Научная статья
УДК 343.23(07)
DOI: 10.37973/KUI.2024.37.40.008

К ВОПРОСУ О СОДЕРЖАНИИ ПРИЗНАКА «ВРЕД КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ РОССИЙСКОЙ ФЕДЕРАЦИИ» ДЛЯ ЦЕЛЕЙ ЧАСТЕЙ 2 И 3 СТАТЬИ 274[1] УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ

Николай Валерьевич Ермолаев,
Уральский юридический институт МВД России, Екатеринбург, Россия,
Nikolaiermolaev96@mail.ru

Аннотация

Введение: в статье приводятся результаты проведенного автором исследования признака «вред критической информационной инфраструктуре Российской Федерации».

Материалы и методы: методологическую базу исследования составили общенаучные и частнонаучные методы познания действительности. Из числа частнонаучных методов применялся формально-юридический метод, включающий определенную систему обработки и анализа нормы уголовного закона и материалов судебной практики по уголовным делам, возбужденным по ст. 274[1] УК РФ. Материалами исследования послужили нормы уголовного законодательства Российской Федерации, положения постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37, материалы судебной практики по уголовным делам, возбужденным по ст. 274[1] УК РФ за 2020 – 2023 годы, а также отечественная научная литература по данной проблематике.

Обзор литературы: теоретической основой исследования послужили труды отечественных ученых в отрасли уголовно-правовых наук, в частности, работы М.А. Ефремовой, Е.А. Русскевича, С.С. Шахрай, Е.А. Соловьевой, А.Ю. Решетникова, И.И. Малыгина.

Результаты исследования: на основе анализа нормативной базы и трудов ученых автор делает вывод, что признак «вред критической информационной инфраструктуре Российской Федерации» раскрыт не полностью. В ходе изучения материалов судебно-следственной практики автор заключает, что суды по-разному описывают признак «вред критической информационной инфраструктуре Российской Федерации». Однако сущность указанного признака, описываемого судами, практически идентична.

Обсуждение и заключение: на основе анализа законодательства о связи, информации и критической информационной инфраструктуры Российской Федерации, а также актуальных материалов судебной практики делается вывод, что такой вред чаще всего определяется как нарушение состояния защищенности компьютерной информации.

Ключевые слова: критическая информационная инфраструктура Российской Федерации; вред критической информационной инфраструктуре Российской Федерации; объекты критической информационной инфраструктуры Российской Федерации; нарушение безопасности компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации

Для цитирования: Ермолаев Н.В. К вопросу о содержании признака «вред критической информационной инфраструктуре Российской Федерации» для целей частей 2 и 3 статьи 274[1] Уголовного кодекса Российской Федерации // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 1 (55). С. 68 – 75. DOI: 10.37973/KUI.2024.37.40.008

Scientific article
UDC 343.23(07)
DOI: 10.37973/KUI.2024.37.40.008

THE CONTENT OF THE SIGN "HARM TO CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION" FOR THE PURPOSES OF PART 2 AND PART 3 OF ARTICLE 274[1] OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

Nikolay Valeryevich Ermolaev,
Ural Law Institute of the Ministry of Internal Affairs of Russia, Yekaterinburg, Russia,
Nikolaiermolaev96@mail.ru

Abstract

Introduction: the author presents results of his study of the attribute "threats to critical information infrastructure of Russia".

Materials and Methods: universal and specific scientific research methods constituted the methodological basis for the study. As well as legal method which included certain processing and analysis of the criminal law and criminal cases initiated under Article 274[1] of the Criminal Code of the Russian Federation.

The Criminal Code of the Russian Federation, provisions of Resolution of the Plenum of the Supreme Court of the Russian Federation No. 37 of 15.12.2022, criminal cases initiated under Article 274[1] for 2020 – 2023, as well as Russian scientific literature on the subject were research materials.

Literature Review: theoretical basis for the study were works by Russian penal scientists such as: M.A. Efremova, E.A. Russkevich, S.S. Shakhrai, E.A. Solovieva, A.Yu. Reshetnikov, and I.I. Malygin.

Results: basing on the legal framework and scientific literature the author concludes that the attribute "threats to critical information infrastructure of Russia" is not fully evolved. During the study of forensic materials, the author concludes that courts use various methods to describe the attribute. However, at the end of the study he finds that the attribute is almost identical in essence.

Discussion and Conclusions: based on the law on telecommunication, information and critical information infrastructure of the Russian Federation, current case law, the author concludes that the threat is determined as computer information security breach.

Keywords: critical information infrastructure of the Russian Federation; damage to CII of the Russian Federation; objects of CII of the Russian Federation; violation of the security of computer information contained in the CII of the Russian Federation

For citation: Ermolaev N.V. The Content of the Sign "Harm to the Critical Information Infrastructure of the Russian Federation" for the Purposes of Article 274[1] of the Criminal Code of the Russian Federation. Bulletin of the Kazan Law Institute of MIA of Russia. 2024;15(1):68-75. (In Russ.). DOI: 10.37973/KUI.2024.37.40.008

Введение

Информационное общество предполагает активное использование критической информационной инфраструктуры Российской Федерации (далее – КИИ РФ) в таких ключевых сферах государственной деятельности, как здравоохранение, связь, банковская и иная финансовая деятельность и т.п. Поэтому, по мнению Е.А. Соловьевой, обеспечение устойчивого и бесперебойного функционирования КИИ РФ в мирное время, в период непосредственной агрессии и в военное время определены доктриной информационной безопасности, утвержденной указом Президента РФ от 5 декабря 2016 № 646[1], как национальный интерес в информационной сфере [1].

Уголовно-правовая охрана объектов КИИ Российской Федерации является приоритетной задачей государства и регулируется в том числе ст. 274[1] УК РФ, которой уголовный закон дополнен еще в 2018 году[2].

Конструкцию ст. 274[1] УК РФ следует считать сложной, поскольку ее части включают самостоятельные и не связанные между собой составы преступлений.

[1] Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 05.12.2016 № 646. СПС «КонсультантПлюс» (дата обращения: 10.10.2023).

[2] Уголовный кодекс Российской Федерации. СПС «КонсультантПлюс» (дата обращения: 10.10.2023).

Тем не менее ч. 2 и 3 ст. 274[1] УК РФ объединяет наличие общественно-опасных последствий – «причинение вреда критической информационной инфраструктуре Российской Федерации».

В частности, ч. 2 ст. 274[1] УК РФ предусматривает ответственность за неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на КИИ РФ, или иных вредоносных компьютерных программ, если он повлек причинение вреда КИИ РФ.

В свою очередь, ч. 3 ст. 274[1] УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой законом компьютерной информации, содержащейся в КИИ РФ, или информационных систем (далее – ИС), информационно-телекоммуникационных сетей (далее – ИТКС), автоматизированных систем управления (далее – АСУ ТП), сетей электросвязи, относящихся к КИИ РФ, либо правил доступа к указанной информации, ИС, ИТКС, АСУ ТП, если оно повлекло причинение вреда КИИ РФ[1].

Материалы и методы

Эмпирическую основу исследования составили опубликованные данные судебной статистики и судебных решений, материалы 48 уголовных дел (на момент исследования), возбужденных по ч.2 и ч.3 ст. 274[1] УК РФ в различных регионах Российской Федерации, а также отечественное законодательство и труды отечественных ученых. Методологическую основу исследования составили общенаучные и частнонаучные методы познания действительности.

Обзор литературы

Исследованию вопросов уголовно-правовой охраны компьютерной информации посвящены научные труды С.С. Шахрая [2], И.И. Малыгина [3], А.В. Суслопарова [4], М.А. Ефремовой [5], В.Г. Степанова-Егиянца [6].

Помимо этого, изучению обозначенных явлений посвящены труды Е.А. Соловьевой [1], И.А. Яковенко [7], Е.А. Русскевича [8], А.В. Пелевиной [9], Р.И. Дремлюги [10], С.Д. Бражника [11] и др.

Результаты исследования

Исходя из смысла диспозиций ч. 2 и ч. 3 ст. 274[1] УК РФ, указанные составы преступлений являются материальными, т.е. считаются оконченными с момента причинения вреда КИИ РФ.

Отметим, что правомерность доступа к компьютерной информации определяется наличием у лица права проникновения в источник информации[2].

Конструкция ч. 3 ст. 274[1] УК РФ является более сложной. Ч. 3 ст. 274[1] УК РФ содержит в диспозиции: «Нарушение правил эксплуатации средств хранения, обработки или передачи информации, находящейся на объектах КИИ РФ, … либо правил доступа к указанной информации, информационным системам…». Разделительный союз «либо» в контексте ч. 3 ст. 274[1] УК РФ означает, что диспозиция содержит в себе два альтернативных варианта действия.

Отметим, что «эксплуатация компьютерной системы» представляет собой ее активное использование с целью достижения определенного результата. В широком смысле эксплуатация средств обработки, хранения и передачи компьютерной информации (информационной системы) включает:

- системное и техническое сопровождение аппаратного обеспечения информационной системы (в том числе модернизацию и сервисное обслуживание информационной системы);
- организацию рабочего процесса.

Доступ к информационной системе подразумевает возможность проникновения в источник информации с целью ознакомления с ней.

По нашему мнению, неправомерный доступ предполагает проникновение в источник информации без правовых оснований для такого доступа. В свою очередь, нарушение правил доступа означает несоблюдение установленных правовых предписаний лицом, которое обязано их соблюдать. В связи с этим полагаем, указанные понятия необходимо разделять.

Предметом преступления, предусмотренного ст. 274[1] УК РФ, является содержащаяся в информационных системах КИИ РФ, охраняемая законом компьютерная информация.

Критическая информационная инфраструктура представляет собой объекты критической информационной инфраструктуры[3].

[1] О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: Федеральный закон от 26.07.2017 № 194-ФЗ. СПС «КонсультантПлюс» (дата обращения: 10.10.2023).

[2] Бриллиантов А.В. Комментарий к Уголовному кодексу Российской Федерации. Т. 2. 2-е изд. Российская Академия правосудия. Москва. 2022. С. 704.

[3] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ. СПС «КонсультантПлюс» (дата обращения: 18.10.2023).

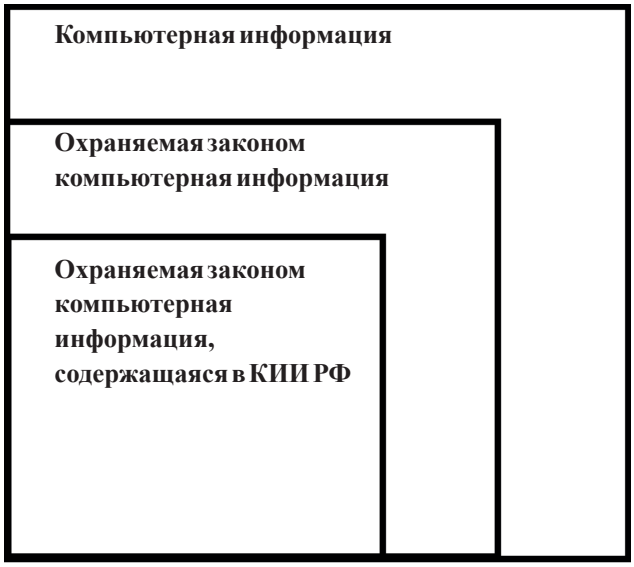

Рисунок 1. Соотношение предмета преступлений. (Данное изображение разработано автором на основе анализа научной отечественной литературы)

Объектами КИИ РФ являются ИС, ИТКС, АСУ ТП субъектов КИИ РФ[1].

Субъектами КИИ РФ признаются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или ином законном основании принадлежат ИС, ИТКС, АСУ ТП, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных объектов[2].

В свою очередь, по смыслу ч. 2 и 3 ст. 274[1] УК РФ в качестве общественно-опасных последствий определено причинение вреда КИИ РФ. Однако содержание вреда, причиняемого КИИ РФ, законодательно не закреплено, как и не определено в постановлении 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»[3].

В данном случае нельзя не согласиться с мнением И.И. Малыгина, который указывает, что «указание на причинение вреда как на обязательное общественно опасное последствие совершенного деяния, является ахиллесовой пятой уголовно-правовой нормы об ответственности за неправомерное воздействие на объекты КИИ России» [12].

Тем не менее в научных кругах предпринимаются попытки раскрыть содержание такого вреда, в частности И.И. Малыгиным. По мнению Е.А. Соловьевой, под вредом, причиняемым КИИ РФ, следует понимать любые неблагоприятные изменения в охраняемой законом КИИ РФ, которые могут выражаться как в материальном, так и нематериальном плане, виновно вызванные неправомерным воздействием и причинно связанные с ним [1].

С мнением Е.А. Соловьевой в целом можно согласиться. Действительно, в содержание вреда можно включать материальные или нематериальные неблагоприятные изменения в информационных системах КИИ РФ, однако указанное автором понятие «любые неблагоприятные последствия» довольно широкое и может включать достаточно большое количество аспектов. В связи с этим обратимся к мнению И.И. Малыгина.

Так, И.И. Малыгин применительно к ст. 274[1] УК РФ полагает, что под вредом следует понимать:

1. Нарушение функционирования объекта критической информационной инфраструктуры (в том числе функционирования сети электросвязи, используемой для организации взаимодействия таких объектов).

2. Прекращение функционирования объекта критической информационной инфраструктуры (в том числе прекращение функционирования сети электросвязи, используемой для организации взаимодействия таких объектов).

3. Нарушение безопасности обрабатываемой таким объектом информации [12].

Полагаем, третий пункт указанного мнения для выполнения цели настоящего исследования в

[1] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ. СПС «КонсультантПлюс» (дата обращения: 18.10.2023).

[2] Там же.

[3] 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. СПС «КонсультантПлюс» (дата обращения: 18.10.2023).

целом подходит, но отметим, что в данном случае И.И. Малыгин говорил именно о вреде для целей всей ст. 274[1] УК РФ, а не об отдельных ее составах.

Решетников А.Ю. полагает, что неправомерный доступ к компьютерной информации в информационной системе объектов КИИ РФ и дальнейшее манипулирование ею (копирование, уничтожение, блокирование, модифицирование) нарушает целостность этой информационной системы, в результате чего циркулирующие в системе сведения теряют объективность, достоверность и актуальность, так называемую триаду информации [13].

Указанные позиции И.И. Малыгина и А.Ю. Решетникова представляются нам заслуживающими внимания, поскольку они наиболее точно описывают признак «вред критической информационной инфраструктуре Российской Федерации».

Обратимся к материалам судебной практики и определим, какие негативные последствия суды вкладывают в содержание признака «вред».

Так, например, гражданин Р., находясь на рабочем месте, с использованием автоматизированного устройства, действуя из корыстных побуждений, используя свое служебное положение, совершил неправомерный доступ к компьютерной информации, содержащейся в КИИ РФ, повлекший ее модификацию, а именно – внесение в Единую государственную информационную систему в сфере здравоохранения недостоверных сведений о вакцинации против новой коронавирусной инфекции (COVID-19) лицам, не прошедшим процедуру вакцинации[1].

В своем решении суд отметил, что гражданин Р. указанными действиями нарушил требования ст. 23 Конституции Российской Федерации, ч. 1, ч. 2 ст. 5 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ[2], п. 7, п. 8 ст. 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ[3], Временные правила учета информации в целях предотвращения распространения новой коронавирусной инфекции (COVID-19), утвержденные постановлением Правительства Российской Федерации от 31.03.2020 № 373[4], и причинил вред объекту КИИ РФ, выраженный в потере компьютерной информации объективности, достоверности и актуальности.

Альтернативным примером может послужить приговор Курганского городского суда Курганской области от 14.03.2023 по делу № 1-143/2023, в котором указано, что гражданин С., будучи сотрудником салона сотовой связи ПАО «ВымпелКом», нарушил правила доступа к охраняемой законом компьютерной информации, содержащейся в КИИ РФ, неправомерно скопировав детализацию о сообщениях и соединениях абонентов ПАО «ВымпелКом» и передав ее за денежное вознаграждение третьим лицам[5].

При схожих обстоятельствах суды определяют содержание вреда как: нарушения состояния защищенности такой системы[6], нарушения безопасности конфиденциальности информации, содержащейся в КИИ РФ[7, 8], несоответствие сведений, содержащихся в компьютерной системе критериям оценки – объективности, достоверности, и актуальности[9], нарушение целостности и достоверности информации, циркулирующей в базе данных[10].

На основании изложенного мы пришли к выводу, что суды определяют содержание вреда КИИ РФ как нарушение состояния защищенности компьютерной информации, содержащейся в КИИ РФ.

Однако следующий приговор содержит указание и на причинение вреда КИИ РФ в виде нарушения безопасности компьютерной информации и причинения репутационного вреда субъекту КИИ РФ, который выразился в дискредитации деятельности компании по хранению и обработке информации, составляющей охраняемую законом

[1] Приговор Армянского городского суда Республики Крым от 19.10.2022 по делу № 1-89/2022.

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ. СПС «КонсультантПлюс» (дата обращения: 20.10.2023).

[3] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ. СПС «КонсультантПлюс» (дата обращения: 20.10.2023).

[4] Временные правила учета информации в целях предотвращения распространения новой коронавирусной инфекции (COVID-19), утвержденные постановлением Правительства Российской Федерации от 31.03.2020 № 373. СПС «КонсультантПлюс» (дата обращения: 20.10.2023).

[5] Приговор Курганского городского суда Курганской области от 14.03.2023 по делу № 1-143/2023.

[6] Приговор Харабалинского районного суда г. Харабали Астраханской области от 21.12.2022 по делу № 1-237/2022.

[7] Приговор Калужского районного суда Калужской области от 11.04.2022 по делу № 1-1-295/2022.

[8] Приговор Ейского городского суда Краснодарского края от 17.06.2022 по делу № 1-118/2022.

[9] Приговор Октябрьского районного суда г. Владимира от 21.11.2022 по делу № 1-351/2022.

[10] Приговор Фрунзенского районного суда г. Ярославля Ярославской области от 10.03.2023 по делу № 1-88/2023.

тайну частной жизни и тайну телефонных переговоров[1].

С выводом суда, касающегося деловой репутации, мы вынуждены не согласиться, поскольку вред деловой репутации субъекта КИИ РФ не является вредом КИИ РФ в целом.

Согласно п. 6 ст. 2 ФЗ № 187, критической информационной инфраструктурой являются объекты КИИ РФ (ИС, ИТКС, АСУ ТП), а также сети электросвязи, используемые для организации взаимодействия таких объектов[2].

Как следует из Федерального закона, субъект КИИ РФ не относится к содержанию КИИ РФ. Таким образом, по нашему мнению, вред деловой репутации, причиненный субъекту КИИ РФ, не является вредом, причиненным КИИ РФ.

На данном этапе ограничимся примерами судебной практики из сферы связи и здравоохранения и для наглядности исследования перейдем к примерам из судебной практики в банковской сфере.

Так, гражданин А., будучи сотрудником АО «Почтабанк», сформировал заявку на открытие сберегательного счета и выпуск пластиковой банковской карты на имя гражданина О. без согласия последнего, чем осуществил неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в КИИ РФ, а именно к компьютерной программе Siebel. (Данная компьютерная программа, согласно решению ФСТЭК, относится к объектам КИИ РФ)[3].

Суд определил, что своими действиями гражданин А. причинил вред КИИ РФ, выразившийся в модификации информации в указанной базе данных, внесении в нее недостоверной информации, что нарушило целостность указанной информационной системы, в результате чего информация, содержащаяся в ней, перестала соответствовать критериям оценки – объективности, достоверности и актуальности, тем самым причинив репутационный вред объекту КИИ РФ.

По нашему мнению, указанное в приговоре суда содержание признака «вред критической информационной инфраструктуре» довольно объемное и сложное, поскольку идет указание сразу на несколько критериев: нарушение целостности системы, несоответствие компьютерной информации критериям оценки, репутационный вред КИИ РФ. Но, скорее, здесь одно закономерно вытекает из другого. По сути, в данном приговоре речь идет о нарушении состояния защищенности такой информации.

Как мы упоминали ранее, в случае с приговором Хасавюртского районного суда Республики Дагестан от 01.03.2023 по делу № 1-49/2023 вред деловой репутации, или репутационный вред, не может включаться в содержание признака «вред КИИ РФ», поскольку такой вред причиняется субъекту КИИ РФ, т.е. ее законному владельцу. Мы уже отмечали, субъект КИИ РФ не относится к содержанию КИИ РФ в целом, а, следовательно, вред, причиненный субъекту КИИ РФ, не будет являться вредом, причиненным объекту КИИ РФ. Таким образом, с решением суда о репутационном вреде мы также вынуждены не согласиться.

При схожих обстоятельствах Куйбышевский районный суд г. Омска в приговоре от 31.07.2023 по делу 1-58/2023 (1-465/2022) определил, что вред объекту КИИ РФ выразился во внесении в систему недостоверных сведений, что нарушило ее целостность, а информация, в ней содержащаяся, перестала соответствовать критериям оценки – объективности, достоверности и актуальности[4].

Обсуждение и заключение

Таким образом, содержание признака «вред критической информационной инфраструктуре Российской Федерации» может выражаться в нарушении:

- безопасности конфиденциальности компьютерной информации, принадлежащей и охраняемой субъектом КИИ РФ[5, 6];

- целостности компьютерной системы КИИ РФ[7, 8, 9].

- состояния защищенности КИИ РФ[10, 11].

[1] Приговор Хасавюртского районного суда Республики Дагестан от 01.03.2023 по делу № 1-49/2023.

[2] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ. СПС «КонсультантПлюс» (дата обращения: 10.10.2023).

[3] Приговор Беловского городского суда Кемеровской области от 06.03.2023 по делу № 1-59/2023.

[4] Приговор Куйбышевского районного суда г. Омска от 31.07.2023 по делу № 1-58/2023 (1-465/2022).

[5] Приговор Армянского городского суда Республики Крым от 19.10.2022 по делу № 1-89/2022.

[6] Приговор Хасавюртского районного суда Республики Дагестан от 01.03.2023 по делу № 1-49/2023.

[7] Приговор Ейского городского суда Краснодарского края от 17.06.2023 по делу № 1-118/2022.

[8] Приговор Куйбышевского районного суда г. Омска от 31.07.2023 по делу № 1-58/2023 (1-465/2022).

[9] Приговор Фрунзенского районного суда г. Ярославля Ярославской области от 10.03.2023 по делу № 1-88/2023.

[10] Приговор Харабалинского районного суда г. Харабали, Астраханская область от 21.12.2022 по делу № 1-237/2022.

[11] Приговор Беловского городского суда Кемеровской области от 06.03.2023 по делу № 1-59/2023.

- безопасности обрабатываемой компьютерной информации[1, 2].

По существу, правоприменитель, используя вышеуказанные фразы, констатирует факт нарушения безопасности охраняемой законом компьютерной информации.

Таким образом, под вредом критической информационной инфраструктуре Российской Федерации предлагается понимать нарушение безопасности компьютерной информации, содержащейся в КИИ РФ.

Под безопасностью компьютерной информации предлагается понимать такое состояние ее защищенности, при котором ее свойства (объективность, достоверность, актуальность) устойчивы перед внешними и внутренними угрозами.

По нашему мнению, существующее постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 нуждается в уточнении содержания признака «вред критической информационной инфраструктуре».

СПИСОК ИСТОЧНИКОВ

1. Соловьева Е.А. Вред как криминообразующий признак в составах преступлений, предусмотренных частями 2 и 3 статьи 274[1] УК РФ // Пермский юридический альманах. 2023. № 6. С. 553 – 569.
2. Шахрай С.С. Система преступлений в сфере компьютерной информации: сравнительно-правовой, социолого-криминологический и уголовно-правовой аспекты: дис. … канд. юрид. наук: 12.00.08 – Уголовное право и криминология; уголовно-исполнительное право. Москва, 2010. 214 с.
3. Малыгин И.И. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: монография. 2023. 164 с.
4. Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера: дис. … канд. юрид. наук: 12.00.08 – Уголовное право и криминология; уголовно-исполнительное право. Владивосток, 2010. 214 с.
5. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. … д-ра юрид. наук: 12.00.08 – Уголовное право и криминология; уголовно-исполнительное право. Москва, 2018. 428 с.
6. Степанов-Егиняц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (Уголовно-правовой аспект): дис. … д-ра юрид. наук: 12.00.08. – Уголовное право и криминология; уголовно-исполнительное право. Москва, 2016. 389 с.
7. Яковенко И.А. Объективные признаки компьютерных преступлений как разновидности преступлений информационного характера // E–scio. 2021 № 2 (53). С. 389 – 395.
8. Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. … д-ра юрид. наук: 12.00.08 – Уголовное право и криминология; уголовно-исполнительное право. Москва, 2021. 521 с.
9. Пелевина А.В. Общая характеристика преступлений в сфере компьютерной информации // Пробелы в российском законодательстве. 2015. № 4. С. 209 – 211.
10. Дремлюга Р.И. Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. 2019. № 2. С. 130 – 139.
11. Бражник С.Д., Пилясов И.А. Технико-юридический анализ нормы о неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации (274.1 УК РФ). EDN MPSAAU // Евразийское Научное Объединение. 2019. № 8-3. С. 198 – 201.
12. Малыгин И.И. Уголовно-правовое противодействие неправомерному воздействию на критическую информационную инфраструктуру: дис. … канд. юрид. наук: 5.1.4 – Уголовно-правовые науки. Москва, 2023. 192 с.
13. Решетников А.Ю. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // ЗАКОНЫ РОССИИ: ОПЫТ, АНАЛИЗ, ПРАКТИКА. 2018. № 2. С. 51 – 55.

[1] Приговор Калужского районного суда Калужской области от 11.04.2022 по делу № 1-1-295/2022.

[2] Приговор Лыткаринского городского суда Московской области от 11.04.2023 по делу № 1-18/ 2023.

REFERENCES

1. Solov'eva E.A. Vred kak kriminoobrazuyushchij priznak v sostavah prestuplenij, predusmotrennyh chastyami 2 i 3 stat'i 2741 UK RF // Permskij yuridicheskij al'manah. 2023. № 6. S. 553 – 569.
2. SHahraj S.S. Sistema prestuplenij v sfere komp'yuternoj informacii: sravnitel'no-pravovoj, sociologo-kriminologicheskij i ugolovno-pravovoj aspekty: dis. … kand. yurid. nauk: 12.00.08 – Ugolovnoe pravo i kriminologiya; ugolovno-ispolnitel'noe pravo. Moskva, 2010. 214 s.
3. Malygin I.I. Ugolovnaya otvetstvennost' za nepravomernoe vozdejstvie na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii: monografiya. 2023. 164 s.
4. Susloparov A.V. Komp'yuternye prestupleniya kak raznovidnost' prestuplenij informacionnogo haraktera: dis. … kand. yurid. nauk: 12.00.08 – Ugolovnoe pravo i kriminologiya; ugolovno-ispolnitel'noe pravo. Vladivostok, 2010. 214 s.
5. Efremova M.A. Ugolovno-pravovaya ohrana informacionnoj bezopasnosti: dis. … d-ra yurid. nauk: 12.00.08 – Ugolovnoe pravo i kriminologiya; ugolovno-ispolnitel'noe pravo. Moskva, 2018. 428 s.
6. Stepanov-Eginyac V.G. Metodologicheskoe i zakonodatel'noe obespechenie bezopasnosti komp'yuternoj informacii v Rossijskoj Federacii (Ugolovno-pravovoj aspekt): dis. … d-ra yurid. nauk: 12.00.08. – Ugolovnoe pravo i kriminologiya; ugolovno-ispolnitel'noe pravo. Moskva, 2016. 389 s.
7. YAkovenko I.A. Ob"ektivnye priznaki komp'yuternyh prestuplenij kak raznovidnosti prestuplenij informacionnogo haraktera // E–scio. 2021 № 2 (53). S. 389 – 395.
8. Russkevich E.A. Differenciaciya otvetstvennosti za prestupleniya, sovershaemye s ispol'zovaniem informacionno-kommunikacionnyh tekhnologij, i problemy ih kvalifikacii: dis. … d-ra yurid. nauk: 12.00.08 – Ugolovnoe pravo i kriminologiya; ugolovno-ispolnitel'noe pravo. Moskva, 2021. 521 s.
9. Pelevina A.V. Obshchaya harakteristika prestuplenij v sfere komp'yuternoj informacii // Probely v rossijskom zakonodatel'stve. 2015. № 4. S. 209 – 211.
10. Dremlyuga R.I. Kriticheskaya informacionnaya infrastruktura kak predmet prestupnogo posyagatel'stva // Aziatsko-Tihookeanskij region: ekonomika, politika, pravo. 2019. № 2. S. 130 – 139.
11. Brazhnik S.D., Pilyasov I.A. Tekhniko-yuridicheskij analiz normy o nepravomernom vozdejstvii na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii (274.1 UK RF). EDN MPSAAU // Evrazijskoe Nauchnoe Ob"edinenie. 2019. № 8-3. S. 198-201.
12. Malygin I.I. Ugolovno-pravovoe protivodejstvie nepravomernomu vozdejstviyu na kriticheskuyu informacionnuyu infrastrukturu: dis. … kand. yurid. nauk: 5.1.4 – Ugolovno-pravovye nauki. Moskva, 2023. 192 s.
13. Reshetnikov A.YU. Ob ugolovnoj otvetstvennosti za nepravomernoe vozdejstvie na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii // ZAKONY ROSSII: OPYT, ANALIZ, PRAKTIKA. 2018. № 2. S. 51-55.

Информация об авторе:
Ермолаев Николай Валерьевич, адъюнкт Уральского юридического института МВД России, Nikolaiermolaev96@mail.ru, ORCID: 0000-0001-9336-4628
Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Ermolaev Nikolay V., Postgraduate of the Ural Law Institute of the Ministry of Internal Affairs of Russia, Yekaterinburg, Russia, Nikolaiermolaev96@mail.ru, ORCID: 0000-0001-9336-4628
The author has read and approved the final version of the manuscript.

Статья получена: 28.11.2023.
Статья принята к публикации: 20.03.2024.
Статья опубликована онлайн: 22.03.2024.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.