

Научная статья

УДК 343.3/7

doi 10.63118/3034-3259.2026.7.1.001



## Правовые меры противодействия преступности в Даркнете

**АЛИНА СЕРГЕЕВНА ЕРДАКОВА**

Кубанский государственный университет, Краснодар, Россия,  
alina.erdakova@yandex.ru, <https://orcid.org/0009-0001-7609-0829>

**МАКСИМ ГЕННАДЬЕВИЧ ГОРЕНКО**

Кубанский государственный университет, Краснодар, Россия,  
Maxim\_gko@mail.ru, <https://orcid.org/0000-0002-0085-1169>

Аннотация. В статье рассматривается актуальная проблема роста преступной деятельности в Даркнете, представляющей глобальную угрозу безопасности. Анализируется статистика, подтверждающая значительный рост кибератак и незаконных сделок в теневом сегменте Интернета. Отмечается, что, несмотря на установленную в Уголовном кодексе РФ ответственность за многие преступления, совершаемые в Даркнете, отсутствуют составы, непосредственно направленные против его инфраструктуры. В связи с этим предлагается ввести в УК РФ новые нормы, криминализирующие создание и рекламу Даркнет-платформ, разработку для них программного обеспечения, а также распространение инструкций по доступу. Предлагается систематизировать эти меры в отдельной главе УК РФ, что позволит снизить вредоносное влияние Даркнета путем сужения доступа к нему и пресечения деятельности, способствующей его развитию.

Ключевые слова: даркнет, киберпреступность, анонимность, теневой Интернет, уголовная ответственность, общественная опасность.

5.1.4 Уголовно-правовые науки.

Для цитирования: Ердакова А. С., Горенко М. Г. Правовые меры противодействия преступности в Даркнете // *Lex criminalis scientiarum*. 2026. Том 3. № 1 (7). С. 9-13. doi 10.63118/3034-3259.2026.7.1.001.

Original article

## Legal measures to counteract crime on the Darknet

**ALINA S. ERDAKOVA**

Kuban State University, Krasnodar, Russia, alina.erdakova@yandex.ru,  
<https://orcid.org/0009-0001-7609-0829>

**MAXIM G. GORENKO**

Kuban State University, Krasnodar, Russia, Maxim\_gko@mail.ru,  
<https://orcid.org/0000-0002-0085-1169>

**Abstract.** The article discusses the current problem of the growth of criminal activity on the Darknet, which poses a global security threat. The statistics confirming a significant increase in cyberattacks and illegal transactions in the shadow segment of the Internet are analyzed. It is noted that, despite the responsibility established in the Criminal Code of the Russian Federation for many crimes committed on the Darknet, there are no compounds directly directed against its infrastructure. In this regard, it is proposed to introduce new norms in the Criminal Code of the Russian Federation criminalizing the creation and advertising of Darknet platforms, the development of software for them, as well as the dissemination of access instructions. It is proposed to systematize these measures in a separate chapter of the Criminal Code of the Russian Federation, which will reduce the harmful influence of the Darknet by narrowing access to it and suppressing activities that contribute to its development.

**Keywords:** darknet, cybercrime, anonymity, shadow Internet, criminal liability, public danger.

#### 5.1.4. Criminal legal sciences.

**For citation:** Erdakova A.S., Gorenko M.G. Legal measures to counteract crime on the Darknet. *Lex criminalis scientiarum*. 2026, vol. 3, no. 1 (7), pp. 9-13. doi 10.63118/3034-3259.2026.7.1.001.

Современный Интернет является неоднородной системой. В нём выделяется три уровня: открытый Интернет, глубокий Интернет и тёмный Интернет. Именно тёмный и зовётся Даркнетом. Даркнет – это часть Интернета, доступ к которой возможен с помощью специального программного обеспечения, позволяющего пользователям сохранять анонимность, занимаясь противоправной деятельностью, такой как незаконный оборот наркотиков, мошенничество, хакерство, незаконная продажа оружия, торговля людьми, подделка документов, заказ убийств.

Актуальность и проблематика данной темы заключается в том, что в последнее время роль Даркнета сильно возросла. Большое количество преступлений совершается там благодаря возможности остаться анонимным. Проблеме Даркнета уделяется недостаточно внимания, а он представляет глобальную угрозу безопасности, скрывает криминальную активность.

Преступления, совершаемые в Даркнете, охватывают практически все главы Особенной части Уголовного кодекса Российской Федерации (далее – УК РФ). Согласно статистике, из 1,8 млн преступлений, зарегистрированных в России за 11 месяцев 2023 года, с использованием Интернета было совершено 477 тыс. (26,5%) [1]. В Даркнете увеличилось количество сообщений, относящихся к стилерам – программам для кражи конфиденциальной информации, такой как учётные данные для входа в систему, финансовые реквизиты и личные данные. По информации компании «Информзащита», в 2024 году количество кибератак с использованием стилеров увеличилось на 54% по сравнению с 2023-м: в 2022 году их было 240 тыс., а к 2024-му показатель вырос до 750 тыс. атак на устройства пользователей [2].

В 2024 году активность киберпреступников в даркнете увеличилась на 30% по сравнению с 2023 годом, достигнув до 2 тыс. объявлений в месяц [3].

Одной из ключевых тенденций 2025 года является рост масштабируемых и умных атак, движимых искусственным интеллектом, шифрованием и автоматизацией. Киберпреступники теперь активно используют «Искусственный интеллект как услугу» (AlaaS). Например, адаптивные фишинговые атаки, которые в реальном времени меняют язык и тон в зависимости от поведения жертвы, а также вредоносное ПО, способное обходить современные системы защиты (EDR) за счет AI-генерации мутаций в своем коде.

Параллельно трансформируется и инфраструктура теневого рынка. Новые торговые площадки появляются каждые 2–3 недели, часто их рекламируют на закрытых форумах или в Telegram-каналах. Всё чаще для анонимных транзакций используют криптовалюту Monero

вместо биткоина [4].

Растет и ущерб: атаки на критическую инфраструктуру России в 2025 году выросли в 4 раза, а общий ущерб от IT-преступлений за первые пять месяцев 2025 года превысил 81 млрд рублей, в основном за счет дистанционного мошенничества.

УК РФ установлена ответственность за преступления, совершаемые в Даркнете, например, за торговлю оружием (ст. 222 УК РФ), однако, не установлена таковая за действия, способствующие развитию теневого Интернета. Поэтому представляется целесообразным установление в УК РФ ответственности за создание Даркнет-сайтов, их рекламу, разработку программного обеспечения для Даркнета, за распространение инструкций и ссылок, позволяющих попасть в теневой Интернет, за обеспечение деятельности данного сектора Интернета.

Даркнет Hydra был создан Яном Кларком в 1999 году и изначально не был связан с запрещенными действиями. Но возможность оставаться анонимным привлекла создателей выпустить программу – Tor. Далее с появлением криптовалют и онлайн-шифрования данная платформа стала хорошим местом для преступников [5]. Все остальные темные платформы, появившиеся по примеру Hydra, создавались уже с целью ведения незаконной деятельности. Под роликами с рекламой Hydra представители данного Даркнета в одном из своих ответов комментаторам написали, что людям не стоит переживать о закрытии данного Даркнета – на месте одного заблокированного канала «вырастут» три новых, ведь они Hydra [6]. Поэтому в УК РФ следует предусмотреть статью, согласно которой лицо, создающее Даркнет платформу с целью ведения незаконной деятельности, несёт уголовную ответственность.

Следующее предложение вытекает из предыдущего – ответственность за разработку программного обеспечения для Даркнета. Поскольку выход в Даркнет осуществляется с помощью специального программного обеспечения TOR (The Onion Router), 2IP (Invisible Internet Project – невидимый Интернет), а также через специальные VPN сервисы для Даркнета [7], то следует ввести в УК РФ статью, согласно которой лицо, создающее и распространяющее специальное программное обеспечение для теневого Интернета, не являющегося общедоступным, подлежит уголовной ответственности. Благодаря этому доступ к «тёмной» платформе значительно сузится.

Также в УК РФ особенно важно предусмотреть ответственность за рекламу Даркнета. Во времена, когда существовала Hydra, было очень много спам рассылок в мессенджерах, прямая открытая реклама на YouTube, в Telegram-каналах, нативная реклама на страницах у блогеров. Hydra тратила на рекламу более миллиарда рублей в год. Было много пиара и рекламных акций. Наиболее громкая история произошла вечером 19 декабря 2022 года, когда автобус с рекламой маркетплейса Kraken (на него нанесли название маркетплейса и QR-код, ведущий на его страницу) перекрыл две полосы на Новом Арбате неподалеку от Министерства иностранных дел. Ещё до своего запуска реклама данного проекта появилась на одном из рекламных кубов в «Москва-Сити». А в январе 2023 года реклама Kraken стала появляться в московском метро [8].

В связи с этим, необходимо ввести в УК РФ статью о запрете рекламирования платформ, торгующих незаконными объектами. В Федеральном законе от 13.03.2006 г. № 38-ФЗ «О рекламе» в ст. 7 представлены объекты рекламирования, реклама которых не допускается [9]. Однако ответственность за такую рекламу не установлена. Поэтому целесообразно ввести в УК статью, согласно которой лица, распространяющие информацию о Даркнете, направленную на потребителя с целью привлечения внимания, в общественных местах, а равно в средствах массовой информации подлежат уголовной ответственности.

Благодаря данной статье можно будет сократить количество людей, знающих о теневых платформах, а значит свести к минимуму число тех, кто пользуется их услугами.

Человек, не знающий алгоритма попадания в теневой Интернет, может легко найти его

на просторах открытого Интернета. Согласно исследованию, проведенному NordVPN, 49% всех поисковых запросов Google, связанных с Даркнетом, пытаются найти способы получить к нему доступ [10]. Среди людей, интересующихся теневым Интернетом, могут быть подростки, у которых не сформировалась психика. Тем более, что необходимое программное обеспечение находится в открытом для скачивания доступе. Данные Даркнета будут негативно влиять на подростков, и у них может сформироваться установка на преступную деятельность. В Даркнете также есть инструкции по созданию взрывчатых веществ. Подростки могут воспользоваться данными схемами и нанести вред как себе, так и окружающим. Именно поэтому в УК РФ стоит ввести статью, согласно которой лица, распространяющие инструкции, ссылки, алгоритмы, видео и иную информацию, которая способствует попаданию в Даркнет, несут уголовную ответственность.

Из-за того, что Даркнет зарекомендовал себя как часть Интернета, известная возможностью вести незаконную деятельность, то следует ввести ответственность за обеспечение деятельности данного сектора Интернета. Имеется ввиду, что на данных платформах есть люди, которые сами непосредственно ничего не продают, но работают, например, в качестве администраторов, модераторов. То есть так или иначе возвращаются в преступной среде.

Предложенные статьи можно объединить в отдельную главу, посвященную Даркнету – Преступления, способствующие развитию теневого сегмента Интернета. И включить данную главу в раздел 9 УК РФ – Преступления против общественной безопасности и общественного порядка.

Таким образом, можно сделать вывод, что, как представляется, полностью избавиться от теневого Интернета не удастся, поскольку мы живём в информационном обществе. Однако можно минимизировать его пагубное воздействие и свести к минимуму совершаемые там преступления посредством предложенных изменений в УК РФ.

## СПИСОК ИСТОЧНИКОВ

1. Каждое четвертое преступление в России совершают через интернет. Москва, 3 января. / ТАСС/. – URL: <https://tass.ru/obschestvo/19669641> (дата обращения: 19.08.2025).
2. Быть на стилере: вирусы-воры паролей маскируются под нейросеть DeepSeek | Статьи | Известия. – URL: <https://iz.ru/1834912/anton-belyi/byt-na-stilere-virusy-vory-parolej-maskiruyutsya-rod-nejroset-deepseek> (дата обращения: 21.08.2025).
3. Исследование показало рост киберпреступности на треть в даркнете в 2024 году - Рамблер/личные финансы. – URL: <https://finance.rambler.ru/money/53852227-issledovanie-pokazalo-rost-kiberprestupnosti-na-tret-v-darknete-v-2024-godu/> (дата обращения: 19.08.2025).
4. Dark Web Statistics 2025–26: Cybercrime Markets, Breaches & Security Insights. – URL: <https://comparecheapssl.com/dark-web-statistics-cybercrime-trends-market-insights-security-implications/> (дата обращения: 10.09.2025).
5. Что такое даркнет и стоит ли его использовать. – URL: [https://webznam.ru/blog/temnaja\\_set\\_darknet/2022-05-26-2046](https://webznam.ru/blog/temnaja_set_darknet/2022-05-26-2046) (дата обращения: 12.09.2025).
6. Кто создал HYDRA? Разбор нарко-империи – Telegraph. – URL: <https://telegra.ph/Kto-sozdal-HYDRARazbor-narko-imperii-12-21> (дата обращения: 23.08.2025).
7. Александров А.Г., Сафронов А.А. Использование сети Даркнет при подготовке и совершении преступлений // Вестник Санкт-Петербургского университета МВД России. 2021. № 1 (89). С. 156–160.
8. Наркотики теперь рекламируют в метро и на улицах Москвы. Как война за наркорынок России вышла за пределы даркнета? Лента.ру. – URL: <https://lenta.ru/articles/2023/01/13/darkpr/> (дата обращения: 13.09.2025).
9. Федеральный закон от 13.03.2006 № 38-ФЗ (ред. от 19.04.2024) "О рекламе" // СПС «КонсультантПлюс». – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_58968/3bfc26317bd01efad6f67aadf9981b248a57ef4b/](https://www.consultant.ru/document/cons_doc_LAW_58968/3bfc26317bd01efad6f67aadf9981b248a57ef4b/)
10. Что такое даркнет и стоит ли его использовать. – URL: [https://webznam.ru/blog/temnaja\\_set\\_darknet/2022-05-26-2046](https://webznam.ru/blog/temnaja_set_darknet/2022-05-26-2046) (дата обращения: 11.09.2025).

## REFERENCES

1. One in four crimes in Russia is committed online. Moscow, 3 January. /TASS/. – URL: <https://tass.ru/obschestvo/19669641> (accessed: 19 August 2025).
2. Staying on the cutting edge: password-stealing viruses masquerade as the DeepSeek neural network | Articles | Izvestia. – URL: <https://iz.ru/1834912/anton-belyi/byt-na-stilere-virusy-vory-parolej-maskiruyutsya-pod-nejroset-deepseek> (accessed: 21 August 2025).
3. Study shows cybercrime on the dark web rose by a third in 2024 – Rambler/Personal Finance. – URL: <https://finance.rambler.ru/money/53852227-issledovanie-pokazalo-rost-kiberprestupnosti-na-tret-v-darknete-v-2024-godu/> (accessed: 19 August 2025).
4. Dark Web Statistics 2025–26: Cybercrime Markets, Breaches & Security Insights. – URL: <https://comparecheapssl.com/dark-web-statistics-cybercrime-trends-market-insights-security-implications/> (accessed: 10 September 2025).
5. What is the dark web and should you use it? – URL: [https://webznam.ru/blog/temnaja\\_set\\_darknet/2022-05-26-2046](https://webznam.ru/blog/temnaja_set_darknet/2022-05-26-2046) (accessed: 12 September 2025).
6. Who created HYDRA? An analysis of the drug empire – Telegraph. – URL: <https://telegra.ph/Kto-sozdal-HYDRARazbor-narko-imperii-12-21> (accessed: 23 August 2025).
7. Aleksandrov A.G., Safronov A.A. The use of the Darknet in the preparation and commission of crimes // Bulletin of St Petersburg University of the Ministry of Internal Affairs of Russia. 2021. No. 1 (89). pp. 156–160.
8. Drugs are now being advertised in the Moscow Underground and on the streets of Moscow. How has the battle for Russia's drug market moved beyond the dark web? Lenta.ru. – URL: <https://lenta.ru/articles/2023/01/13/darkpr/> (accessed 13 September 2025).
9. Federal Law No. 38-FZ of 13 March 2006 (as amended on 19 April 2024) 'On Advertising' // SPS 'ConsultantPlus'. – URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_58968/3bfc26317bd01efad6f67aadf9981b248a57ef4b/](https://www.consultant.ru/document/cons_doc_LAW_58968/3bfc26317bd01efad6f67aadf9981b248a57ef4b/)
10. What is the dark web and is it worth using? – URL: [https://webznam.ru/blog/temnaja\\_set\\_darknet/2022-05-26-2046](https://webznam.ru/blog/temnaja_set_darknet/2022-05-26-2046) (accessed: 11 September 2025).

## СВЕДЕНИЯ ОБ АВТОРАХ

**АЛИНА СЕРГЕЕВНА ЕРДАКОВА** – студентка 5 курса юридического факультета им. А.А. Хмырова Федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный университет», Краснодар, Россия, [alina.erdakova@yandex.ru](mailto:alina.erdakova@yandex.ru), <https://orcid.org/0009-0001-7609-0829>

**МАКСИМ ГЕННАДЬЕВИЧ ГОРЕНКО** – кандидат юридических наук, преподаватель кафедры уголовного права и криминологии юридического факультета им. А.А. Хмырова Федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный университет», Краснодар, Россия, [Maxim\\_gko@mail.ru](mailto:Maxim_gko@mail.ru), <https://orcid.org/0000-0002-0085-1169>

## INFORMATION ABOUT THE AUTHORS

**ALINA S. ERDAKOVA** – Fifth-year student at the A.A. Khmyrov Faculty of Law, Kuban State University (a federal state-funded higher education institution), Krasnodar, Russia, [alina.erdakova@yandex.ru](mailto:alina.erdakova@yandex.ru), <https://orcid.org/0009-0001-7609-0829>

**MAXIM GENNADIEVICH GORENKO** – PhD in Law, Lecturer in the Department of Criminal Law and Criminology, A.A. Khmyrov Faculty of Law, Kuban State University, a Federal State Budgetary Educational Institution of Higher Education, Krasnodar, Russia, [Maxim\\_gko@mail.ru](mailto:Maxim_gko@mail.ru), <https://orcid.org/0000-0002-0085-1169>

*Статья поступила 23.11.2025  
Принята к печати 26.03.2026*