Дата поступления рукописи в редакцию: 13.03.2026 г.
Дата принятия рукописи в печать: 03.04.2026 г.
DOI: 10.24412/2076-1503-2026-3-43-46

АББУД Руслан Ратебович,
Кандидат юридических наук,
старший преподаватель кафедры международного права
Российского государственного университета
правосудия имени В.М. Лебедева,
e-mail: ruslan625@yandex.ru

КОМЕНДАНТОВ Сергей Васильевич,
Кандидат юридических наук, доцент,
доцент кафедры международного права
Дипломатической академии МГИМО МИД России,
e-mail: wtolaw@yandex.ru

ПОЗИЦИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ОТНОСИТЕЛЬНО ПОНЯТИЯ И ТРАНСГРАНИЧНОСТИ КИБЕРПРЕСТУПЛЕНИЯ

Аннотация. *В данной статье авторы анализируют определение и трансграничность киберпреступления с точки зрения позиции Российской Федерации на основании правовых документов, принятых на уровне в целях развития международно-правовой базы в части преследования не только тех киберпреступлений, совершаемых в отношении ИКТ (кибератака на конфиденциальность, доступность и целостность компьютерных данных), но и посредством ИКТ (дипфейк, кибербуллинг), а также международных соглашений.*

В век цифровизации и стремительного прогресса информационных технологий практически не осталось сфер, где киберпреступления не оставили свой след. По данным Международного союза электросвязи, текущий уровень киберпреступлений оценивается приблизительно в 2200 кибератак в мире ежедневно, при этом ежегодно количество кибератак в мире увеличивается на 80%. Схожие данные приводит и Роскомнадзор, указывая на то, что число компьютерных и DDoS-атак ежегодно увеличивается в среднем на 70%. Кроме того, в соответствии с информацией мирового индикатора Estimated Cost of Cybercrime, совершение киберпреступлений в период с 2024 г. по 2029 г. будет идти по нарастающей с каждым годом на 6,4 трлн долл. США.

В настоящее время экономический, а также финансовый сектор, являются одними из самых популярных целей для киберпреступников. В первую очередь страдают компании, производящие товары, а также предоставляющие услуги по страхованию. Более того, кибератаки часто совершаются в отношении интеллектуальной собственности, а также на системы управления объектами жизнеобеспечения. Бороться с этой уязвимостью компании пытаются при помощи выделения средств на финансирование в целях повышения иммунитета от киберугроз и противодействию киберпреступлениям.

Ключевые слова: *киберпреступление, Конвенция ООН против киберпреступности 2024 года, трансграничность, ИКТ, Российская Федерация.*

ABBUD Ruslan Ratebovich,
candidate of law, Senior Lecturer Professor of the International Law
Department at the Lebedev Russian State University of Justice

KOMENDANTOV Sergey Vasilievich,
candidate of law, associate professor,
associate professor of the Department of International Law,
Diplomatic Academy of the Moscow State Institute
of International Relations (University) of the Ministry
of Foreign Affairs of the Russian Federation

THE POSITION OF THE RUSSIAN FEDERATION ON THE CONCEPT AND CROSS-BORDER OF CYBERCRIME

Annotation. *In this article, the authors analyze the definition and signs of cybercrime from the point of view of the position of the Russian Federation on the basis of legal documents adopted at the domestic level in order to develop an international legal framework for the prosecution of not only those cybercrimes committed against ICT (cyber attacks on confidentiality, accessibility and integrity of computer data), but also through ICT (deepfake, cyberbullying), as well as international agreements.*

In the age of digitalization and the rapid progress of information technology, there are practically no areas where cybercrimes have not left their mark. According to the International Telecommunication Union, the current level of cybercrime is estimated at about 2,200 cyber attacks in the world every day, while the number of cyber attacks in the world increases by 80% annually. Roskomnadzor provides similar data, indicating that the number of computer and DDoS attacks increases by an average of 70% annually. In addition, according to the information provided by the global Estimated Cost of Cybercrime indicator, the commission of cybercrimes in the period from 2024 to 2029 will increase by 6.4 trillion US dollars every year.

Currently, the economic as well as the financial sector are among the most popular targets for cybercriminals. First of all, companies that produce goods and provide insurance services are affected. Moreover, cyber attacks are often carried out against intellectual property, as well as against life support management systems. Companies are trying to combat this vulnerability by allocating funds for financing in order to increase immunity from cyber threats and counter cybercrime.

Key words: *cybercrime, the UN Convention on Cybercrime of 2024, cross-border, ICT, the Russian Federation.*

На сегодняшний день в научном дискурсе участвуют сторонники как широкого, так и узкого подхода в части определения киберпреступления. Позиция Российской Федерации эксплицитно ратует за широкий подход в части понимания определения киберпреступления, однако на сегодняшний день на законодательном уровне не выработана легальная дефиниция в части определения киберпреступления. По мнению В.Н. Русиновой, государства, реагируя на случаи вредоносного использования ИКТ, предпочитают выбирать политическую, а не юридическую риторику, а если обращаются к праву, то используют национальные нормы [1]. На национальном уровне в Российской Федерации действуют документы, направленные на развитие международно-правовой базы в части преследования киберпреступлений. К этим правовым документам можно отнести:

1) Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
2) Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации»;
3) Концепция внешней политики Российской Федерации, утверждённая Указом Президента РФ от 31 марта 2023 г. № 229.

На основе вышеназванных документов позиция Российской Федерации заключается в том, чтобы международное определение киберпреступления включало в себя не только так называемые «чистые киберпреступления» (вирусы, DDoS-атаки), но и преступления, совершаемые с помощью ИКТ (использование ИКТ для террористических и экстремистских целей). Кроме того, Российская Федерация активно выступает за включение в международное определение деяний, связанных с распространением противоправной, а также дискредитирующей информации. Это часто является камнем преткновения в части спора с западными странами. Приоритет государственного суверенитета является ключевым элементом позиции нашей страны. Определение киберпреступления и механизмы борьбы с ним не должны позволять иностранным спецслужбам получать трансграничный доступ к компьютерным данным и информации на территории Российской Федерации без официального согласия российских властей. Именно из-за статьи 32 b Будапештской конвенции, допускающей такой доступ, Россия отказалась ее подписывать. До недавнего времени не существовало единого, универсального международно-правового договора, направленного на пресечение киберпреступности [2]. Однако в 2024 году резолюцией 79/243 ГА принята универсальная Конвенция ООН против киберпреступности. Несмотря на то, что Российская Федерация является ее инициатором, наша страна намерена в этом году разработать дополнительный протокол к Конвенции. В частности, речь идет о расширении перечня криминализируемых деяний (экстремизм, терроризм).

Таким образом, для Российской Федерации киберпреступление – это не только технических взлом, но и любое использование цифровой среды для совершения общественно опасных деяний, при этом борьба с ними должна вестись в соответствии с строгим соблюдением цифрового суверенитета государств.

Вопрос трансграничности киберпреступления является также составной и неотъемлемой части данного криминогенного деяния. Позиция Российской Федерации в отношении трансграничности киберпреступлений является одной из самых принципиальных и последовательных на международной арене. Она строится на балансе между признанием глобального характера угрозы и защитой цифрового суверенитета.

По своей природе киберпреступления не имеют границ. По мнению Н.А. Чернядьевой, о трансграничном характере говорит то, что киберпреступление не ограничено территориальными границами одного государства [3]. Преступник может находиться в одной стране, использовать серверы в другой, а ущерб наносить жертве в третьей. Таким образом, это делает невозможной эффективную борьбу с такими преступлениями в одиночку, без международного сотрудничества.

Так, в деле США против Карима Баратова, обвиняемый взломал аккаунты пользователей Yahoo (около 500 млн аккаунтов) и украл их личные данные, включая адреса электронной почты и номера телефонов. Хакер был арестован в Канаде. Затем киберпреступника экстрадировали в США. Федеральный суд Северного округа Калифорнии в Сан-Франциско приговорил гражданина Казахстана к 5 годам лишения свободы и штрафу в четверть миллиона.

Таким образом, в данном юридическом кейсе указаны базовые признаки преступлений транснационального характера, отображенные в ст. 3 Конвенции ООН против транснациональной организованной преступности 2000 г. в частности, киберпреступление совершено в одном государстве, но его существенные последствия имеют место в другом государстве.

Говоря о методах, которое предлагает наше государство в целях предотвращения киберпреступлений, то здесь выкристаллизовывается такая модель, при которой любое трансграничное взаимодействие должно идти через официальные запросы о правовой помощи. Например, следователь одной страны не может сам зайти на сервер в другой стране. Далее он должен направить запрос в компетентный орган (Генеральная прокуратура или МВД). Местные власти сами изымают данные и передают их запрашивающей стороне. Стоит отметить, что именно эта модель легла в основу проекта Конвенции ООН против киберпреступности.

Подход России относительно трансграничности заключается в том, что первичной является юрисдикция того государства, на чьей территории находится физическая инфраструктура (серверы) или где находится подозреваемый. Наша страна выступает против «экстерриториальной юрисдикции» (когда США или другие страны пытаются судить людей за действия, совершенные вне их территории, просто на основании того, что транзакция прошла через их банк или сервис).

В Конвенции ООН против киберпреступности от 2024 г., закреплены следующие принципы трансграничного сотрудничества, отображающие риторику нашего государства: уважение суверенитета; создание круглосуточных каналов связи (сети 24/7) для оперативной передачи данных, но под контролем национальных властей; четкий перечень оснований для отказа в выдаче данных (например, если это угрожает национальной безопасности).

Таким образом, трансграничность киберпреступлений – это повод для межгосударственного сотрудничества, а не для трансграничного вмешательства. Позиция Российской Федерации заключается в том, что сеть «Интернет» не является «ничейной землей», и каждое государство должно иметь полный контроль над своим сегментом киберпространства, взаимодействуя с соседями на основании соблюдения принципов международного права и соблюдения международных договоров.

Из всего вышесказанного полагаем логичным заключить следующее. Позиция Российской Федерации представляет собой суверенно-ориентированную концепцию, в которой технический прогресс и глобальный характер информационных сетей не должны превалировать над базовыми принципами международного права – суверенного равенства государств и невмешательства во внутренние дела.

Кроме того, Российский подход в части определения киберпреступления характеризуется максимальной широтой и универсальностью. В отличие от западной традиции, ограничивающей киберпреступление преимущественно атаками на компьютерные данные и системы, Россия настаивает на включении в это понятие широкого спектра сопутствующих преступлений. Данный тезис расширяет объект международно-правовой охраны, включая в него не только информационную безопасность, но и общественную безопасность, экономическую стабильность и государственный строй. Особое внимание к контентным преступлениям (экстремизм, терроризм, дезин-

формация) свидетельствует о стремлении Российской Федерации закрепить на международном уровне ответственность за использование ИКТ как инструмента политической и социальной дестабилизации.

Кроме того, Россия выступает против концепции трансграничного доступа к данным (ст. 32. b Будапештской конвенции), квалифицируя её как попытку легализации цифрового экспансионизма. Вместо этого предлагается модель «контролируемого сотрудничества», где трансграничное расследование возможно исключительно через механизмы взаимной правовой помощи и центральные государственные органы.

Российская Федерация формирует альтернативную парадигму международного информационного права, где борьба с киберпреступлениями является не поводом для создания прозрачного цифрового мира без границ, но инструментом укрепления межгосударственного взаимодействия на основе четкого соблюдения национальных юрисдикций и официальных процедур в рамках осуществления международно-правовой помощи.

Список литературы:

[1] Русинова В.Н. Международно-правовая квалификация вредоносного использования информационно-коммуникационных технологий: в поисках консенсуса // Московский журнал международного права. 2022. № 1. С. 38-51.

[2] Штодина Д.Д. Конвенция Организации Объединенных Наций против киберпреступности 2024 года – итог «киберкомпромисса»? // Московский журнал международного права. 2025. № 1. С. 110-124.

[3] Чернядьева Н.А. Цифровые технологии и права человека: эпоха взаимозависимости или кризис международной системы защиты прав человека? // Правопорядок: история, теория, практика. № 2 (37) / 2023. С. 164 – 172.

References:

[1] Rusinova V.N. International legal qualification of the malicious use of information and communication technologies: in search of consensus//Moscow Journal of International Law. 2022. № 1. S. 38-51.

[2] Stodina D.D. United Nations Convention against Cybercrime 2024 - the result of “cyber compromise” ?//Moscow Journal of International Law. 2025. № 1. S. 110-124.

[3] Chernyadyeva N.A. Digital technologies and human rights: the era of interdependence or the crisis of the international system for the protection of human rights ?//Law and order: history, theory, practice. № 2 (37) / 2023. S. 164-172.