Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: терминологическая неопределённость и предложения по правовой регламентации ст. 274.1 УК РФ

Колмыков Илья Александрович
адъюнкт; Орловский юридический институт МВД РФ им. В.В. Лукьянова, Ilyakolmykov01@mail.ru

Предметом исследования настоящей статьи выступают отдельные элементы нормативного содержания ст. 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». В рамках исследования автором уделяется особое внимание анализу значения таких терминов, как «заведомо», «иная компьютерная информация», «модификация». С целью устранения терминологической неопределенности категорий "модификация" и "иная компьютерная информация" автором был проведен сравнительный анализ существующих теоретических позиций к их содержание, на основе которых был сформирован авторский подход к их сущности. Автором, рассуждается вопрос о возможном изменении редакции ч. 1 ст. 274.1 УК РФ – путем включения в ее альтернативные действия термина «модификация». Автор отмечает, что добавление термина "модификация" в диспозицию ч.1 ст. 274.1 УК РФ необходимо осуществлять с учетом комплексного определения условий, при которых действия по созданию, распространению, использованию или модификации программ признаются заведомо предназначенными для неправомерного воздействия на КИИ. По мнению автора такими условиями могут являться следующие факты: создание программ, специально предназначенных для атак на КИИ; модификация программ общего назначения для нейтрализации систем защиты объектов КИИ; использование программ, предназначенных для воздействия на инфраструктуры, использующие однотипные системы защиты.

Ключевые слова: критическая информационная инфраструктура, иная компьютерная информация, заведомость, терминологическая неопределённость, правила эксплуатации, модификация программного обеспечения, категорирование, объекты, тяжкие последствия, программное обеспечение

Введение

Современные технологии и постоянное совершенствование информационного обеспечения общества обуславливают необходимость повышения качественной защиты информации, хранящейся в различных информационных базах (системах), в том числе в системе критической информационной инфраструктуры Российской Федерации (далее — КИИ). Методология исследования и исследовательская процедура, критерии отбора научных позиций.

В качестве общенаучных применялись анализ и синтез — для раскрытия содержания признаков состава преступления ст. 274.1 УК РФ и объединения отдельных выводов в целостную систему предложений по совершенствованию нормы. Исследовательская процедура формировалась за счет авторской выборке научных позиций и научных статей по теме исследования при помощи электронных научных библиотек (eLIBRARY, КиберЛенинка и т.п). Для отбора научных позиций и научных статей приоритет отдавался работам, содержащим эмпирическую базу (анализ судебной практики, приговоров, статистики), содержащим контрверсии к другим исследователям в данной области.

Исследовательская часть.

В рамках анализа уголовного законодательства, нормативных правовых актов и специальной научной литературы нами были выявлены возможные проблемы для следственно-судебной деятельности, в числе которых:

неоднозначная практика оценки предмета преступления;

отсутствие упоминания в дефиниции статьи термина «модификация» компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации;

отсутствие законодательного определения «иной компьютерной информации» применительно к ст. 274.1 УК РФ;

Стоит начать рассмотрение указанных проблем с предмета преступления. Так, предмет преступления по ч. 1 ст. 274.1 УК РФ составляют компьютерные программы или иная компьютерная информация, заведомо предназначенные для совершения компьютерных атак на объекты КИИ (далее — ОКИИ). Анализ законодательной конструкции предмета данного деяния приводит к выводу о её неоднозначности в части трактовки терминов «заведомо» и «иная компьютерная информация».

Как справедливо отмечают Р. И. Дремлюга, С. С. Зотов и В. Ю. Павлинская, «ч. 1 ст. 274.1 УК РФ может быть неправильно квалифицирована, так как большинство вредоносных средств имеют широкий спектр применения и, скорее всего, могут применяться в том числе и против объектов критической инфраструктуры» [1]. Похожее мнение мы также можем найти в работах Е. А. Русскевича [2], М. А. Ефремовой [3], Л.И. Федосеева [4] и др.

Представители данного подхода правильно отмечают нарушение законодателем сущности признака «заведомости» программы. С данным мнением следует согласиться по следующей причине: термин «заведомо созданный» может противоречить факту создания программного обеспечения, предназначенного для широкого круга объектов, но применяемого также для неправомерного воздействия на КИИ. Мы считаем, что лица, осуществляющие противоправные деяния, крайне редко создают специализированное программное обеспечение, направленное исключительно на объекты КИИ. Современные вредоносные программы воздействуют на различные инфраструктуры и в основном функционируют на основе выявления уязвимостей, не закрытых средствами антивирусной защиты. Технологические возможности современной вредоносной программы представляют широкий инструмент для осуществления кибератаки на группу информационных объектов, ОКИИ.

Второй подход представлен группой авторов Л. Л. Кругликова, С. Д. Бражника и И. А. Пилясова, которые в своей работе кардинальным образом предлагают решить данную проблему, а именно:

«представляется целесообразным исключить из диспозиций ст. 273 и ч. 1-2 ст. 274.1 УК указание на «заведомость», чтобы избежать проблем при квалификации указанных деяний, которые с неизбежностью будут возникать у правоприменителя» [5]. Данный подход действительно может представлять интерес в рамках теоретического осмысления сущности и содержания термина «заведомо», однако применительно к практическому осмыслению разграничения информационного преступления между смежными составами преступлений, по нашему мнению, это не представляется возможным. Данное авторское предположение основано на специфике конструкции уголовно-правовых норм, закреплённых действующим уголовным законодательством (глава 28 Уголовного кодекса РФ).

Третий подход мы можем найти в работе И. И. Малыгина, который утверждает следующее: «программа и информация должны с точки зрения своего содержания и функционала обладать уникальностью действия именно в отношении объектов критической информационной инфраструктуры, и с другой стороны, эту предназначенность можно также понимать как фактическую эффективность (применимость) программы против того или иного критически важного объекта, хотя в целом «вредонос» может иметь широкий спектр действия и не обладать какой-либо внутренней спецификой» [6].

В данном подходе идёт смещение фокуса с предназначенности на применимость программы, что, по нашему мнению, является правильным подходом. С точки зрения существующей следственно-судебной практики доказать признаки «заведомо предназначенной» как самостоятельную категорию не всегда представляется возможным. Описанный И. И. Малыгиным подход не исключает уникальность программы, используемой преступниками, а напротив интерпретирует ее как фактическую эффективность (применимость). Уточнив первую обозначенную нами проблему, считаем целесообразным перейти к следующей.

Вторым спорным моментом является вопрос об использовании легального специализированного программного обеспечения, приобретённого и модифицированного для атаки на информационные ресурсы и системы. Такое программное обеспечение может изначально создаваться для проверки защищённости объектов, не относящихся к КИИ, но при последующей модификации его кода или логики работы предназначаться для неправомерного воздействия на объекты КИИ. В данном случае возникает вопрос: является ли факт модификации ПО основанием для признания программы «заведомо созданной» для атаки на КИИ?

Лица, модифицирующие специализированное ПО, по существу, не создают новую программу, а модернизируют логику уже существующей. Как отмечают А. Б. Абазов и Т. А. Файрушин, «законодатель не указывает на принципиальную разницу таких программ, но анализ накопленной судебной практики позволяет прийти к выводу о том, что преступники применяют вредоносное программное обеспечение, созданное не только с прямой целью нанести ущерб структуре КИИ, но и различные инструменты, разработанные для иных задач» [7].

Для разрешения данной проблемы рассматривается возможность дополнения действующей редакции ч. 1 ст. 274.1 УК РФ термином «модификация», изложив её в следующей редакции: «Создание, распространение и (или) использование, модификация компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации». Мы отмечаем, что данное изменение требует комплексного рассмотрения в рамках отдельных исследований, однако отметим некоторые основания для внесения предложенного изменения в анализируемую статью. В настоящее время, анализируя законодательство нашей страны, мы приходим к выводу, что легальное определение модификации компьютерной программы содержится лишь в одном нормативном правовом акте, а именно в Гражданском кодексе Российской Федерации (закреплено в подпункте 9 пункта 2 статьи 1270 Гражданского кодекса РФ). Использование данной дефиниции в настоящем исследовании носит аналогический характер: в уголовном законе легальное определение модификации отсутствует, что само по себе может подтверждать наличие законодательного пробела. Согласно вышеуказанному нормативному правовому акту, под модификацией компьютерной программы принято понимать любые её изменения, в том числе перевод такой программы или такой базы данных с одного языка на другой язык, за исключением адаптации, то есть внесения изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя.

Как справедливо отмечают Ю. В. Смирнова и А. Г. Серго: «Модификация, в свою очередь, отличается от переработки тем, что не предполагает создание новой программы, однако приводит к существенным доработкам в исходной программе для ЭВМ» [8].

При рассмотрении гражданского законодательства мы можем сделать чёткое разделение между созданием и модификацией компьютерной программы, однако в рамках уголовного законодательства это не всегда берётся во внимание. Судебное толкование применительно к статье 273 УК РФ исходит из того, что создание программы может осуществляться в том числе путём внесения изменений в уже существующие программы, однако ключевая проблема применительно к ст. 274.1 УК РФ, с нашей точки зрения, заключается в разграничении целей действия программы и объекта воздействия.

В п. 9 Постановления Пленума Верховного Суда РФ 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"» (далее — ПП ВС РФ № 37) упоминается следующее: «создание вредоносных компьютерных программ или иной вредоносной компьютерной информации представляет собой деятельность, направленную на разработку, подготовку программ (в том числе путем внесения изменений в существующие программы) или иной компьютерной информации, предназначенных для несанкционированного доступа, то есть совершаемого без согласия обладателя информации, лицом, не наделенным необходимыми для такого доступа полномочиями, либо в нарушение установленного нормативными правовыми актами порядка уничтожения, блокирования, модифицирования, копирования компьютерной информации или нейтрализации средств ее защиты». Мы отмечаем, что законодатель указывает предназначенность программы для несанкционированного доступа (ст. 273 УК РФ), а в анализируемой нами норме (ст. 274.1 УК РФ) программа либо иная компьютерная информация предназначена для неправомерного воздействия на КИИ. В рамках детального анализа дефиниций указанных статей и содержания ПП ВС РФ № 37 мы акцентируем внимание в главной степени на различие в направленности действий программ — «доступ» и «воздействие».

Сложившаяся судебная практика фактически приравнивает модификацию компьютерной программы к созданию новой программы в рамках ст. 273 УК РФ, что позволяет охватить составом данной статьи сам факт использования программы, «заведомо предназначенной для несанкционированного» уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (как правило, неопределённого типа). Ключевой признак такого рода программы — «заведомо предназначенной для несанкционированного…». Подобное расширительное толкование не влияет качественным образом на совершение действий, описанных в рамках ст. 273 УК РФ, однако применительно к ст. 274.1 УК РФ это может являться ключевым признаком при определении факта совершения уголовно-правового деяния и возможной конкуренции между анализируемыми уголовно-правовыми нормами, поскольку в ст. 274.1 УК РФ законодателем акцент делается на: «создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру» (программа модифицируется под конкретный объект КИИ, особенности его функционирования и средства защиты информации). При детальном сравнении дефиниций ст. 274.1 УК РФ и ст. 273 УК РФ становится очевидным факт разнородности объекта информационного посягательства и способа достижения данной цели (модификация, приравненная к факту создания новой программы в рамках ст. 273 УК РФ, и модификация для использования законодательного пробела — отсутствия данного термина в ст. 274.1 УК РФ — для ухода от уголовной ответственности). Вывод сделан на основе последовательного описания терминологической неопределенности «заведомо предназначенной» и отсутствием альтернативного воздействия на программу «модификации» для осуществления неправомерного воздействия на КИИ.

Следующей проблемой является отсутствие законодательного определения «иной компьютерной информации». Обращаясь к ПП ВС РФ № 37, отметим, что разъяснение данного термина дано лишь применительно к ст. 273 УК РФ: «к иной компьютерной информации отнесены ключи доступа, элементы кодов компьютерных программ, способных скрытно уничтожать и копировать информацию». Однако законодатель не даёт определения данного термина, а лишь перечисляет элементы, которые могут быть к ней отнесены. Это порождает вопросы: какие именно ключи доступа таковыми являются; на какой стадии программирования элементы кода приобретают данный статус?

Как указывает Н. В. Ермолаев, «ключи доступа представляют собой логин или код-пароль, которые, хоть и не являются компьютерной программой, но предоставляют доступ к информационной системе объектов КИИ РФ» [9].

Ф.Б. Гребенкин под иной компьютерной информацией подразумевает любую информацию со встроенными в нее вредоносными программными кодами (например, логическая бомба) [10].

Как указывает П. В. Галушин, «комбинация компьютерной информации разных типов, не являющихся программой или взаимодействующих с невредоносными программами, которые способны осуществить блокирование, модификацию, копирование компьютерной информации без согласия обладателя такой информации» [11].

Полагаем, что законодатель должен дать чёткое определение «иной компьютерной информации» и дополнительно указать, что, кроме элементов кода и ключей доступа, к ней могут относиться логины и пароли, предназначенные для активации специализированного программного обеспечения. Авторское понимание данного термина следующее: «Иная компьютерная информация» — это совокупность системных данных, определяющих параметры, логику, состояние безопасности и технологическую возможность исполнения информационного объекта, а также служащие для идентификации и подтверждения доступа (защитным элементом). К ним относятся: учётные данные, списки пользователей, конфигурационные файлы, скрипты автоматизации, ключи шифрования.

Часть 5 ст. 274.1 УК РФ устанавливает ответственность за деяния, повлёкшие тяжкие последствия. Данный признак является оценочным и не определён законодательно, что порождает неоднозначность в правоприменении. Для целей квалификации тяжкие последствия целесообразно определять через совокупность критериев:

материальный (денежный) ущерб — затраты на восстановление функционирования объекта КИИ, восстановление утраченной информации, замену оборудования, а также упущенная выгода;

нарушение доступности и непрерывности — длительность прекращения или существенного снижения качества предоставления государственных услуг, социально значимых сервисов, производственных или технологических процессов;

масштаб последствий — количество затронутых пользователей, территориальный охват, количество нарушенных информационных процессов или систем;

угроза жизни и здоровью — создание реальной опасности для людей в результате нарушения работы автоматизированных систем управления (например, на объектах энергетики, транспорта, химической промышленности).

Отмечаем необходимость проведения дополнительного исследования по определению размера материального ущерба для следующих категорий: значительный размер ущерба, крупный размер ущерба или особо крупный ущерб. Данные категории должны быть выражены в денежном эквиваленте. Однако материальный критерий не должен быть единственным: при отсутствии значительного ущерба, но при наличии существенного нарушения функционирования социально значимых сервисов или угрозы жизни и здоровью последствия также могут быть признаны тяжкими. Отмечаем, что предложенная система критериев носит рекомендательный характер и требует дальнейшей эмпирической верификации

Заключение

Таким образом, проведённый нами анализ позволяет сделать следующие выводы. Термин «заведомо» в ч. 1 ст. 274.1 УК РФ нуждается в уточнении. Предлагаем рассмотреть возможность дополнить диспозицию термином «модификация» и определить условия, при которых действия по созданию, распространению, использованию или модификации программ признаются заведомо предназначенными для неправомерного воздействия на КИИ: создание программ, специально предназначенных для атак на КИИ; модификация программ общего назначения для нейтрализации систем защиты объектов КИИ; использование программ, предназначенных для воздействия на инфраструктуры, использующие однотипные системы защиты. Необходимо законодательное определение «иной компьютерной информации» для ст. 274.1 УК РФ с указанием, что к ней относятся ключи доступа, элементы кода, логины и пароли, предназначенные для активации или нейтрализации средств защиты объектов КИИ. Для единообразной квалификации по ч. 5 ст. 274.1 УК РФ необходимо закрепить совокупность критериев тяжких последствий: материальный ущерб, нарушение доступности и непрерывности, масштаб воздействия, угроза жизни и здоровью. Перспективой дальнейшего исследования видится разработка критериев дифференциации тяжких последствий по размеру материального ущерба, а также детальное обоснование включения термина «модификация» в диспозицию ч. 1 ст. 274.1 УК РФ.

Литература

1. Дремлюга, Р. И. Критическая информационная инфраструктура как предмет преступного посягательства / Р. И. Дремлюга, С. С. Зотов, В. Ю. Павлинская // Азиатско-тихоокеанский регион: экономика, политика, право. – 2019. – Т. 21, № 2. – С. 130-139. – DOI 10.24866/1813-3274/2019-2/130-139. – EDN MMQOOR.

2. Уголовное право и «цифровая преступность»: проблемы и решения: монография / Е. А. Русскевич. — 2-е изд., перераб. и доп. — Москва: ИНФРА-М, 2023. — 351 с. — (Научная мысль). — DOI: 10.12737/1840963

3. Ефремова М. А. Уголовно-правовая охрана информационной безопасности: монография / М. А. Ефремова. — Москва: Юрлитинформ, 2018. — 306 с. — (Уголовное право). — ISBN 978-5-4396-1540-7.

4. Федосеев, Л. И. Анализ отдельных положений статьи 274.1 Уголовного кодекса Российской Федерации / Л. И. Федосеев // Законность и правопорядок: история, современность, актуальные проблемы : Материалы IV межвузовской студенческой научной конференции, Москва, 03 декабря 2019 года / Под общей редакцией С.В. Ширяевой. – Москва: Московский педагогический государственный университет, 2020. – С. 190-194. – EDN TSEZUV.

5. Кругликов Л. Л., Бражник С. Д., Пилясов И. А. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ): некоторые проблемы определения признаков состава преступления // Журнал юридических исследований. 2019. № 3. С. 53-62. URL: https://naukaru.ru/ru/nauka/publications/article/6a9c146832807fdbab85e18d/nepravomernoe-vozdeystvie-na-kriticheskuyu-informacionnuyu-infrastrukturu-rossiyskoy-federacii-st-274-1-uk-rf-nekotorye-problemy-opredeleniya-priznakov-sostava-prestupleniya/view. (дата обращения: 26.10.2026).

6. Малыгин, И. И. Актуальные проблемы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации / И. И. Малыгин // Известия Юго-Западного государственного университета. Серия: История и право. – 2023. – Т. 13, № 2. – С. 165-176. – DOI 10.21869/2223-1501-2023-13-2-165-176. – EDN XUTRYN.

7. Абазов, А. Б. К вопросу об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 ук РФ) / А. Б. Абазов, Т. А. Файрушин // Вестник Уфимского юридического института МВД России. – 2023. – № 4(102). – С. 86-92. – EDN DOZCTD.

8. Смирнова Ю.В., Серго А.Г. Свободное ПО в реестре российских программ // Интеллектуальная собственность. Авторское право и смежные права. 2020. № 1. С. 5-20. EDN: WVOHDB.

9. Ермолаев, Н. В. К вопросу о содержании термина «иная компьютерная информация» для целей статьи 274.1 Уголовного кодекса Российской Федерации / Н. В. Ермолаев // Вестник Уральского юридического института МВД России. – 2024. – № 1(41). – С. 146-150. – EDN DUJLYY.

10. Гребенкин, Ф.Б. Некоторые проблемные вопросы объективных признаков состава преступления, предусмотренного ст. 273 УК РФ / Ф.Б. Гребенкин, Л.А. Коврижных // Вестник гуманитарного образования. – 2017 – № 2 – С. 71-77.

11. Галушин, П. В. Иная вредоносная компьютерная информациякак предмет преступления, предусмотренного статьей 273

УК РФ / П. В. Галушин, Е. А. Лапина // Научный компонент. – 2020. – № 1(5). – С. 61-67. – DOI 10.51980/2686-939X_2020_1_61. – EDN VWXZIN.

Unlawful Interference with the Critical Information Infrastructure of the Russian Federation: Terminological Ambiguity and Proposals for the Legal Regulation of Article 274.1 of the Criminal Code of the Russian Federation

Kolmikov I.A.

Oryol Law Institute of the Ministry of Internal Affairs of the Russian Federation named after V.V. Lukyanov

The subject of this article is certain elements of the normative content of Article 274.1 of the Criminal Code of the Russian Federation, “Unlawful Impact on the Critical Information Infrastructure of the Russian Federation.” Within the framework of the study, the author pays special attention to analyzing the meaning of such terms as “knowingly,” “other computer information,” and “modification.” In order to eliminate the terminological ambiguity surrounding the categories of “modification” and “other computer information,” the author conducted a comparative analysis of the existing theoretical positions regarding their content, on the basis of which the author developed their own approach to their essence. The author discusses the issue of a possible amendment to Part 1 of Article 274.1 of the Criminal Code of the Russian Federation – by including the term “modification” in its alternative actions. The author notes that the addition of the term “modification” to the disposition of Part 1 of Article 274.1 of the Criminal Code of the Russian Federation should be carried out taking into account a comprehensive definition of the conditions under which actions involving the creation, distribution, use, or modification of programs are deemed to be knowingly intended for unlawful impact on critical information infrastructure. According to the author, such conditions may include the following facts: the creation of programs specifically designed to attack CII; modification of general-purpose programs to neutralize CII protection systems; the use of programs designed to affect infrastructures using the same type of protection systems.

Keywords: critical information infrastructure, other computer information, knowledge, terminological uncertainty, operating rules, software modification, categorization, objects, grave consequences, software.

References

1. Dremlyuga, R. I., Zotov, S. S., & Pavlinskaya, V. Yu. (2019). Critical Information Infrastructure as an Object of Criminal Encroachment. *Pacific Rim: Economics, Politics, Law*, 21(2), 130–139. DOI: 10.24866/1813-3274/2019-2/130-139. EDN: MMQOOR.
2. Russkevich, E. A. (2023). *Criminal Law and "Digital Crime": Problems and Solutions* (2nd ed., rev. and exp.). Moscow: INFRA-M. 351 p. (Scientific Thought). DOI: 10.12737/1840963
3. Efremova, M. A. (2018). *Criminal Law Protection of Information Security*. Moscow: Yurlitinform. 306 p. (Criminal Law). ISBN 978-5-4396-1540-7.
4. Fedoseev, L. I. (2019). Analysis of Certain Provisions of Article 274.1 of the Criminal Code of the Russian Federation. In S. V. Shiryaeva (Ed.), *Legality and Law and Order: History, Modernity, and Current Issues: Proceedings of the IV Interuniversity Student Scientific Conference* (Moscow, December 3, 2019). – Moscow: Moscow Pedagogical State University, 2020. – pp. 190–194. – EDN TSEZUV.
5. Kruglikov L. L., Brazhnik S. D., Pilyasov I. A. Unlawful Interference with the Critical Information Infrastructure of the Russian Federation (Article 274.1 of the Criminal Code of the Russian Federation): Some Issues in Defining the Elements of the Offense // Journal of Legal Research. 2019. No. 3. pp. 53–62. URL: https://naukaru.ru/ru/nauka/publications/article/6a9c146832807fdbab85e18d/nepravomernoe-vozdeystvie-na-kriticheskuyu-informacionnuyu-infrastrukturu-rossiyskoy-federacii-st-274-1-uk-rf-nekotorye-problemy-opredeleniya-priznakov-sostava-prestupleniya/view. (accessed: 26.10.2026).
6. Malygin, I. I. Current Issues in the Legal Classification of Unlawful Interference with the Critical Information Infrastructure of the Russian Federation / I. I. Malygin // Proceedings of the Southwest State University. Series: History and Law. – 2023. – Vol. 13, No. 2. – pp. 165–176. – DOI 10.21869/2223-1501-2023-13-2-165-176. – EDN XUTRYN. 7. Abazov, A. B., & Fairushin, T. A. (2023). On the Issue of Criminal Liability for Unlawful Interference with the Critical Information Infrastructure of the Russian Federation (Article 274.1 of the Criminal Code of the Russian Federation). *Bulletin of the Ufa Law Institute of the Ministry of Internal Affairs of Russia*, (4(102)), 86–92. EDN: DOZCTD.
8. Smirnova, Yu. V., & Sergo, A. G. (2020). Free Software in the Registry of Russian Programs. *Intellectual Property. Copyright and Related Rights*, (1), 5–20. EDN: WVOHDB.
9. Ermolaev, N. V. (2024). On the Content of the Term "Other Computer Information" for the Purposes of Article 274.1 of the Criminal Code of the Russian Federation. *Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia*, (1(41)), 146–150. EDN: DUJLYY.
10. Grebenkin, F. B., & Kovrizhnykh, L. A. (2017). Some Problematic Issues Regarding the Objective Elements of the Offense Provided for by Article 273 of the Criminal Code of the Russian Federation. *Bulletin of Humanitarian Education*, (2), 71–77.
11. Galushin, P. V., & Lapina, E. A. (2020). "Other Malicious Computer Information" as the Subject of the Offense Provided for by Article 273 of the Criminal Code of the Russian Federation. *Scientific Component*, (1(5)). – pp. 61-67. – DOI 10.51980/2686-939X_2020_1_61. – EDN VWXZIN.