УГОЛОВНО-ПРАВОВЫЕ НАУКИ / CRIMINAL LAW SCIENCES

DOI: https://doi.org/10.60797/IRJ.2024.148.32

ПОНЯТИЕ И ХАРАКТЕРИСТИКИ КИБЕРПРОСТРАНСТВА

Научная статья

Смушкин А.Б.[1, *]
[1] ORCID : 0000-0003-1619-8325;
[1] Саратовская государственная юридическая академия, Саратов, Российская Федерация

* Корреспондирующий автор (skif32[at]yandex.ru)

Аннотация

Статья посвящена разработке вопросов понятия и характеристик киберпространства, являющегося одним из основных объектов изучения цифровой криминалистики. Анализируя основные подходы к наименованию данного цифрового пространства в научных исследованиях, законодательстве и судебной практике, констатируется, что оптимальным наименованием является именно категория «Киберпространство» В криминалистических целях возможно также конкретизация наименования: инцидентное киберпространство, как кибернетическое пространство отражения виртуальных следов преступления или иного инцидента. Рассматривая основные характеристики киберпространства, автор развивает мысль о трехмерности киберпространства в идею о его многомерности, подчеркивая, что уже сейчас необходимо использование нового измерения – «время». Автор анализирует использование данного измерения в идентификационных, аутентификационных, верификационных криминалистических целях.

Ключевые слова: криминалистическое исследование киберпространства, инцидентное кибернетическое пространство, цифровая криминалистика, цифровой отпечаток компьютерного устройства, элементы киберпространства.

CONCEPT AND CHARACTERISTICS OF CYBERSPACE

Research article

Smushkin A.B.[1, *]
[1] ORCID : 0000-0003-1619-8325;
[1] Saratov State Law Academy, Saratov, Russian Federation

* Corresponding author (skif32[at]yandex.ru)

Abstract

The article is dedicated to the development of the concept and characteristics of cyberspace, which is one of the main objects of study of digital forensics. Analysing the main approaches to the name of this digital space in scientific research, legislation and judicial practice, it is stated that the optimal name is the category "Cyberspace". For forensic purposes, it is also possible to specify the name: incident cyberspace as a cybernetic space of reflection of virtual traces of a crime or other incident. Examining the main characteristics of cyberspace, the author develops the idea of three-dimensional cyberspace into the idea of its multidimensionality, emphasizing that it is already necessary to use a new dimension – "time". The author analyses the use of this dimension for identification, authentication, verification and forensic purposes.

Keywords: forensic cyberspace investigation, incident cyberspace, digital forensics, digital footprint of a computer device, elements of cyberspace.

Введение

Концепция киберпространства, как особого пространства компьютеров и связей между ними впервые прозвучала в фантастической новелле «Сожжение Хром» («Burning Chrome», 1982 г) Уильяма Гибсона (на русском языке сборник рассказов вышел в 1997 г. [1]) и вскоре после этого, завоевала свое место и в научном мире. Несмотря на прошедшие с этого времени более 40 лет, относительно сущности и характеристик киберпространства между учеными согласия достигнуто не было. Отсутствует консенсус даже по поводу самого термина, характеризующего данное компьютерное пространство. Между тем данный, ранее чисто компьютерный, концепт, приобретает особое значение и для криминалистических исследований компьютерной информации, ведь только редкое преступление (даже традиционное, не компьютерное) и редкий преступник нее оставляет сейчас виртуальные следы в киберпространстве. Указанные обстоятельства требуют четкого понимания категории «Киберпространство» и ее основных характеристик для криминалистических исследований.

Статья основана на использовании материалистической диалектики как всеобщего метода, а также общенаучных методов, таких как методы анализа, синтеза, моделирования, экстраполяции и другие.

Обсуждение

В настоящее время предлагаются несколько основных подходов к рассматриваемому концепту. Не оспаривая основную сущность и содержание данного пространства, ряд авторов именует его «виртуальным» [2], [3], [4], [5], указывая что «это среда, в которой возникают, изменяются и прекращаются информационные отношения на основе комплекса средств, позволяющих обеспечить непрерывное протекание информационных процессов» [6, С. 176]. К подобному наименованию склоняется и судебная практика [7], [8], [9], [10]. Нам же представляется, что данный

оборот может быть смешан с категорией «пространство виртуальной реальности», что явно является различными концепциями. Ряд авторов применяет категорию информационная сфера (информационное пространство) [11]. Законодатель также чаще использует оборот «Информационное пространство» [12]. Между тем данная характеристика скрывает компьютерную, кибернетическую сущность пространства, да и просто может быть воспринято как пространство информации не только в цифровой, но и в аналоговой форме.

Нам представляется оптимальной характеристикой данного явления категория киберпространство (или кибернетическое пространство), как отражающее сущность и основу концепта. Модельный закон «О противодействии киберпреступности» определяет киберпространство как цифровую среду, возникающую в результате взаимодействия людей, программного обеспечения и сервисов в информационно-телекоммуникационных сетях, включая сеть «Интернет», посредством связанных с ними технологических устройств и сетей, не существующую в физической форме» [13]. Однако Модельный закон не является в полной мере национальным законодательством и требует еще имплементации в отечественные нормы права. В криминалистических целях возможно также конкретизация наименования: инцидентное киберпространство, как кибернетическое пространство отражения виртуальных следов преступления или иного инцидента.

И. Дзялошинский, аккумулировав основные мнения указал, что существует 3 основных подхода к трактовке киберпространства: «Первый подход связан с рассмотрением киберпространства как обычного пространства, у которого есть два основных свойства: быть местом размещения чего-либо и иметь границы. Второй подход определяет киберпространство как пространство определенных информационных взаимодействий. При таком подходе понятие «киберпространство» используется как синоним понятия «информационное пространство»; «информационное поле» и т.д. В рамках третьего подхода киберпространство рассматривается как совокупность определенных социальных структур (индивидов, их групп и организаций), соединенных информационными отношениями, то есть отношениями сбора, производства, распространения и потребления информации с помощью глобальных компьютерных сетей» [14]. Киберпространство является сложным и многоаспектным явлением, рассмотрение которого возможно с философской, социологической, политической, экономической, психологической и иных точек зрения.

С криминалистических позиций, один из первых, киберпространство рассматривал в своей докторской диссертации В.А. Мещеряков [15, С. 45]. При этом в последних работах он указывает, что как динамическую среду присутствия человека, состоящую из следующих элементов:

1) информационно-техническая инфраструктура компьютерных систем и их сетей;

2) система информационных цифровых объектов созданных и функционирующих в этой инфраструктуре;

3) системы акторов (пользователей и созданных ими компьютерных программ), использующих информационно-цифровые объекты в инфраструктуре компьютерных сетей для решения целевых задач;

4) установленных правил (протоколов) сетевого взаимодействия всех указанных выше элементов [16, С. 33].

Среди криминалистически значимых черт киберпространства можно отметить следующие: трансграничность, требующая для расследования налаженного межгосударственнгого взаимодействия; собственная архитектоника, требующая разработки иных средств и методов исследования, по сравнению со следами материального мира; быстрое или даже сверхбыстрое изменение информации; возможность одновременной работы с информацией нескольких пользователей в дистанционном режиме, в том числе без сохранения информации на своем устройстве; большое количество состояний информации (например – распределенная форма информации); использование уникальных программных орудий преступления; использование криптографических и стеганографических методов защиты информации.

Как и реальное пространство киберпространство обладает рядом измерений. Авторы монографии «Высокотехнологичный уголовный процесс» говорят об особом строении, трехмерность киберпространства [17, С. 38]. Аналогичную позицию занимает и Д.А. Степаненко, указывая на «трёхмерность, иерархию системных доменов, разделение пространства на структурные зоны» [18, С. 78]. При этом условно мерилом расстояния в кибергеографии будет либо время соединения между компьютерными устройствами, либо количество переходов по гиперссылкам [19], [20]. Многоуровневость, объемность киберпространства обеспечивают гиперссылки. Некоторые ученые подчеркивают, что киберпространство характеризуется отсутствием центрального стержневого корня и состоит из множества хаотически переплетающихся, периодически отмирающих и регенерирующих, непредсказуемых в своем развитии побегов [21, С. 11], [22, С. 118].

Кроме того, сам Интернет, как глобальная сеть, состоит из трех слоев: «большой» интернет (основной, открытый, clear net, clear web), глубокий интернет (deep net- часть интернета, не индексируемая поисковыми системами) и темный интернет, dark net (часть интернета, с повышенной анонимизацией не видимая и недоступная без специальных программных средств).

Однако нам представляется, что относительно киберпространства можно говорить даже не о трёхмерности, а о многомерности пространства, поскольку, как минимум, еще одним дополнительным элементом, дополнительным измерением здесь будет являться время.

Во многих случаях именно от временного фактора зависит основание привлечения к уголовной ответственности, верификация доказательств, идентификация и аутентификация пользователей, а также цифровых отпечатков компьютерного оборудования и цифровых поведенческих отпечатков (включающих такие параметры как время выполнения операций по обработке звука операционной системы или звуковой карты устройства, время отрисовки фигуры по запросу, временные факторы взаимодействия с сенсорным экраном или мышью, динамики движений или конкретно нажатия клавиш и т.д.). Элементы дорожки электронно-цифровых следов в киберпространстве также учитываются с точки зрения хронологии их возникновения.

В некоторых случаях, чувствительность к времени отклика мешает полномасштабному функционированию цифровых систем – например, системы жизнеобеспечения или системы управления высокотехнологичными,

дистанционно пилотируемыми или автопилотируемыми транспортными средствами. Для нивелирования временных факторов в цифровых системах разрабатываются даже целые новые концепции, например, концепция уже не облачных, а туманных вычислений, в которых модель состоит из туманных узлов, являющихся «посредниками» между конечными устройствами пользователя и облачными сервисами. Туманные вычисления, по сравнению с облачными являются более близким к пользователю уровнем сбора и анализа данных с низкой задержкой и лучшей взаимосвязью с устройством пользователя.

С развитием систем виртуальной реальности и, в перспективе, появления устройств полного погружения, можно будет уже поднимать вопрос о N- мерности киберпространства, где, в качестве значения N, могут появиться и другие показатели.

Заключение

Таким образом, проведенное исследование позволяет сделать следующие выводы:

1. Можно констатировать, что основной категорией, характеризующей рассматриваемое цифровое пространство, является именно «киберпространство», а в криминалистических целях также «Инцидентное киберпространство».

2. Среди проблем правового регулирования можно отметить отсутствие трактовки термина «Киберпространство» в национальном законодательстве. Модельный закон, в котором содержится достаточно удачная трактовка данной категории требует еще имплементации в отечественные нормы права. Подобная регламентация может быть проведена в рамках разрабатываемого многими коллективами «Цифрового кодекса». При этом в рассматриваемые в перспективе нормы должны быть внесены и основные, значимые свойства и признаки киберпространства.

3. Киберпространство характеризуется не трехмерностью, как подчёркивают многие авторы, а многомерностью, где, даже на настоящий момент, можно говорить о «времени» как отдельном измерении, используемом в идентификационных, аутентификационных и верификационных целях в автоматизированных системах, а также в рамках судопроизводства.

4. Именно указанные выше подходы будут способствовать обеспечению оптимизации защиты безопасности киберпространства.

Финансирование

Исследование выполнено за счет гранта Российского научного фонда № № 24-28-00312, https://rscf.ru/project/24-28-00312/.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Funding

The research was carried out at the expense of a grant from the Russian Science Foundation No. 24-28-00312, https://rscf.ru/project/24-28-00312/.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Гибсон У. Нейромант. Сожжение хром : Фантастический роман и рассказы / У. Гибсон. — Москва : ТКО АСТ, 1997. — 576 с.

2. Рассолов И.М. Право и Интернет. Теоретические проблемы / И.М. Рассолов. — Москва : Норма, 2009. — 383 с.

3. Ищенко Е.П. О некоторых подходах к выявлению и расследованию преступлений, совершаемых в виртуальном пространстве / Е.П. Ищенко // Использование современных информационных технологий в правоохранительной деятельности и региональные проблемы информационной безопасности. — Калининград, 2006. — С. 214–226.

4. Яковлев А.Н. Цифровая криминалистика и её значение для расследования преступлений в современном информационном обществе / А.Н. Яковлев // Совершенствование следственной деятельности в условиях информатизации. — Минск : Редакция журнала «Промышленно-торговое право», 2018. — С. 357–362.

5. Овчинникова О.В. Особенности расследования сбыта наркотических средств, совершенных с использованием сети Интернет / О.В. Овчинникова // Правопорядок: история, теория, практика. — 2018. — № 1(16). — С. 94–98.

6. Переверзева Е.С. Виртуальные и цифровые следы: новый подход в понимании / Е.С. Переверзева, А.В. Комов // Вестник Санкт-Петербургского университета МВД России. — 2021. — № 1(89). — С. 172–178.

7. Приговор по делу № 1-397/2019 от 29 ноября 2019 г. Октябрьско-го районного суда г. Липецка // Архив Октябрьского районного суда г. Липецка. — URL: https://sudact.ru/regular/doc/BmFc1yAdgeJT/?ysclid=m16dqmsyus341442370 (дата обращения: 15.07.2024).

8. Решение по делу № 2А-225/2019 от 2 апреля 2019 г. Арского районного суда Республики Татарстан // Архив Арского районного суда Республики Татарстан. — URL: https://actofact.ru/case-16OS0000-33-7097-2019-2019-04-02-0-1/?ysclid=m16dzgmteq116487773 (дата обращения: 15.07.2024).

9. Приговор Октябрьского районного суда г. Ростова-на-Дону по делу № 1-332/2017 от 29 сентября 2017 г. // Архив Октябрьского районного суда г. Ростова-на-Дону. — URL: https://sudact.ru/regular/court/reshenya-oktiabrskii-raionnyi-sud-g-rostova-na-donu-rostovskaia-oblast/?ysclid=m16e0wcnrk344396896 (дата обращения: 15.07.2024).

10. Приговор Выксунского городского суда Нижегородской области по делу № 1-117/2016 1-7/2017 от 8 августа 2017 // Архив Выксунского городского суда Нижегородской области. — URL: https://actofact.ru/case-52RS0013-1-7-2017-1-117-2016-2016-04-01-2-0/?ysclid=m16ekd8bvy286186155 (дата обращения: 15.07.2024).

11. Яковец Е.Н. Правовые основы обеспечения информационной безопасности Российской Федерации : учеб. пособие / Е.Н. Яковец. — М. : Юрлитинформ, 2014. — 406 с.

12. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы УТВ // Указ Президента Российской Федерации от 09.05.2017 г. № 203. — URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 15.07.2024).

13. Модельный закон о противодействии киберпреступности» (Принят 14.04.2023 в г. Санкт-Петербурге Постановлением 55-20 на 55-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) // Информационный бюллетень. — 2023. — № 78.

14. Дзялошинский И.М. Особенности коммуникативного поведения в киберпространстве / И.М. Дзялошинский. — URL: https://dzyalosh.ru/02-01-Auditoriya-Media/Kiberprostranstvo.pdf (дата обращения: 15.07.2024).

15. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации : дисс. ... д.ю.н. / В.А. Мещеряков. — Воронеж, 2001. — 387 с.

16. Мещеряков В.А. Теоретические основы механизма следообразования в цифровой криминалистике : монография / В.А. Мещеряков. — Москва : Проспект, 2022. — 176 с.

17. Высокотехнологичный уголовный процесс : монография / под ред. С.В. Зуева, Л.Н. Масленниковой. — М. : Юрлитинформ, 2023. — 216 с.

18. Степаненко Д.А. Киберпространство как модулятор процесса расследования преступлений и развития криминалистической науки / Д.А. Степаненко // Сибирские уголовно-процессуальные и криминалистические чтения. — 2020. — № 1(27). — С. 77–78.

19. Романенко М.А. Следственный осмотр по делам о преступных нарушениях авторских прав в сфере программного обеспечения / М.А. Романенко // Вестник Омского университета. Серия: Право. — 2008. — № 1. — С. 171–175.

20. Хуторной С.Н. Киберпространство и реальный мир / С.Н. Хуторной // Вестник Московского государственного областного университета. Серия: Философские науки. — 2011. — № 2. — С. 67–71.

21. Делез Ж. Тысяча плато: Капитализм и шизофрения / Ж. Делез, Ф. Гваттари. — Екатеринбург : У-Фактория, 2010. — 892 с.

22. Сороковикова В.И. Постмодернизм: эстетический, культурологический и философский аспекты изучения / В.И. Сороковикова // Актуальные проблемы гуманитарных и естественных наук. — 2010. — № 1. — С.114–119.

Список литературы на английском языке / References in English

1. Gibson W. Nejromant. Sozhzhenie hrom : Fantasticheskij roman i rasskazy [A neuromancer. Burning Chrome : A Fantastic Novel and short Stories] / W. Gibson. — Moscow : TKO AST, 1997. — 576 p. [in Russian]

2. Rassolov I.M. Pravo i Internet. Teoreticheskie problemy [Law and the Internet. Theoretical problems] / I.M. Rassolov. — Moscow : Norma, 2009. — 383 p. [in Russian]

3. Ishchenko E.P. O nekotoryh podhodah k vyjavleniju i rassledovaniju prestuplenij, sovershaemyh v virtual'nom prostranstve [On some approaches to the identification and investigation of crimes committed in the virtual space] / E.P. Ishchenko // Ispol'zovanie sovremennyh informacionnyh tehnologij v pravoohranitel'noj dejatel'nosti i regional'nye problemy informacionnoj bezopasnosti [The use of modern information technologies in law enforcement and regional problems of information security]. — Kaliningrad, 2006. — P. 214–226. [in Russian]

4. Yakovlev A.N. Cifrovaja kriminalistika i ejo znachenie dlja rassledovanija prestuplenij v sovremennom informacionnom obshhestve [Digital criminalistics and its importance for the investigation of crimes in the modern information society] / A.N. Yakovlev // Sovershenstvovanie sledstvennoj dejatel'nosti v uslovijah informatizacii [Improving investigative activities in the context of informatization]. — Minsk : Editorial office of the journal "Industrial and Commercial Law", 2018. — P. 357–362. [in Russian]

5. Ovchinnikova O.V. Osobennosti rassledovanija sbyta narkoticheskih sredstv, sovershennyh s ispol'zovaniem seti Internet [Features of the investigation of the sale of narcotic drugs committed using the Internet] / O.V. Ovchinnikova // Pravoporjadok: istorija, teorija, praktika [Law and order: history, theory, practice]. — 2018. — № 1(16). — P. 94–98. [in Russian]

6. Pereverzeva E.S. Virtual'nye i cifrovye sledy: novyj podhod v ponimanii [Virtual and digital traces: a new approach in understanding] / E.S. Pereverzeva, A.V. Komov // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii [Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia]. — 2021. — № 1(89). — P. 172–178. [in Russian]

7. Prigovor po delu № 1-397/2019 ot 29 nojabrja 2019 g. Oktjabr'sko-go rajonnogo suda g. Lipecka [Verdict in case No. 1-397/2019 dated November 29, 2019 Oktyabrsky district court of Lipetsk] // Arhiv Oktjabr'skogo rajonnogo suda g. Lipecka [Archive of the Oktyabrsky district Court of Lipetsk]. — URL: https://sudact.ru/regular/doc/BmFc1yAdgeJT/?ysclid=m16dqmsyus341442370 (accessed: 15.07.2024). [in Russian]

8. Reshenie po delu № 2A-225/2019 ot 2 aprelja 2019 g. Arskogo rajonnogo suda Respubliki Tatarstan [Decision on case No. 2A-225/2019 dated April 2, 2019 of the Arsky District Court of the Republic of Tatarstan] // Arhiv Arskogo rajonnogo suda Respubliki Tatarstan [Archive of the Arsky District Court of the Republic of Tatarstan]. — URL: https://actofact.ru/case-16OS0000-33-7097-2019-2019-04-02-0-1/?ysclid=m16dzgmteq116487773 (accessed: 15.07.2024). [in Russian]

9. Prigovor Oktjabr'skogo rajonnogo suda g. Rostova-na-Donu po delu № 1-332/2017 ot 29 sentjabrja 2017 g. [The verdict of Rostov-on-Don Rostov-on-Don District Court in case No. 1-332/2017 dated September 29, 2017] // Arhiv Oktjabr'skogo rajonnogo suda g. Rostova-na-Donu [Archive of the Oktyabrsky District Court of Rostov-on-Don]. — URL: https://sudact.ru/regular/court/reshenya-oktiabrskii-raionnyi-sud-g-rostova-na-donu-rostovskaia-oblast/?ysclid=m16e0wcnrk344396896 (accessed: 15.07.2024). [in Russian]

10. Prigovor Vyksunskogo gorodskogo suda Nizhegorodskoj oblasti po delu № 1-117/2016 1-7/2017 ot 8 avgusta 2017 [The verdict of the Vyksa City Court of the Nizhny Novgorod region in case no. 1-117/2016 1-7/2017 from August 8, 2017] // Arhiv Vyksunskogo gorodskogo suda Nizhegorodskoj oblasti [Archive of the Vyksa City Court of the Nizhny Novgorod region]. — URL: https://actofact.ru/case-52RS0013-1-7-2017-1-117-2016-2016-04-01-2-0/?ysclid=m16ekd8bvy286186155 (accessed: 15.07.2024). [in Russian]

11. Yakovets E.N. Pravovye osnovy obespechenija informacionnoj bezopasnosti Rossijskoj Federacii [Legal bases of information security of the Russian Federation] : textbook. the manual / E.N. Yakovets. — M. : Yurlitinform, 2014. — 406 p. [in Russian]

12. Strategija razvitija informacionnogo obshhestva v Rossijskoj Federacii na 2017–2030 gody UTV [The Strategy for the development of the Information society in the Russian Federation for 2017-2030 APPROVED] // Ukaz Prezidenta Rossijskoj Federacii ot 09.05.2017 g. № 203 [Decree of the President of the Russian Federation dated 09.05.2017 No. 203]. — URL: http://www.kremlin.ru/acts/bank/41919 (accessed: 15.07.2024). [in Russian]

13. Model'nyj zakon o protivodejstvii kiberprestupnosti» (Prinjat 14.04.2023 v g. Sankt-Peterburge Postanovleniem 55-20 na 55-om plenarnom zasedanii Mezhparlamentskoj Assamblei gosudarstv-uchastnikov SNG) [The Model Law on Countering Cybercrime" (Adopted on 04/14/2023 in St. Petersburg by Resolution 55-20 at the 55th plenary meeting of the Interparliamentary Assembly of the CIS Member States)] // Informacionnyj bjulleten' [Newsletter]. — 2023. — № 78. [in Russian]

14. Dzyaloshinsky I.M. Osobennosti kommunikativnogo povedenija v kiberprostranstve [Features of communicative behavior in cyberspace] / I.M. Dzyaloshinsky. — URL: https://dzyalosh.ru/02-01-Auditoriya-Media/Kiberprostranstvo.pdf (accessed: 15.07.2024). [in Russian]

15. Meshcheryakov V.A. Osnovy metodiki rassledovanija prestuplenij v sfere komp'juternoj informacii [Fundamentals of the methodology for investigating crimes in the field of computer information] : dis. ... Doctor of Law / V.A. Meshcheryakov. — Voronezh, 2001. — 387 p. [in Russian]

16. Meshcheryakov V.A. Teoreticheskie osnovy mehanizma sledoobrazovanija v cifrovoj kriminalistike [Theoretical foundations of the mechanism of trace formation in digital criminology] : monograph / V.A. Meshcheryakov. — Moscow : Prospekt, 2022. — 176 p. [in Russian]

17. Vysokotehnologichnyj ugolovnyj process [Hightech criminal process] : monograph / edited by S.V. Zuev, L.N. Maslennikova. — M. : Yurlitinform, 2023. — 216 p. [in Russian]

18. Stepanenko D.A. Kiberprostranstvo kak moduljator processa rassledovanija prestuplenij i razvitija kriminalisticheskoj nauki [Cyberspace as a modulator of the crime investigation process and the development of criminalistic science] / D.A. Stepanenko // Sibirskie ugolovno-processual'nye i kriminalisticheskie chtenija [Siberian Criminal Procedural and criminalistic readings]. — 2020. — № 1(27). — P. 77–78. [in Russian]

19. Romanenko M.A. Sledstvennyj osmotr po delam o prestupnyh narushenijah avtorskih prav v sfere programmnogo obespechenija [Investigative examination in cases of criminal copyright violations in the field of software] / M.A. Romanenko // Vestnik Omskogo universiteta. Serija: Pravo [Bulletin of Omsk University. Series: Law]. — 2008. — № 1. — P. 171–175. [in Russian]

20. Khutoroi S.N. Kiberprostranstvo i real'nyj mir [Cyberspace and the real world] / S.N. Khutoroi // Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Serija: Filosofskie nauki [Bulletin of the Moscow State Regional University. Series: Philosophical Sciences]. — 2011. — № 2. — P. 67–71. [in Russian]

21. Deleuze J. Tysjacha plato: Kapitalizm i shizofrenija [A Thousand Plateaus: Capitalism and schizophrenia] / J. Deleuze, F. Guattari. — Yekaterinburg : U-Factoriya, 2010. — 892 p. [in Russian]

22. Sorokovikova V.I. Postmodernizm: jesteticheskij, kul'turologicheskij i filosofskij aspekty izuchenija [Postmodernism: aesthetic, cultural and philosophical aspects of study] / V.I. Sorokovikova // Aktual'nye problemy gumanitarnyh i estestvennyh nauk [Actual problems of the humanities and natural sciences]. — 2010. — № 1. — P.114–119. [in Russian]