

КРИМИНАЛИСТИКА И КРИМИНОЛОГИЯ. СУДЕБНАЯ ЭКСПЕРТИЗА

DOI: 10.17803/1994-1471.2026.188.7.122-134

А. Н. Халиков*

Проблемы правовой основы международного взаимодействия для выявления и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий

Аннотация. Киберпреступления составляют одну из актуальных внутренних и внешних проблем государства, борьба с которыми требует новых правовых и технических способов защиты от преступных посягательств в цифровом пространстве. В то же время киберпреступления носят в основном международный характер, успешная борьба с ними может идти только при тесном взаимодействии всех государств и их правоохранительных органов. Правовой основой такого взаимодействия является принятая в 2001 г. Будапештская конвенция, посвященная борьбе с киберпреступлениями, которая объединяет более 80 государств. Однако Россия вышла из работы по данной Конвенции вследствие норм, затрагивающих суверенитет нашей страны. Вместе с тем Россией и рядом других государств предложен новый проект конвенции по борьбе с киберпреступлениями, где предусмотрены новые, более эффективные механизмы взаимодействия правоохранительных органов государств, правовые и технические меры по борьбе с киберпреступлениями на современном уровне. В статье анализируется содержание данного проекта конвенции и его соотношения с Будапештской конвенцией и прогнозируются пути применения обоих международных актов.

Ключевые слова: Интернет; информационно-коммуникационные технологии; киберпреступления; конвенция; международное взаимодействие; международное расследование; правоохранительные органы; преступления; следственные действия; трафик; цифровое пространство

Для цитирования: Халиков А. Н. Проблемы правовой основы международного взаимодействия для выявления и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий // Актуальные проблемы российского права. — 2026. — Т. 21. — № 7. — С. 122–134. — DOI: 10.17803/1994-1471.2026.188.7.122-134

© Халиков А. Н., 2026

* Халиков Аслям Наилевич, доктор юридических наук, профессор, профессор кафедры криминалистики Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева, профессор кафедры криминалистики Института права Уфимского университета науки и технологий ул. Врубеля, д. 12, г. Москва, Российская Федерация, 125080 han010@yandex.ru

Legal Framework Challenges in International Cooperation for the Investigation of Cybercrimes

Aslyam N. Khalikov, Dr. Sci. (Law), Professor, Professor, Department of Forensic Science, Moscow Academy of the Investigative Committee of the Russian Federation named after A.Ya. Sukharev, Professor, Department of Forensic Science, Institute of Law, Ufa University of Science and Technology, Moscow, Russian Federation
han010@yandex.ru

Abstract. Cybercrime is one of the most urgent domestic and foreign policy challenges facing the modern state. Counteracting the crime requires new legal and technical safeguards against criminal activity in the digital domain. At the same time, cybercrime is primarily international in nature; successfully combating such can only be achieved through close cooperation between all states and their law enforcement agencies. The prevailing legal framework for such cooperation is the 2001 Budapest Convention on Cybercrime, which now comprises over 80 member states. However, Russia has withdrawn from the Convention, citing provisions that it considers incompatible with its national sovereignty. In response, Russia and several other states have put forward a new draft convention on combating cybercrime, which envisions more effective mechanisms for interstate law enforcement cooperation, as well as up-to-date legal and technical countermeasures. The paper examines the content of the proposed draft convention, compares it with the Budapest Convention, and explores the potential scenarios for the implementation of both international instruments

Keywords: Internet; information and communication technologies; cybercrime; convention; international cooperation; international investigation; law enforcement; crimes; investigative actions; traffic; digital space

Cite as: Khalikov AKh. Legal Framework Challenges in International Cooperation for the Investigation of Cybercrimes. *Aktual'nye problemy rossijskogo prava*. 2026;21(7):122-134. (In Russ.). DOI: 10.17803/1994-1471.2026.188.7.122-134

Информационно-коммуникационные технологии (ИКТ) составляют материально-интеллектуальную сферу сегодняшнего мира, ее наиболее активную часть в области политики, экономики, социального общения, сферу цифрового пространства. Этот виртуальный мир не имеет четкой локализации и строгих границ между государствами, что в целом положительно сказывается на обеспечении свободы мирового сообщества, трудовой и научной деятельности, многообразии международных коммуникаций. Однако в цифровой сфере происходит быстрая эволюция криминальных явлений, что заставляет говорить о негативных и опасных тенденциях развития современных компьютерных технологий в преступном мире, которые в силу своего совершенства, ускорения и масштабов существенно влияют на рост преступности, вплоть до угроз внутренней и внешней безопасности государств с учетом взаимосвязанности цифровых технологий и ядерного потенциала

стран¹. При этом как на внутреннем уровне, так и на внешнем, то есть в сфере международных отношений, сегодня крайне слаба техническая, правовая, оперативная защита компьютерных технологий от криминальных посягательств.

В противоположность динамичному развитию преступности с применением ИКТ, международных механизмов совершения и сокрытия преступлений, о чем свидетельствуют многомиллиардные хищения дистанционного формата в России и международные хакерские атаки, в настоящее время недостаточно разработаны действенные правовые механизмы выявления, раскрытия, пресечения и расследования противоправных деяний в сфере компьютерной информации в трансграничном пространстве. Причины такого положения заключаются как в состоянии современных международных отношений, так и в правовом нигилизме при построении сотрудничества в сфере международного уголовного права. В результате возникает про-

¹ См.: Аббуд Р. Р. Международно-правовое регулирование противодействия киберпреступлениям : дис. ... канд. юрид. наук. М., 2025. С. 163–170.

тиворечие между быстрой эволюцией киберпреступлений на межгосударственном уровне и дефицитом правового регулирования и международного взаимодействия по борьбе с этими преступлениями.

Начиная с конца XX в. такие международные организации, как ООН, Совет Европы, ШОС, ОДКБ, озаботились совершением первых киберпреступлений, связанным с интенсивным развитием ИКТ в мире. Были приняты соответствующие международные акты, которые сыграли определенную роль в противодействии криминалу в компьютерной сфере, хотя и не остановили его рост. Причем вряд ли следует разделять киберпреступления и компьютерные преступления, как предлагает М. А. Дубко, поскольку фактически одно без другого в большинстве случаев невозможно².

Одним из первых нормативных актов, направленных на борьбу с киберпреступностью, стала Рекомендация от 13.09.1989 № R89(9) Комитета Министров стран — членов Совета Европы о преступлениях, связанных с использованием компьютера, где практически впервые были определены преступления с использованием компьютерных технологий по 12 составам³. Далее, наиболее полной стала действующая на сегодняшний день Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве), принятая в г. Будапеште 23 ноября 2001 г. В этой Конвенции закреплено девять наименований преступлений, разрабо-

таны основы международного сотрудничества между странами по выявлению и пресечению киберпреступлений в уголовно-правовой и уголовно-процессуальной сферах⁴. Вопросы киберпреступности частично стали предметом содержания Конвенции ООН против транснациональной организованной преступности, принятой Генеральной Ассамблеей ООН 15 ноября 2000 г. Следует отметить Арабскую конвенцию о борьбе с преступлениями в сфере информационных технологий от 21.12.2010 и Конвенцию Африканского союза о кибербезопасности и защите персональных данных от 27.06.2014. По линии СНГ было подписано второе Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28.09.2018⁵. Существуют и другие локальные и международные акты, полностью или частично посвященные борьбе с киберпреступлениями в межгосударственной сфере⁶.

Как мы указали, наиболее универсальной и с широким участием других государств стала Европейская конвенция по киберпреступлениям 2001 г. (г. Будапешт). На сегодняшний день, кроме стран Совета Европы, документ ратифицировали 45 государств всех континентов, включая США, что в целом образует 81 государство. В России названная Конвенция вступила в силу в соответствии с распоряжением Президента РФ от 15.11.2005⁷, однако затем Россия вышла из Конвенции. Причиной выхода стала возмож-

² Дубко М. А. Международное сотрудничество в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией // Вестник Полоцкого государственного университета. Серия D. Экономические и юридические науки. 2012. № 14. С. 180–183.

³ См.: Швед Н. А. Сравнительный анализ уголовной ответственности за несанкционированный доступ к компьютерной информации в странах ЕС // Вестник Нижегородского университета имени Н.И. Лобачевского. 2016. № 5. С. 222.

⁴ Шестак В. А., Чеботарь А. С. Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования // Образование и право. 2023. № 8. С. 305–310.

⁵ URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/multilateral_contract/53417/.

⁶ См.: Мороз Н. О. Международно-правовые основы обеспечения международной информационной безопасности // Труд. Профсоюзы. Общество. 2016. № 1 (51). С. 77–81.

⁷ Распоряжение Президента Российской Федерации от 15.11.2005 № 557-рп «О подписании Конвенции о киберпреступности» // СЗ РФ. 2005. № 47. Ст. 4929.

ность доступа иностранных спецслужб и других правительственных организаций к ИКТ России исходя из положений дополнительных протоколов к Конвенции, что могло серьезно подорвать суверенитет России⁸.

Вместе с тем Будапештская конвенция по своей структуре и содержанию наиболее полно отразила уголовно-правовые, процессуальные и международно-правовые проблемы киберпреступности и наметила реальные шаги международного сотрудничества государств по противодействию в этой сфере. Конвенция заложила основы международных действий правоохранительных органов государств для получения взаимной процессуальной и оперативной информации, пресечения, раскрытия и расследования киберпреступлений, в связи с чем документ получил положительный отклик в научном мире⁹.

В то же время с момента принятия Будапештской конвенции прошло более 20 лет, за это время изменились и технические, и политические, и правовые условия действия Конвенции, тем более что крупнейшая страна в мире — Россия — не участвует в ней. Но главным недостатком Будапештской конвенции стала ее неэффективность ввиду развития современных компьютерных преступлений, требующих новых технологических и правовых методов реагирования, способов взаимодействия участников Конвенции. Данные обстоятельства позволили России и ряду других государств на международном уровне в рамках Организации Объединенных Наций предложить более совершенный вариант конвенции против киберпреступности, предусматривающий создание действенных механизмов международного сотрудничества в борьбе

с преступлениями, совершаемыми с использованием информационно-коммуникационных систем и обмена доказательствами¹⁰. И 24 декабря 2024 г. Генеральная Ассамблея Организации Объединенных Наций приняла проект конвенции против киберпреступности (далее — проект Конвенции, Конвенция)¹¹. В дальнейшем, осенью 2025 г., эту Конвенцию планируется подписать членами ООН в г. Ханое (Вьетнам), после чего должен начаться процесс ее ратификации подписавшими государствами¹².

Значимость новой Конвенции против киберпреступности — в ее правовом и техническом совершенстве, введении новых методических и тактических способов и приемов в деятельность правоохранительных органов по борьбе с преступлениями в области ИКТ. Наравне с аналогичными международными актами по борьбе с отдельными видами преступлений — Конвенцией ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ (1988), Конвенцией ООН о борьбе с финансированием терроризма (1999), Конвенцией ООН против коррупции (2003) и другими — рассматриваемая Конвенция не только носит специальный характер (борьба с киберпреступлениями), но и по своей сути направлена на противодействие другим преступлениям, совершаемым в киберпространстве.

Если говорить о политической стороне конструирования и принятия новой Конвенции, то инициатором ее разработки в рамках структуры ООН, как мы отметили, стала Российская Федерация в 2017–2024 гг. Причем западные страны, такие как США, Великобритания и другие, были против многих положений данного международного документа, в связи с чем шли

⁸ См.: Кириленко В. П., Алексеев Г. В. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы // Всероссийский криминологический журнал. 2020. Т. 14. № 6. С. 898–913.

⁹ Волеводз А. Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. 2007. № 2. С. 17–25.

¹⁰ Конвенция Организации Объединенных Наций против киберпреступности (2025) // URL: <https://www.un.org/ru/documents>.

¹¹ URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243>.

¹² См.: Горелик И. Б. Формирование международно-правовой системы противодействия киберпреступности: от терминологии до проекта универсальной конвенции // Международное право. 2022. № 4. С. 60–71.

довольно долгие дискуссии не только о содержании Конвенции, но и о правомерности ее создания в целом. Как пишет Э. Чернухин, вследствие негативной позиции западных стран из проекта Конвенции выпали положения о противодействии использованию информационно-коммуникативных систем в террористических и экстремистских целях, для незаконного оборота наркотиков и оружия, доведения детей до самоубийства, а также о защите объектов критической информационной инфраструктуры¹³. В то же время, соглашаясь с мнением об острой необходимости существования рассматриваемой Конвенции против киберпреступности, полагаем, что у западных стран были свои причины отчасти критически подходить к некоторым ее положениям. Речь может идти о свободе информации; использовании положений Конвенции в целях излишних запретов общения между людьми в мировом пространстве посредством сети Интернет; избыточной активности спецслужб, направленной не на выявление и раскрытие конкретных преступлений, а на борьбу с политическими преступлениями, неоднозначно оцениваемыми в странах Запада и Востока. Всё это могло и может иметь негативные характеристики при соотношении соблюдения прав и интересов человека с развитием информационно-коммуникационных систем в международном масштабе, препятствовать взаимодействию правоохранительных органов по борьбе с названными преступлениями. Таким образом, проект новой Конвенции по киберпреступности, удаляясь от политической тематики, должен находить свою реализацию в решении наиболее актуальных проблем противодействия совершению компьютерных и общеуголовных преступлений с применением ИКТ, точно выявлять, раскрывать и пресекать наиболее тяжкие и особо тяжкие криминальные деяния, связанные с компьютерными технологиями.

По мнению П. А. Литвишко, Будапештская конвенция против киберпреступности и проект новой Конвенции фактически образуют конкуренцию в международных правоотношениях по противодействию преступлениям в сфере компьютерных технологий¹⁴. Это действительно имеет место, поскольку основные положения двух конвенций дублируют друг друга. Несомненно, проект Конвенции, предложенный Россией, носит более качественный характер, детально регламентируя многие вопросы взаимодействия правоохранительных органов, механизмы производства международных следственных и оперативно-разыскных действий, технические параметры блокирования и пресечения преступлений в компьютерной сети и иные позиции.

Вместе с тем нельзя игнорировать и участие более 80 стран в структуре Будапештской конвенции с учетом суверенной позиции каждого из государств, присоединившихся к Конвенции с 2001 г. Такая ситуация может привести к существованию одновременно двух конвенций против киберпреступности, что хотя и создаст ряд правовых и политических коллизий, однако не станет критическим фактором в борьбе с названными преступлениями. Более того, так как любая монополия несет больше негативного, чем положительного, конкурирование двух правовых систем в сфере борьбы с компьютерными преступлениями может одновременно создавать и эффективные зоны взаимодействия по действующим конвенциям, вводить дополнительный контроль за методами и способами выявления и расследования преступлений в данной сфере, привлечет большее количество государств, заинтересованных в обеспечении коллективной безопасности от киберпреступлений. Дело в том, что область киберпреступлений — это часть виртуального (или цифрового) пространства, называемая иногда киберпростран-

¹³ Чернухин Э. Об истории создания и итогах работы специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях // Международная жизнь. 2025. № 2. С. 111.

¹⁴ Литвишко П. А. Первый глобальный договор против киберпреступности: от геополитической конфронтации к профессиональному компромиссу // Международная жизнь. 2024. № 11. С. 1–27.

ством, которая сегодня фактически является параллельной реальностью мира, в котором мы физически существуем. Глубина и потенциал ИКТ больше, чем ученые в состоянии себе представить, в этих технологиях еще много неизведанного. И когда в этой области происходит неконтролируемое посягательство на информационную систему человеческой деятельности с помощью компьютерных средств или киберинструментов, создается реальная угроза исчезновения значительной части информации, тогда, исходя из здравого смысла, избыток правовых механизмов борьбы с такими общественно опасными тенденциями предпочтительнее, чем их недостаток. Из этого следует, что как Будапештская конвенция, так и проект новой Конвенции от имени Российской Федерации направлены если не на ликвидацию киберпреступлений (это в идеале), то на достижение состояния разумного баланса сдерживания активности криминальной части ИКТ в мировом пространстве, что допускает взаимное существование в определенный период двух конвенций против киберпреступности.

Проект новой Конвенции начинается с преамбулы, где подчеркивается важность борьбы с киберпреступлениями вследствие огромного потенциала ИКТ и его системного развития при совершении разнообразных преступлений, масштабов организованной и транснациональной преступности, использующей ИКТ, необходимость глобальной международной политики против киберпреступности, а также необходимость международного преследования преступников, совершающих киберпреступления или использующих ИКТ. Одновременно в Конвенции подчеркнута необходимость решения задач правоприменения, уважения прав человека и основных свобод с защитой от произвольного и незаконного вмешательства в частную жизнь людей.

Учитывая четко выраженную ориентацию целей и задач борьбы с киберпреступлениями, обозначенную в преамбуле Конвенции, и ее соотношение с правами и интересами человека, в первую очередь подразумевается необходимость свободы киберпространства, а следовательно, ресурсов Интернета, но за исключением

совершения криминальных деяний в цифровом пространстве. Иными словами, в соотношении количества преступлений и преступников в сфере ИКТ, составляющих единицы от всей массы населения государств, борьба с киберпреступлениями должна быть направлена на обеспечение нормального и свободного функционирования ИКТ и интернет-ресурсов, а не их запрет или ограничение, что нарушает права и свободы человека и общества, а значит, не отвечает задачам борьбы с преступностью.

Первая глава (ст. 1–6) указывает на правовые цели Конвенции, которые исходят из содержания ее преамбулы. Приводятся основные технические и правовые термины, обозначается сфера применения, перечисляются преступления, признаваемые таковыми в соответствии как с рассматриваемой Конвенцией, так и с другими конвенциями по борьбе с преступлениями, если они совершаются с использованием ИКТ. Отдельно выделяются нормы о защите суверенитета государств в ходе борьбы с киберпреступлениями и соблюдении при этом прав человека.

Глава вторая (ст. 7–21) посвящена вопросам криминализации деяний при применении ИКТ. К международным составам киберпреступлений отнесены:

- 1) незаконный доступ к ИКТ, включая соединения с другой информационно-коммуникационной системой;
- 2) незаконный перехват передач электронных данных в системе ИКТ;
- 3) воздействие на электронные данные в виде их повреждения, удаления, порчи, изменения или блокирования;
- 4) воздействие на информационно-коммуникационную систему;
- 5) неправомерное использование устройств ИКТ в виде приобретения, ввоза, распространения или предоставления иным способом;
- 6) подлог с применением информационно-коммуникативной системы, приводящий к возникновению неаутентичных данных, используемых в качестве аутентичных;
- 7) мошенничество или извлечение денежной либо имущественной выгоды с использованием информационно-коммуникационной системы;

8) преступления, связанные с размещением в Интернете материалов со сценами сексуальных надругательств над детьми (не достигшими 18-летнего возраста) или их сексуальной эксплуатации;

9) домогательство или создание доверительных отношений с целью совершения сексуального преступления в отношении ребенка;

10) распространение интимных изображений без согласия лиц старше 18 лет и особые условия для лиц, не достигших возраста 18 лет;

11) отмыwanie доходов от преступлений в самом широком диапазоне понимания данного правонарушения при совершении всех вышеперечисленных преступлений.

Представленные составы преступлений можно разделить на четыре группы: 1) киберпреступления или преступления в сфере ИКТ; 2) мошенничество или иные виды хищений с применением ИКТ; 3) сексуальные посягательства с использованием ИКТ; 4) отмыwanie незаконных доходов при совершении перечисленных преступлений.

Здесь речь идет о преступлениях международного характера или конвенционных преступлениях, посягающих на стабильные позитивные отношения между странами, наносящих ущерб мирной кооперации в разных сферах, а также организациям и гражданам, наказуемых по нормам, установленным в международных соглашениях, либо нормам внутригосударственного уголовного права в соответствии с этими соглашениями¹⁵. Кроме этого, Конвенция предполагает необходимость определения ответственности юридических лиц, понятий участия и покушения по вышеназванным видам преступлений, критериев для установления более продолжительных сроков давности при перечисленных в ней криминальных деяниях.

Как мы указали, исключение из данных составов деяний с политическими или экстремистскими конструкциями при современном диапазоне различия политических и социально-экономических режимов государств является

вполне оправданным. В то же время, отрицая политические составы, традиционно вместе с водой выплеснули и ребенка. На наш взгляд, в данном перечне преступлений, часто подготавливаемых, совершаемых и затем скрываемых, отсутствует такое наиболее тяжкое общественно опасное деяние, как убийство, которое всё же нужно было бы назвать, если оно совершено с применением механизма ИКТ. Априори убийство всё же более опасно, чем сексуальное насилие, если в последнем случае человек остается живым. При наличии посягательства на жизнь человека речь может идти о его похищении, безвестном исчезновении, использовании его органов и т.д., что сегодня совершается в подавляющем большинстве случаев с применением электронных средств связи и компьютерных технологий. Соответственно, нормы Конвенции как наиболее эффективные при антикриминальной деятельности и антикриминальном анализе состояния современного информационного пространства должны использоваться при защите основного права человека на жизнь, что стоило бы отразить в рассматриваемом документе в качестве серьезного преступления.

Глава третья (ст. 22) устанавливает традиционные нормы юрисдикции, относящиеся к территории и лицам по делам о киберпреступлениях в условиях взаимодействия между государствами.

В главе четвертой (ст. 23–34) изложены процессуальные меры и способы правоприменения при осуществлении уголовных расследований и судебных разбирательств по преступлениям, указанным в Конвенции, другим уголовным правонарушениям, совершаемым с помощью ИКТ, сбора доказательств в электронной форме, относящихся к любым преступлениям. Представлены условия и гарантии обеспечения прав человека, включая право на защиту.

Со статьи 25 начинаются положения Конвенции, направленные на криминалистическое и оперативное обеспечение выявления, раскрытия и расследования киберпреступлений с

¹⁵ Международное уголовное право : учебник для бакалавриата и магистратуры / А. В. Наумов, А. Г. Кибальник, В. Н. Орлов, П. В. Волосюк / под ред. А. В. Наумова, А. Г. Кибальника. 2-е изд., перераб. и доп. М. : Юрайт, 2014. С. 277–278.

регламентацией основных технических способов борьбы с ними. Конвенция регулирует оперативное обеспечение сохранности хранимых электронных данных и трафика в государствах-участниках, поскольку эти данные «особенно подвержены риску утраты и изменения». Здесь важно отметить, что в Российской Федерации эта проблема решена на законодательном уровне. С 2017 г., согласно ст. 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации»¹⁶, организатор распространения информации в сети Интернет обязан хранить на территории РФ любую информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение трех лет с момента окончания осуществления таких действий. А текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения — до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Эти положения дублируются в ст. 64 Федерального закона «О связи»¹⁷, они относятся ко всем операторам связи.

Сроки хранения сведений, голосовой и текстовой информации должны быть синхронизированы по правилам названной Конвенции. Однако не исключено, что другие страны регламентируют сроки хранения разнообразной цифровой информации по аналогии с российским законодательством, что будет составлять единый международный стандарт сохранения электронной информации.

Далее говорится об оперативном обеспечении сохранности и частичном раскрытии данных о трафике с возможностью обеспечения полномочий компетентных органов давать распоряжения о предоставлении информации. Данные о трафике, исходя из ст. 2 Конвенции, означают любые электронные данные, которые относятся

к сообщению, осуществляемому посредством информационно-коммуникационной системы, генерируются информационно-коммуникационной системой, являющейся составной частью коммуникационной цепочки, и указывают на источник, адресат, маршрут, время, дату, размер и продолжительность сообщения или тип базовой услуги.

Перечисленные действия по раскрытию и расследованию киберпреступлений обеспечиваются рядом следственных и процессуальных действий международного характера. В этой части Конвенцией предусмотрены правила обыска и изъятия хранимых электронных данных с возможностью сбора в режиме реального времени сведений о трафике, перехвата данных о содержании любых сообщений с помощью ИКТ, введены условия замораживания, ареста и конфискации доходов от преступлений. Правила производства обысков, получения сведений о трафике, перехвата данных о содержании, ареста и конфискации доходов от преступлений впервые в Конвенции подобного направления изложены с учетом взаимовыгодного сотрудничества между компетентными органами государств, проведения совместных следственно-оперативных мероприятий и с изъятием объектов, представляющих обоюдный интерес. В этом плане отдельно выделены нормы о взаимном обмене информацией о судимостях с получением судебных приговоров, правила защиты свидетелей и потерпевших.

Из Конвенции становится ясно, что при осуществлении перечисленных и иных процессуальных и следственных действий правоохранительные органы должны руководствоваться национальным уголовно-процессуальным законодательством. Думается, что, ввиду наличия единых стандартов норм о защите прав и интересов гражданина и человека, основывающихся на международных актах ООН, не будет возникать неразрешимых коллизий при производстве процессуальных и оперативных действий правоохранительных органов различных госу-

¹⁶ Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

¹⁷ Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. Ст. 2895.

дарств. Однако при производстве следственных действий на территории других государств либо получении информации из других государств должно быть исключено нарушение их суверенитета, о чем велись дискуссии при обсуждении Конвенции. В этой части следует назвать новый состав преступления, введенный Федеральным законом от 31.07.2025 № 282-ФЗ¹⁸, которым предусмотрена уголовная ответственность по ст. 294.1 УК РФ за незаконное осуществление следственных, иных процессуальных действий и оперативно-разыскных мероприятий на территории РФ.

Глава 5 (ст. 35–53) содержит нормы об общих принципах международного сотрудничества и защиты персональных данных согласно национальному законодательству. Подробно изложены правила выдачи преступников с их арестом или без такового, а также норма о выдаче осужденных. Тем не менее вызывает сомнение положение, разрешающее выдачу гражданина страны другой стране, хотя и с гарантиями справедливого правосудия и возврата гражданина обратно. В первую очередь оно противоречит ст. 61 Конституции РФ, указывающей, что «гражданин Российской Федерации не может быть выслан за пределы Российской Федерации или выдан другому государству». Считаем, что это положение не нуждается в широком толковании о возможностях временной выдачи гражданина России. Излишние условия о выдаче преступника — с гарантиями или без них — в любом случае будут нарушать конституционную норму. Здесь должны включаться иные механизмы следственного и оперативного сотрудничества, например расследование на территории другого государства с применением норм УПК РФ и положений Конвенции либо порядок передачи уголовного производства другой стране, что также предусмотрено Конвенцией.

В Конвенции наиболее полно представлена норма об общих принципах и процедурах взаимной правовой помощи по международному обмену при расследовании преступлений (ст. 40). Предполагается, что государства-участ-

ники оказывают друг другу самую широкую взаимную правовую помощь в расследовании, уголовном преследовании и судебном разбирательстве по преступлениям, признанным таковыми в соответствии с Конвенцией, а также сборе доказательств в электронной форме о преступлениях согласно Конвенции и иных серьезных преступлениях.

В Конвенции перечислены процессуальные мероприятия, а фактически следственные действия, которые могут быть проведены при сотрудничестве нескольких государств. В этом перечне получение показаний, проведение обыска, сбор в режиме реального времени данных о трафике, предоставление информации, доказательств и заключений экспертов, представление подлинников или заверенных копий соответствующих документов и материалов, выявление или отслеживание доходов от преступлений, оказание любого иного вида помощи, не противоречащего внутреннему законодательству запрашиваемого государства-участника, а также передача необходимой информации без запросов, но с соблюдением интересов другого государства. Новацией в описываемом перечне процессуальных действий стало положение о временной выдаче лица для целей расследования в другом государстве с учетом типичных правовых гарантий обеспечения его прав и возврата выдавшему государству. Данное правило, как мы указали выше, требует дополнительного обсуждения, даже принимая во внимание предложенные правовые гарантии, ввиду известного конституционного запрета о выдаче своих граждан. И в этом смысле актуальны нормы Конвенции об основаниях и правилах отказа в правовой помощи в случае негативных обстоятельств для запрашиваемой стороны.

Отдельные положения Конвенции ориентированы на сотрудничество между правоохранительными органами, включая каналы Международной организации уголовной полиции, с целью поиска лиц, имущества и доходов от преступлений, проведение совместных расследований по соглашению в отдельных случаях.

¹⁸ Федеральный закон от 31.07.2025 № 282-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2025. № 31. Ст. 4636.

Введены механизмы возвращения имущества путем международного сотрудничества в деле конфискации.

Наиболее значимыми являются нормы о создании постоянного режима работы национальных и международных правоохранительных служб по борьбе с киберпреступлениями. В этом направлении для оперативного взаимовыгодного сотрудничества введена статья 41 с характерным наименованием «24/7» о необходимости образования и деятельности круглосуточных контактных центров в странах — участниках Конвенции с соответствующими полномочиями согласно положениям Конвенции.

На наш взгляд, важно создать не только контактные центры в отдельных государствах, но и единый международный центр по борьбе с киберпреступлениями (далее — Центр) по аналогии, например, с Интерполом, но с более эффективными средствами правоохранительной деятельности в киберпространстве. Масштаб и глубина работы такого Центра будут носить глобальный характер в рамках Конвенции и внутреннего процессуального регламента. В функции Центра должны входить оперативный обмен информацией между странами в режиме реального времени, обнаружение денежных потоков между банками и государствами и пресечение незаконной деятельности, блокирование компьютерных и иных связей между пользователями сети Интернет и иными средствами связи, выдача указаний об остановке работы средств связи или ограничении потребления электроэнергии. Центр будет обеспечивать международное сотрудничество и взаимную правовую помощь в целях оперативного обеспечения сохранности хранимых электронных данных, оперативного представления сохраненных данных о трафике, перехвата данных о содержании. Основным преимуществом работы Центра и выполнения перечисленных мероприятий будет его деятельность в режиме реального времени.

Заключительные главы Конвенции носят больше организационный характер. Шестая глава посвящена мерам по предупреждению киберпреступлений. Седьмая устанавливает нормы об осуществлении технической помощи между государствами и наращивании потенциа-

ла, возможности обмена информацией. Восьмая глава решает организационные вопросы исполнения Конвенции, такие как учреждение конференции государств — участников Конвенции и обслуживание Конвенции отдельным секретариатом. В последней, девятой главе говорится об осуществлении и действии Конвенции между государствами; взаимном обмене протоколами; процедурах урегулирования споров, подписания, ратификации, принятия, утверждения и присоединения к Конвенции; вступлении ее в силу и возможных поправках.

Изложенное содержание проекта новой Конвенции по борьбе с киберпреступлениями позволяет говорить, что в ней отражены наиболее острые современные направления борьбы с криминальными явлениями в области ИКТ при эффективном взаимодействии правоохранительных органов государств. В данном случае целесообразно создание единого международного Центра по выявлению, раскрытию, пресечению и расследованию таких преступлений, работающего в режиме 24/7, который стал бы координирующей системой с функциями электронного аккумулирования всей криминальной информации по киберпреступлениям и полицейского расследования.

Возможен ли реальный межгосударственный масштаб такой оперативной и следственной деятельности уголовно-правового направления с учетом современного уровня международных отношений? На первый взгляд, это трудно представить. Несмотря на единое киберпространство при совершении преступлений с использованием ИКТ, мир традиционно разделяется на блоки, союзы, альянсы, что не способствует борьбе с такими преступлениями. Однако проблема борьбы с киберпреступлениями становится острее с каждым днем при условной невидимости этих криминальных деяний и реальном ущербе, ими причиняемом. Изохронные хакерские атаки, дистанционные хищения, измеряемые в миллиардных показателях, активность БПЛА, не говоря уже об общеуголовных преступлениях, — всё это активизируется на фоне совершенствования ИКТ в криминальных целях.

Подлинная борьба с киберпреступлениями в системном режиме еще не развернулась. И при

такой ситуации создание международного Центра борьбы с киберпреступлениями и начало его работы будет новой ступенью эффективного противостояния государства в цифровом пространстве. Иными словами, в силу необходимости борьбы с киберпреступлениями, которые имеют исключительно транснациональный характер, наличие постоянно действующего рабочего органа в этой сфере является обязательным¹⁹. Исходя из норм Конвенции предполагается тесная взаимосвязь такого Центра с международными полицейскими организациями — Интерполом, Европолом, Америкой — на уровне информационного и административно-оперативного взаимодействия. При таком Центре должны работать следственный и оперативный аппарат, экспертные службы, подразделения процессуального и международно-правового контроля²⁰. Думается, что подобному Центру понадобятся космические спутники и спутники стратосферной платформы на региональном уровне с функциями фиксации и пресечения деяний с признаками киберпреступлений, от дистанционных хищений и до

масштабных хакерских атак или воздействий на критическую информационную инфраструктуру.

Завершая наши суждения, отметим, что предлагаемый проект Конвенции по борьбе с киберпреступлениями может стать объединяющим документом для большинства государств, заменить или дополнить европейские, азиатские, африканские и другие соглашения локального характера, которые при современном состоянии ИКТ в целом не справляются с задачами борьбы с преступлениями в данной сфере. И в этом аспекте повторим главную мысль, что борьба с киберпреступлениями, преступлениями в компьютерной области возможна только в режиме реального времени, когда само преступление совершается в секунды и доли секунд. И проект Конвенции предлагает наиболее эффективный на сегодня способ такой борьбы — создание международного Центра борьбы с киберпреступлениями, обеспечение его деятельности совокупностью следственных, оперативных и процессуальных действий с учетом национальных и международных интересов государств.

БИБЛИОГРАФИЯ

1. Аббуд Р. Р. Международно-правовое регулирование противодействия киберпреступлениям : дис. ... канд. юрид. наук. — М., 2025.
2. Волеводз А. Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. — 2007. — № 2. — С. 17–25.
3. Горелик И. Б. Возможные направления развития международно-правовых институтов в области обеспечения глобальной кибербезопасности // Международное право. — 2023. — № 2. — С. 33–44.
4. Горелик И. Б. Формирование международно-правовой системы противодействия киберпреступности: от терминологии до проекта универсальной конвенции // Международное право. — 2022. — № 4. — С. 60–71.
5. Дубко М. А. Международное сотрудничество в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией // Вестник Полоцкого государственного университета. Серия D. Экономические и юридические науки. — 2012. — № 14. — С. 180–183.
6. Кириленко В. П., Алексеев Г. В. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы // Всероссийский криминологический журнал. — 2020. — Т. 14. — № 6. — С. 898–913.

¹⁹ См.: Лепешкина О. И. Международное сотрудничество государств СНГ по противодействию киберпреступности // Евразийская интеграция: экономика, право, политика. 2023. Т. 17. № 4. С. 82–91.

²⁰ См.: Горелик И. Б. Возможные направления развития международно-правовых институтов в области обеспечения глобальной кибербезопасности // Международное право. 2023. № 2. С. 33–44.

7. Лепешкина О. И. Международное сотрудничество государств СНГ по противодействию киберпреступности // Евразийская интеграция: экономика, право, политика. — 2023. — Т. 17. — № 4. — С. 82–91.
8. Литивишко П. А. Первый глобальный договор против киберпреступности: от геополитической конфронтации к профессиональному компромиссу // Международная жизнь. — 2024. — № 11. — С. 1–27.
9. Международное уголовное право : учебник для бакалавриата и магистратуры / А. В. Наумов, А. Г. Кибальник, В. Н. Орлов, П. В. Волосяк / под ред. А. В. Наумова, А. Г. Кибальника. — 2-е изд., перераб. и доп. — М. : Юрайт, 2014. — 510 с.
10. Мороз Н. О. Международно-правовые основы обеспечения международной информационной безопасности // Труд. Профсоюзы. Общество. — 2016. — № 1 (51). — С. 77–81.
11. Чернухин Э. Об истории создания и итогах работы специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях // Международная жизнь. — 2025. — № 2. — С. 108–113.
12. Швед Н. А. Сравнительный анализ уголовной ответственности за несанкционированный доступ к компьютерной информации в странах ЕС // Вестник Нижегородского университета имени Н.И. Лобачевского. — 2016. — № 5. — С. 222–226.
13. Шестак В. А., Чеботарь А. С. Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования // Образование и право. — 2023. — № 8. — С. 305–310.

Материал поступил в редакцию 17 сентября 2025 г.

REFERENCES (TRANSLITERATION)

1. Abbud R. R. Mezhdunarodno-pravovoe regulirovanie protivodeystviya kiberprestupleniyam: dis. ... kand. yurid. nauk. — M., 2025.
2. Volevodz A. G. Konventsiya o kiberprestupnosti: novatsii pravovogo regulirovaniya // Pravovye voprosy svyazi. — 2007. — № 2. — S. 17–25.
3. Gorelik I. B. Vozmozhnye napravleniya razvitiya mezhdunarodno-pravovykh institutov v oblasti obespecheniya globalnoy kiberbezopasnosti // Mezhdunarodnoe pravo. — 2023. — № 2. — S. 33–44.
4. Gorelik I. B. Formirovanie mezhdunarodno-pravovoy sistemy protivodeystviya kiberprestupnosti: ot terminologii do proekta universalnoy konventsii // Mezhdunarodnoe pravo. — 2022. — № 4. — S. 60–71.
5. Dubko M. A. Mezhdunarodnoe sotrudnichestvo v sfere ugovovno-pravovoy borby s nepravomernym zavladeniem kompyuternoy informatsiyey // Vestnik Polotskogo gosudarstvennogo universiteta. Seriya D. Ekonomicheskie i yuridicheskie nauki. — 2012. — № 14. — S. 180–183.
6. Kirilenko V. P., Alekseev G. V. Garmonizatsiya rossiyskogo ugovovnogo zakonodatelstva o protivodeystvii kiberprestupnosti s pravovymi standartami Soveta Evropy // Vserossiyskiy kriminologicheskiy zhurnal. — 2020. — T. 14. — № 6. — S. 898–913.
7. Lepeshkina O. I. Mezhdunarodnoe sotrudnichestvo gosudarstv SNG po protivodeystviyu kiberprestupnosti // Evraziyskaya integratsiya: ekonomika, pravo, politika. — 2023. — T. 17. — № 4. — S. 82–91.
8. Litivishko P. A. Pervyy globalnyy dogovor protiv kiberprestupnosti: ot geopoliticheskoy konfrontatsii k professionalnomu kompromissu // Mezhdunarodnaya zhizn. — 2024. — № 11. — S. 1–27.
9. Mezhdunarodnoe ugovovnoe pravo: uchebnik dlya bakalavriata i magistratury / A. V. Naumov, A. G. Kibalnik, V. N. Orlov, P. V. Volosyuk / pod red. A. V. Naumova, A. G. Kibalnika. — 2-e izd., pererab. i dop. — M.: Yurayt, 2014. — 510 s.
10. Moroz N. O. Mezhdunarodno-pravovye osnovy obespecheniya mezhdunarodnoy informatsionnoy bezopasnosti // Trud. Profsoyuzy. Obshchestvo. — 2016. — № 1 (51). — S. 77–81.

11. Chernukhin E. Ob istorii sozdaniya i itogakh raboty spetsialnogo komiteta po razrabotke vseobemlyushchey mezhdunarodnoy konventsii o protivodeystvii ispolzovaniyu IKT v prestupnykh tselyakh // Mezhdunarodnaya zhizn. — 2025. — № 2. — S. 108–113.
12. Shved N. A. Sravnitelnyy analiz ugovnoy otvetstvennosti za nesanktsionirovannyi dostup k kompyuternoy informatsii v stranakh ES // Vestnik Nizhegorodskogo universiteta imeni N.I. Lobachevskogo. — 2016. — № 5. — S. 222–226.
13. Shestak V. A., Chebotar A. S. Budapeshtskaya konventsiya kak osnovopolagayushchiy mekhanizm protivodeystviya kiberprestupnosti: novatsii i perspektivy mezhdunarodno-pravovogo regulirovaniya // Obrazovanie i pravo. — 2023. — № 8. — S. 305–310.