УДК 343.98 DOI 10.21777/2587-9472-2026-1-53-57

К ВОПРОСУ О ПОНЯТИИ «КИБЕРПРЕСТУПЛЕНИЕ» В КРИМИНАЛИСТИКЕ

Меркулова Марина Викторовна[1],
канд. юрид. наук,
e-mail: merkulova.mosu@gmail.com
[1]*Московский университет имени С.Ю. Витте, г. Москва, Россия*

Рассматриваются актуальные вопросы относительно содержания и сущности понятия «киберпреступление», а также его связи с понятиями «киберугроза» и «кибербезопасность». Дается типовая схема реализации киберугрозы. Приводится перечень основных угроз в киберпространстве на сегодняшний день с акцентированием внимания на новейших тенденциях (Интернет вещей и др.). Через призму криминалистической классификации (систематизации) рассматриваются виды высокотехнологичных преступлений как с точки зрения экспертов ООН, стоявших у истоков понятия «киберпреступление», так и с позиций современных ученых и практиков. Формулируется обобщающее понятие киберпреступления, при этом подчеркивается единство понимания сущности киберпреступлений в современном мире. На основе данных официальной статистики показываются изменения в динамике киберпреступности в Российской Федерации с 2024 года. Анализируется качественная структура современной киберпреступности, оставшаяся фактически неизменной. В заключении приводится обоснованный вывод о необходимости дальнейших научных исследований рассматриваемой проблематики.
По тексту статьи Российская Федерация сокращенно указывается – РФ.

Ключевые слова: киберпреступление, киберугроза, киберзащита, информационно-телекоммуникационные технологии, расследование, криминалистическая классификация преступлений, Организация Объединенных Наций

ON THE ISSUE OF THE CONCEPT OF CYBERCRIME IN FORENSICS

Merkulova M.V.[1],
Candidate of Legal Sciences,
e-mail: merkulova.mosu@gmail.com
[1]*Moscow Witte University, Moscow, Russia*

The current issues regarding the content and essence of the concept of "cybercrime", as well as its connection with the concepts of "cyber threat" and "cybersecurity" are considered. A typical scheme of cyber threat implementation is given. The state-of-the-art list of the main threats in cyberspace is given, focusing on the latest trends (Internet of Things, etc.). Through the prism of forensic classification (systematization) types of high-tech crimes are considered, both from the point of view of UN experts, who were at the origin of the concept of "cybercrime", and from the perspective of modern scientists and practitioners. The concept of cybercrime is formulated, emphasizing the unity of understanding of the essence of cybercrime in the modern world. Based on official statistics, changes in the dynamics of cybercrime in the Russian Federation have been shown since 2024. The qualitative structure of modern cybercrime, which has remained virtually unchanged, is analyzed. In conclusion, a valid conclusion is made about the need for further scientific research on the issue under consideration. In the text of the article, the Russian Federation is abbreviated as RF.

Keywords: cybercrime, cyber threat, cyber defense, information and telecommunication technologies, investigation, forensic classification of crimes, United Nations

Нарастающее развитие и внедрение в общественные отношения компьютерных технологий предполагает, с одной стороны, повышение качества жизни общества, с другой – пропорциональное увеличение количества вероятных угроз ее безопасности и стабильности. Источники и механизмы и цели таких угроз могут быть самыми различными, но объединяет их наличие вредоносного потенциала и реализация в цифровом пространстве (киберпространстве) посредством информационно-телекоммуникационных технологий и действий людей.

Киберугрозы [1, с. 3] могут реализовываться как в виде создания определенного вредоносного контента, так и в виде прямых атак на информационное пространство компьютеров, в которых находятся сведения, представляющие интерес для инициатора атаки (рисунок 1). В связи с этим ключевое значение приобретает организация информационной защиты объекта (кибезащиты) – деятельности по предотвращению неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов [2, с. 105; 3, с. 21; 4, с. 29; 5, с. 5].

КИБЕРУГРОЗА	
Условия реализации (наличие уязвимостей информационного объекта):	Факторы воздействия на информационный объект:
— недостатки в обеспечении защиты информации; — недостатки в системе обработки информации	— явления природного или техногенного характера; — процессы хранения, обработки и передачи информации; — действия людей

Рисунок 1 – Схема реализации киберугрозы

К основным угрозам в киберпространстве на международном уровне относят:

– разработку вредоносных компьютерных программ и средств (разработка «программ-вымогателей», троянских и других вредоносных программ, организация DDoS-атак и ботов);

– кибератаки на критическую инфраструктуру экономики и государства (электростанции, транспортные узлы, объекты промышленности);

– интернет-контент, касающийся сексуальной эксплуатации детей;

– террористическую активность в Интернете;

– кибермошенничество (в т.ч. с банковскими картами и безналичными платежами);

– интернет-торговлю оружием, наркотическими средствами, иными запрещенными товарами, незаконная торговля людьми;

– онлайн-оборот контрафактной продукции;

– хищение криптовалют, а также использование криптовалют (Bitcoin, Monero, Ethereum, Zcach) при совершении различного рода преступлений и «отмывании» незаконных денежных средств;

– угрозы и риски, связанные с устройствами, системами и услугами Интернета вещей.

Последний пункт, на наш взгляд, нуждается в некотором пояснении. Под Интернетом вещей понимается современная техническая концепция, согласно которой физические предметы повседневной жизни соединяются в сеть при помощи интернета и обмениваются данными между собой без необходимости прямого взаимодействия с человеком**.** Эти объекты – «умные» устройства – могут собирать и передавать информацию, а также автоматически выполнять определенные задачи. Примером могут служить автоматизированные («умные») дома и промышленные объекты, которые в некоторых случаях становятся мишенью для заинтересованных лиц. Так, если у автоматизированного объекта шина управления находится извне и ничем не защищена, то злоумышленник фактически может подключиться к ней через любой модем и осуществлять удаленное управление системой.

Преступная деятельность, связанная с использованием высоких технологий, явившись закономерным следствием всеобъемлющей цифровизации современного общества, потребовала не только

принятия адекватных мер реагирования со стороны правоохранительных органов, но и (что вполне очевидно) научно-практической систематизации появляющихся видов общественно-опасных деяний.

Заметим, что термин «киберпреступность» впервые появился за рубежом. Так, в 2000 году на десятом Конгрессе ООН по предупреждению преступности и обращению с правонарушителями понятие киберпреступности было использовано для обозначения «компьютерных» преступлений, где объектом является информационная безопасность, а предметом – компьютер, а также посягательств на любые общественные отношения, совершаемых с использованием компьютеров в качестве орудия или средства. При этом киберпреступления разделили на пять категорий:

1. Несанкционированный доступ к устройству.
2. Повреждение компьютерных данных или программ.
3. Саботаж для нарушения работы компьютерной системы или сети.
4. Несанкционированный перехват данных внутри системы или сети.
5. Компьютерный шпионаж [6, с. 129][1].

В настоящее же время в науке и практике существует несколько формулировок-синонимов высокотехнологичных преступлений:

– преступления в сфере компьютерной информации;
– преступления в сфере высоких технологий;
– киберпреступления;
– компьютерные преступления и т.д.

Следует отметить, что законодатель не приводит определений данных понятий и их перечень. Исключение составляют лишь преступления в сфере компьютерной информации, указанные в главе 28 УК РФ. Вполне очевидно, что к данной группе высокотехнологичных преступлений необходимо относить не только преступления в сфере компьютерной информации, но и иные общеуголовные и экономические преступления, совершенные с использованием информационно-коммуникационных технологий [7, с. 89; 8, с. 79]. Таким образом, понятие «киберпреступление» охватывает:

– преступления в сфере компьютерной информации (гл. 28 УК РФ);
– мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);
– мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ);
– кража с банковского счета, а равно в отношении электронных денежных средств (ст. 158 ч. 3 п. «Г» УК РФ);
– нарушение авторских и смежных прав (ст. 146 УК РФ);
– незаконный оборот наркотических средств (ст. 228–228.4 УК РФ) и др.

Соответственно, под киберпреступлениями можно понимать любые преступления, совершаемые с использованием информационно-телекоммуникационных технологий. Такого подхода к трактовке рассматриваемого понятия практически единогласно придерживаются не только ученые-криминалисты, но и IT-компании, специализирующиеся на разработке систем защиты от киберугроз, в том числе АО «Лаборатория Касперского»[2].

Согласно данным официальной статистики, еще год назад киберпреступность имела выраженную тенденцию к росту[3], однако в текущем году можно говорить об изменении этой ситуации. Так, за январь – август 2025 года преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, по сравнению с январем – августом 2024 года зарегистрировано на 5,4% меньше. При этом количество преступлений в сфере компьютер-

[1] См.: Справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети. – Текст: электронный. Управление ООН по наркотикам и преступности [офиц. сайт]. – URL: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks_R.pdf (дата обращения: 16.10.2025).

[2] Что такое киберпреступность? Как защититься? – Текст: электронный // АО «Лаборатория Касперского» kaspersky.ru [офиц. сайт]. – URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 16.10.2025).

[3] См.: Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года. – Текст: электронный // Материалы ФКУ ГИАЦ. Министерство внутренних дел Российской Федерации [офиц. сайт]. – URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 16.10.2025).

ной информации снизилось на 34,4%, дистанционных краж – на 17,1%[4]. Снизить уровень киберпреступности во многом удалось благодаря системным мерам МВД РФ и изменениям в законодательстве – в частности, введению ответственности за использование «дропов»[5] и сим-боксов[6], а также активному пресечению деятельности колл-центров, занимавшихся телефонным и онлайн-мошенничеством, и преступных групп, создававших и распространявших вредоносное программное обеспечение. Как подчеркнул начальник Следственного департамента МВД России С.Н. Лебедев, современное законодательство дает правоохранительным органам весь необходимый инструментарий для борьбы с киберпреступностью, в связи с чем ключевой задачей становится его эффективное применение и межведомственная координация деятельности[7].

Вместе с тем, соотношение отдельных видов киберпреступлений не претерпевает серьезных изменений: по-прежнему порядка двух третей таких преступлений совершается путем кражи или мошенничества. Среди краж, совершаемых с использованием компьютерных технологий, наиболее распространены хищения денежных средств в системе дистанционного банковского обслуживания (ДБО), банкоматов, POS-терминалов[8], а также компьютерных систем кредитных организаций. Подобные преступления совершаются путем несанкционированной модификации кода систем ДБО, установки поддельных POS-терминалов, взлома мобильных устройств, брокерских систем в Интернете и напрямую банковских систем, а также разработки и применения вредоносных программных продуктов целевого действия, ориентированных на программную систему конкретной кредитной организации. Кибермошенничество же чаще всего заключается в несанкционированных действиях в финансовой сфере с использованием так называемой «социальной инженерии» – практики получения конфиденциальной информации путем психологического воздействия на легальных пользователей[9].

Нет сомнения в том, что вопросы криминалистической классификации (систематизации) киберпреступлений, а также уточнения связанного с этим понятийного аппарата должны стать предметом дальнейших научных разработок. Постоянная трансформация ныне существующих и прогнозируемое появление новых видов высокотехнологичных преступлений требует своевременного пересмотра и упорядочивания криминалистических знаний в области методики их раскрытия и расследования.

Список литературы

1. *Язов Ю.К.* Об определении понятия «кибербезопасность» и связанных с ним терминов // Вопросы кибербезопасности. – 2025. – № 1(65). – С. 2–6. – DOI 10.21681/2311-3456-2025-1-2-6. – EDN HNKWDB.
2. *Малюк А.А.* Информационная война и современные проблемы обеспечения информационной безопасности // Вопросы кибербезопасности. – 2024. – № 5(63). – С. 105–114. – DOI 10.21681/2311-3456-2024-5-105-114. – EDN AGFENP.

---

[4] См.: Краткая характеристика состояния преступности в Российской Федерации за январь – август 2025 года. – Текст: электронный // Материалы ФКУ ГИАЦ. Министерство внутренних дел Российской Федерации [офиц. сайт]. – URL: https://мвд.рф/reports/item/70644759/ (дата обращения: 16.10.2025 г.).

[5] «Дроп» – сленговый термин (от англ. drop – «сбросить», «исключить», «снизить»), значение которого может варьироваться в зависимости от контекста. С точки зрения совершения мошеннических действий, «дроп» или «дроппер» – посредник в мошеннических схемах, принимающий участие в совершении преступления как осознанно, так и неосознанно.

[6] Сим-бокс (SIM-box) – программно-аппаратный комплекс, предназначенный для объединения большого количества сим-карт под единым управлением. Это устройство обеспечивает удаленный доступ к каждой из этих сим-карт, предоставляя возможность совершать телефонные звонки и рассылать текстовые сообщения неограниченному числу абонентов дистанционно.

[7] Сергей Лебедев провел совещание по вопросам противодействия дистанционным хищениям и преступлениям в сфере компьютерной информации. – Текст: электронный // «МВД медиа» [офиц. портал]. – URL: https://mvdmedia.ru/news/official/sergey-lebedev-provel-soveshchanie-po-voprosam-protivodeystviya-distantsionnym-khishcheniyam-i-prest (дата обращения: 16.10.2025).

[8] POS-терминал (от англ. point of sale – точка продажи и terminal – окончание) – электронное программно-техническое устройство для приема к оплате платежных карт (при этом зачастую под POS-терминалом подразумевают весь программно-аппаратный комплекс, который установлен на рабочем месте кассира). Существует также виртуальный POS-терминал, который представляет собой веб-интерфейс, заменяющий физическое устройство и предполагающий схему обслуживания «клиент → оператор → виртуальный POS-терминал». В данном случае клиент вводит свои данные и данные своей карты через веб-интерфейс, взаимодействующий с системой банка, после чего проходит транзакция об оплате.

[9] О понятии социальной инженерии см.: ГОСТ Р МЭК 62443-2-1-2015 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики. Пункт 3.1.39. – Текст: электронный. – URL: https://docs.cntd.ru/document/1200121982 (дата обращения: 30.10.2025).

3. *Карцхия А.А.* Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права / А.А. Карцхия, Г.И. Макаренко, М.Ю. Сергин // Вопросы кибербезопасности. – 2019. – № 3(31). – С. 18–23. – DOI 10.21681/2311-3456-2019-3-18-23. – EDN ZWLJGJ.
4. *Марков А.С.* Руководящие указания по кибербезопасности в контексте ISO 27032 / А.С. Марков, В.Л. Цирлов // Вопросы кибербезопасности. – 2014. – № 1(2). – С. 28–35. – EDN RXWJWL.
5. *Мещеряков Р.В.* Перспективные направления применения технологий искусственного интеллекта при защите информации / Р.В. Мещеряков, С.Ю. Мельников, В.А. Пересыпкин, А.А. Хорев // Вопросы кибербезопасности. – 2024. – № 4(62). – С. 2–12. – DOI 10.21681/2311-3456-2024-4-02-12. – EDN GJWQWP.
6. *Витвицкая С.С.* Киберпреступления: понятие, классификация, международное противодействие / С.С. Витвицкая, А.А. Витвицкий, Ю.И. Исакова // Правовой порядок и правовые ценности. – 2023. – Т. 1, № 1. – С. 126–136. – DOI 10.23947/2949-1843-2023-1-1-126-136. – EDN OKGPLW.
7. *Камалиев Д.С.* О соотношении понятий «преступления в сфере компьютерной информации», «компьютерные преступления», «киберпреступления» // Актуальные научные исследования в современном мире. – 2021. – № 4-6(72). – С. 87–90. – EDN BLVCKY.
8. *Кучерков И.А.* О понятии «киберпреступление» в законодательстве и научной доктрине // Юридическая наука. – 2019. – № 10. – С. 78–81. – EDN ZCRUDX.

References

1. *Yazov Yu.K.* On the definition of the concept of “cybersecurity” and related terms // Cybersecurity issues. – 2025. – № 1(65). – Pp. 2–6. – DOI 10.21681/2311-3456-2025-1-2-6. – EDN HNKWDB.
2. *Malyuk A.A.* Information warfare and modern problems of ensuring information security // Cybersecurity issues. – 2024. – № 5(63). – Pp. 105–114. – DOI 10.21681/2311-3456-2024-5-105-114. – EDN AGFENP.
3. *Kartskhiya A.A.* Modern trends in cyber threats and the transformation of the concept of cybersecurity in the context of the digitalization of the legal system / A.A. Kartskhiya, G.I. Makarenko, M.Y. Sergin // Cybersecurity issues. – 2019. – № 3(31). – Pp. 18–23. – DOI 10.21681/2311-3456-2019-3-18-23. – EDN ZWLJGJ.
4. *Markov A.S.* Guidelines on cybersecurity in the context of ISO 27032 / A.S. Markov, V.L. Cirlov // Cybersecurity issues. – 2014. – № 1(2). – Pp. 28–35. – EDN RXWJWL.
5. *Meshcheryakov R.V.* Promising areas of application of artificial intelligence technologies in information protection / R.V. Meshcheryakov, S.Yu. Melnikov, V.A. Peresypkin, A.A. Khorev // Cybersecurity issues. – 2024. – № 4(62). – Pp. 2–12. – DOI 10.21681/2311-3456-2024-4-02-12. – EDN GJWQWP.
6. *Vitvitskaya S.S.* Cybercrimes: concept, classification, international counteraction / S.S. Vitvitskaya, A.A. Vitvitsky, Yu.I. Isakova // Legal order and legal values. – 2023. – Vol. 1, No. 1. – Pp. 126–136. – DOI 10.23947/2949-1843-2023-1-1-126-136. – EDN OKGPLW.
7. *Kamaliev D.S.* On the correlation of the concepts of “crimes in the field of computer information”, “computer crimes”, “cybercrimes” // Actual scientific research in the modern world. – 2021. – № 4-6(72). – Pp. 87–90. – EDN BLVCKY.
8. *Kucherkov I.A.* On the concept of “cybercrime” in legislation and scientific doctrine // Legal Science. – 2019. – No. 10. – Pp. 78–81. – EDN ZCRUDX.

Статья поступила в редакцию: 31.10.2025
Статья принята к публикации: 25.11.2025

Received: 31.10.2025
Accepted: 25.11.2025