A. S. Osobennosti ob"ekta i predmeta prestuplenij v sfere komp'yuternoj informacii // Materialy nacional'noj nauchno-prakticheskoj konferencii, 8 dekabrya 2017 goda, CHita: Zabajkal'skij gosudarstvennyj universitet, 2018. – S. 173-177.

2. Orazdurdyev, A. M. Harakteristika ob"ekta sostavnogo prestupleniya // Vestnik Volzhskogo universiteta im. V.N. Tatishcheva. – 2011. – № 75. – S. 80-85.

3. Dineka, V. I., ZHabskij, V. A., Denisenko, M. V. Predmet prestupleniya v ugolovnom prave // Uchenye trudy Rossijskoj akademii advokatury i notariata. – 2022. – № 1(64). – S. 40-47.

4. Kolmakov, P. A. K voprosu o soderzhanii i ob"eme predmeta prestuplenij v sfere komp'yuternoj informacii / P. A. Kolmakov, V. V. Vorob'ev // Vestnik Orenburgskogo gosudarstvennogo universiteta. – 2011. – № 3(122). – S. 66-69.

5. Mickevich A.F., Susloparov A.V., 5.3. Ponyatie komp'yuternoj informacii po rossijskomu i zarubezhnomu ugolovnomu pravu/Probely v Rossijskom zakonodatel'stve. // Izdatel'skij dom «YUr-VAK». – 2010. – № 2. – s. 206-209.

6. Vekhov V.B. Prestupleniya, svyazannye s nepravomernym ispol'zovaniem baz dannyh i soderzhashchejsya v nih komp'yuternoj informacii/Zashchita informacii. Insajd. //OOO Izdatel'skij dom «Afina». – 2008. ¬– № 2 (20). S. 78-81.

7. Zajceva, S. E. Issledovanie i analiz ugolovnoj otvetstvennosti za prestupleniya v sfere komp'yuternoj informacii v Rossijskoj Federacii i zarubezhnyh stranah / S. E. Zajceva, S. R. Sosnovskaya // Aktual'nye problemy sovremennoj nauki : sbornik statej mezhdunarodnoj nauchnoj konferencii, Sankt-Peterburg, 21 aprelya 2023 goda. – Sankt-Peterburg: CHastnoe nauchno-obrazovatel'noe uchrezhdenie dopolnitel'nogo professional'nogo obrazovaniya Gumanitarnyj nacional'nyj issledovatel'skij institut «NACRAZVITIE», 2023. – S. 78-83;

8. Zajcev V.S., Gorban', V.S. Problemy kvalifikacii prestupleniya, predusmotrennogo st. 272 UK RF / V.S. Zajcev, V.S. Gorban' // Nauchnoe i obrazovatel'noe prostranstvo: perspektivy razvitiya. Sbornik materialov III

Mezhdunarodnoj nauchno-prakticheskoj konferencii: v 2-h tomah. Tom 2. - 2016 – S. 200-204.
9. Demin, D. V. Problemy kvalifikacii nepravomernogo dostupa k komp'yuternoj informacii / D. V. Demin // E-Scio. – 2022. – № 8(71). – S. 301-305.
10. Russkevich, E. A. O problemah kvalifikacii nepravomernogo dostupa k komp'yuternoj informacii / E. A. Russkevich // Ugolovnoe pravo. – 2017. – № 5. – S. 85-91.
11. Karamnov, A. YU. Ugolovnaya otvetstvennost' za prestupleniya v sfere komp'yuternoj informacii v Rossii i zarubezhnyh gosudarstvah / A. YU. Karamnov, M. YU. Dvoreckij // Vestnik Voronezhskogo instituta MVD Rossii. – 2011. – № 2. – S. 165-169;
12. Reshetnikov, A. YU., Russkevich, E. A. Nekotorye voprosy kvalifikacii neokonchennyh prestuplenij v sfere komp'yuternoj informacii // Ugolovnoe pravo. – 2018. – № 2. – S. 86-95;
13. Haliullin, A. I. Ugolovno-pravovoj aspekt nepravomernogo unichtozheniya komp'yuternoj informacii // Vestnik Samarskoj gumanitarnoj akademii. Seriya: Pravo. – 2013. – № 2(14). – S. 100-105.
14. Greben'kov, A.A. Unichtozhenie komp'yuternoj informacii kak informacionnoe prestuplenie // Aprobaciya. – 2016. – № 7(46). – S. 26-27.
15. Antonov A.G., Kryukov D.V. K voprosu ob obshchestvennoj opasnosti nepravomernogo dostupa k komp'yuternoj informacii, povlekshego ee blokirovanie // Leningradskij yuridicheskij zhurnal. 2021. № 2(64). S. 168–179.

Представленный материал ранее нигде не публиковался и в настоящее время не находится на рассмотрении на предмет публикации в других изданиях. Заявляем об отсутствии конфликта интересов, связанного с публикацией данной статьи в журнале «Вестник Калининградского филиала Санкт-Петербургского университета МВД России». Разрешаем размещение полнотекстовой версии статьи, а также её частей в открытом доступе в сети Интернет, а также на официальных каналах журнала в социальных сетях.

При создании статьи не использовались возможности искусственного интеллекта.

Авторы внесли равный вклад в создание статьи.