# УГОЛОВНОЕ ПРАВО И ОСОБЕННОСТИ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ

**Сергей Владимирович ВЕКЛЕНКО,**
доктор юридических наук, профессор, ORCID 0000-0002-8625-8656
Санкт-Петербургский университет МВД России (г. Санкт-Петербург)
профессор кафедры уголовного права
Заслуженный работник высшей школы Российской Федерации
*veklenkosv@mail.ru*

**Алексей Игоревич ЛОКНОВ,**
кандидат технических наук, доцент, ORCID 0000-0003-4425-1939
Санкт-Петербургский университет МВД России (г. Санкт-Петербург)
доцент кафедры информационной безопасности
*info_for_aleksey@mail.ru*

Научная статья
УДК 343.34

# СОВЕРШЕНСТВОВАНИЕ УГОЛОВНО-ПРАВОВОГО ПРОТИВОДЕЙСТВИЯ НЕПРАВОМЕРНОМУ ДОСТУПУ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

**КЛЮЧЕВЫЕ СЛОВА. Неправомерный доступ, компьютерная информация, компьютерные преступления, уголовно-правовое противодействие.**

**АННОТАЦИЯ.** ***Введение.*** *Актуальность исследования продиктована необходимостью анализа норм уголовного закона о преступлениях, связанных с неправомерным доступом к компьютерной информации, объективных и субъективных признаков составов данных преступлений, уголовной ответственности за их совершение, а также необходимостью формулирования 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 неопределенности трактовки понятий, связанных с неправомерным доступом к компьютерной информации, что вполне закономерно обусловливает отсутствие единообразной судебно-следственной практики применения данной статьи. Проведен анализ объективных и субъективных признаков рассматриваемого 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.*** *Проведенное исследование показывает, что, несмотря на активную разработку вопросов практического применения положений ст. 272 Уголовного кодекса Российской Федерации в отечественной науке, есть основания констатировать, что на сегодняшний день многие аспекты квалификации данного посягательства носят спорный и нормативно неразрешенный характер. Авторы предлагают внести в указанную статью кодекса дополнение, которое позволит правоприменителям более точно определять и квалифицировать преступления, связанные с незаконным доступом к компьютерной информации.*

## ВВЕДЕНИЕ

В современном обществе информационные технологии и цифровизация играют весьма существенную роль, проникая в различные сферы жизни людей. Разнообразные виды коммуникации, повседневное общение, возможность быстрого и целенаправленного планирования рабочих задач и полный незабываемых впечатлений досуг неразрывно связаны с компьютерной информацией. В процессе своей жизнедеятельности люди постоянно используют компьютерные технологии: для фотографирования, видеосъемки, аудиозаписи, быстрого обмена текстовыми и голосовыми сообщениями, документами, изобра-

**Sergey V. VEKLENKO,**
Doctor of Law, Professor, ORCID 0000-0002-8625-8656
Saint-Petersburg University of the Ministry of the Interior of Russia (Saint-Petersburg, Russia)
Professor of the Department of Criminal Law
Honored Worker of the Higher School of the Russian Federation
*veklenkosv@mail.ru*

**Aleksey I. LOKNOV,**
Cand. Sci. (Engineering), Associate Professor, ORCID 0000-0003-4425-1939
Saint-Petersburg University of the Ministry of the Interior of Russia (Saint-Petersburg, Russia)
Associate Professor of the Department of Information Security
*info_for_aleksey@mail.ru*

**IMPROVEMENT OF CRIMINAL LAW COUNTERACTION TO ILLEGAL ACCESS TO COMPUTER INFORMATION**

**KEYWORDS. Unauthorized access, computer information, computer crimes, criminal legal counteraction.**

**ANNOTATION.** ***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 Art. 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.*

жениями, управления финансами, осуществления денежных переводов и т.д. Наличие столь объемного информационного пространства подразумевает широкое использование компьютерной информации. В первую очередь, безусловно, в благих целях. Но вместе с тем актуализирует и активизирует противоправную деятельность недобросовестных личностей и целых преступных групп, связанную с неправомерным доступом к такой информации.

## МЕТОДЫ

В настоящей статье изложены основные результаты проведенного авторами исследования. При его осуществлении 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 приему платежей), а также информация, которую они передают и хранят, – не только затрагивают все сферы деятельности нашего общества, но и являются в высокой степени социально значимым благом, посягательство на которое должно преследоваться уголовным законом. 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 этих данных и этой информации или техники, во вторую очередь – от соблюдения требований, предъявляемых к обработке и передаче информации, и правил эксплуатации компьютерной техники.

Проникновение в системы хранения и обработки компьютерной информации и незаконное ознакомление с ней может подорвать нормальный порядок выполнения банковских операций, создать помехи обороноспособности страны, нарушить деятельность системы социального обеспечения, привести к повреждению транспортной инфраструктуры и в конечном итоге нанести ущерб национальной безопасности[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 преступления, предусмотренного ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», указывая лишь сферу

[1] Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2021. № 27. Ч. II. Ст. 5351.

охраняемых отношений. На основе результатов анализа структуры Уголовного кодекса Российской Федерации можно сделать вывод о том, что родовым объектом такого преступления 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 преступления в данном случае 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 общественной опасности исследуемого преступления. Таковым могут быть отношения в области права собственности, в области авторского права, личные права и свободы граждан, неприкосновенность частной жизни.

Большой научный и практический интерес вызывает вопрос об определении предмета неправомерного доступа к 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 качестве предмета преступления ученые рассматривают не только материальные объекты, но и объекты нематериального мира. Например, П.А. Колмаков и В.В. Воробьев с учетом специфичности и многообразности преступлений в сфере компьютерной информации считают, что необходим более широкий подход к определению предмета преступления. В зависимости от вида преступления его предметом следует видеть 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]. А.Ф. Мищкевич и А.В. Суслопаров называют предметом преступлений изучаемой нами группы «данные» [5, с. 206]. В.Б. Вехов полагает, что предметом таких преступлений является машинная информация, компьютер, компьютерная система или компьютерная сеть [6, с. 79].

Несмотря на то, что ст. 272 УК РФ, предусматривающая уголовную ответственность за неправомерный доступ к компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, является, согласно официальной статистике[1], наиболее востребованным и наиболее часто применяемым при квалификации составом преступления из всех уголовно-правовых запретов гл. 28 УК РФ, проблемы с ее практическим применением остаются.

Как показывает практика, законодательство не поспевает за развитием современных технологий и возникновением все новых форм преступности [7, с. 78]. Среди последних, например, 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) и т.д.

Необходимо подчеркнуть, что при квалификации общественно опасных деяний, ответственность за которые предусмотрена ст. 272 УК РФ, вызывает серьезные затруднения неоднозначность трактовки понятия «неправомерный доступ к компьютерной информации» [8, с. 201].

Обратим внимание на то, что существуют различия в трактовке терминов «информация», «сведения», «сообщения», «данные». В то время как данные представляют собой объективные факты или сведения, информация возникает только у субъекта, который анализирует и сопоставляет эти данные со своими знаниями об объекте. То есть информация используется субъектом для принятия управленческих решений. С учетом этого применение термина «информация» в тех или иных контекстах с точки зрения науки информатики может считаться некорректным, однако в примечании к ст. 272 УК РФ законодатель между терминами «информация», «сведения», «сообщения», «данные» фактически поставил знак равенства.

Кроме того, остался неразрешенным вопрос о правильном толковании термина «охраняемая законом информация», что вполне закономерно обусловливает отсутствие единообразной судебно-следственной практики применения ст. 272 УК РФ. Некоторые суды, придерживаясь рекомендаций Генеральной прокуратуры Российской Федерации, указывают на то, 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,

[1] Судебная статистика РФ // URL: https://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17?ysclid=ln60fdhccm646861487 (дата обращения: 10.11.2023).

в отношении которых установлен специальный режим правовой защиты (например государственная, служебная и коммерческая тайна, персональные данные)[1].

Так, Верховный Суд Чувашской Республики, отменяя обвинительный приговор в качестве вышестоящего суда, отметил следующее: «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 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»[2].

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 преступления, которым является неправомерный доступ к охраняемой законом компьютерной информации, А.Ю. Решетников и Е.А. Русскевич определяют как «осуществление лицом действий, которые направлены на преодоление средств защиты информации и их нейтрализацию» [12, с. 87].

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

Обязательный элемент объективной стороны состава преступления рассматриваемого вида – 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.

Статья 272 УК РФ устанавливает ответственность за незаконное получение доступа к охраняемой информации, содержащейся в компьютерных системах. Само по себе проникновение в машинные носители (например для ознакомления с информацией путем прочтения) не является достаточным для квалификации преступления по данной статье. Согласно тому, как выстроена объективная сторона преступления в соответствии со ст. 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[3]. 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 стирания блокировка позволяет сохранить информацию, но делает ее недоступной для определенного пользователя или группы пользователей. Для блокировки могут использоваться различные методы, например 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 деяния рассматриваемого нами вида более очевидно в случае наступления последствий, отраженных в квали-

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации: утв. Генпрокуратурой России от 30.05.2014 // СПС «Гарант».
[2] Приговор Верховного Суда Чувашской Республики от 03.06.2015 № 22-1054/2015 // Судебные и нормативные акты РФ // URL: https://sudact.ru.
[3] Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: Дис. ... канд. юрид. наук. М., 2007.

фицирующих признаках, установленных ч.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 должны мешать работе программы или базы данных.

Использование «взломанной» или модифицированной программы без наличия других преступных действий не является составом преступления по ст. 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 процессом, отличающимся от модификации. Декомпиляция представляет собой преобразование машинного кода в исходный текст программы с целью изучения ее структуры и кодирования. Машинный код – это исходный текст, который был скомпилирован в символы, понятные компьютеру, в то время как сам по себе исходный текст является алгоритмом для обработки данных или управления ими, описанным 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, способного привести к серьезным негативным последствиям как для индивидуальных лиц, так и для общества в целом. Необходимо четко понимать, что бывают ситуации, когда действия человека представляют угрозу обществу, являются общественно опасными, но при этом неправомерный доступ к компьютерной информации в их рамках был осуществлен исключительно для ознакомления с той или иной конкретной информацией.

Учитывая вышеизложенное, предлагаем в ч. 1 ст. 272 УК РФ внести изменение, а именно дополнить ее формулировку после слова «повлекло» словами «несанкционированное ознакомление»:

*«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 определять 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**

В результате проведенного исследования мы приходим к выводу о том, что, несмотря на активную разработку вопросов практического применения положений ст. 272 УК РФ, в отечественной науке многие аспекты квалификации описанного в ней посягательства в настоящее время носят спорный и нормативно неразрешенный 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, блокирования, изменения или копирования информации.

Законодательное закрепление предложенного нами дополнения частично поможет устранить давно назревшую необходимость внесения изменений в действующее законодательство. Однако оно не решит все имеющиеся проблемы правового и организационного характера, касающиеся применения на практике ст. 272 УК РФ. Некоторые положения законодательных и иных нормативных правовых актов необходимо совершенствовать, устраняя существующие между ними противоречия, вызывающие неоднозначное толкование норм, представленных в ст. 272 УК РФ, не только правоприменителями, но и рядом ученых. ■

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Клещева А.С. Особенности объекта и предмета преступлений в сфере компьютерной информации // Материалы национальной научно-практической конференции. Чита, 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., Воробьев В.В. К вопросу о содержании и объеме предмета преступлений в сфере компьютерной информации // Вестник Оренбургского государственного университета. 2011. № 3 (122). С. 66-69.

5. Мицкевич А.Ф., Суслопаров А.В. Понятие компьютерной информации по российскому и зарубежному уголовному праву // Пробелы в российском законодательстве. 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. 2008. № 2 (20). С. 78-81.

7. Зайцева С.Е., Сосновская С.Р. Исследование и анализ уголовной ответственности за преступления в сфере компьютерной информации в Российской Федерации и зарубежных странах // Актуальные проблемы современной науки: сборник статей международной научной конференции, Санкт-Петербург, 21 апреля 2023 г. СПб, 2023. С. 78-83.

8. Зайцев В.С., Горбань В.С. Проблемы квалификации преступления, предусмотренного ст. 272 УК РФ // Научное и образовательное пространство: перспективы развития. Сборник материалов III Международной научно-практической конференции: в 2-х т. Чебоксары, 2016. Т. 2. С. 200-204.

9. Демин Д.В. Проблемы квалификации неправомерного доступа к компьютерной информации // E-Scio. 2022. № 8 (71). С. 301-305.

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

11. Карамнов А.Ю., Дворецкий М.Ю. Уголовная ответственность за преступления в сфере компьютерной информации в России и зарубежных государствах // 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.

**REFERENCES**

1. Kleshcheva A.S. Osobennosti ob»ekta i predmeta prestuplenij v sfere komp'yuternoj informacii // Materialy nacional'noj nauchno-prakticheskoj konferencii, 8 dekabrya 2017 g. 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., Vorob'ev V.V. K voprosu o soderzhanii i ob»eme predmeta prestuplenij v sfere komp'yuternoj informacii // Vestnik Orenburgskogo gosudarstvennogo universiteta. 2011. № 3 (122). S. 66-69.

5. Mickevich A.F., Susloparov A.V. Ponyatie komp'yuternoj informacii po rossijskomu i zarubezhnomu ugolovnomu pravu // Probely v Rossijskom zakonodatel'stve. 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. 2008. № 2 (20). S. 78-81.

7. Zajceva S.E., Sosnovskaya S.R. Issledovanie i analiz ugolovnoj otvetstvennosti za prestupleniya v sfere komp'yuternoj informacii v Rossijskoj Federacii i zarubezhnyh stranah // Aktual'nye problemy sovremennoj nauki: sbornik statej mezhdunarodnoj nauchnoj konferencii, Sankt-Peterburg, 21 aprelya 2023 g. Sankt-Peterburg, 2023. S. 78-83.

8. Zajcev V.S., Gorban' V.S. Problemy kvalifikacii prestupleniya, predusmotrennogo st. 272 UK RF // Nauchnoe i obrazovatel'noe prostranstvo: perspektivy razvitiya. Sbornik materialov III Mezhdunarodnoj nauchno-prakticheskoj konferencii: v 2-h t. Cheboksary, 2016. T. 2. S. 200-204.

9. Demin D.V. Problemy kvalifikacii nepravomernogo dostupa k komp'yuternoj informacii // E-Scio. 2022. № 8 (71). S. 301-305.

10. Russkevich E.A. O problemah kvalifikacii nepravomernogo dostupa k komp'yuternoj informacii // Ugolovnoe pravo. 2017. № 5. S. 85-91.

11. Karamnov A.Yu., Dvoreckij M.Yu. Ugolovnaya otvetstvennost' za prestupleniya v sfere komp'yuternoj informacii v Rossii i zarubezhnyh gosudarstvah // 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.

*Авторы заявляют об отсутствии конфликта интересов.*
*Авторами внесён равный вклад в написание статьи.*
*The authors declare no conflicts of interests.*
*The authors have made an equal contribution to the writing of the article.*


**ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ**
Векленко С.В., Локнов А.И. Совершенствование уголовно-правового противодействия неправомерному доступу к компьютерной информации // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2024. № 1 (75). С. 9-15.