

Ибатуллина Диана Марсовна

преподаватель

ФГКОУ ВО «Казанский юридический институт МВД РФ»

г. Казань, Республика Татарстан

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРХИЩЕНИЯМ

Аннотация: в статье анализируются развитие международной нормативной базы по противодействию киберхищениям, а также проблемы в области международного сотрудничества в указанной сфере. Автор приходит к выводу о необходимости дальнейшего совершенствования системы взаимопомощи при расследовании трансграничных киберпреступлений, внедрения более гибких и оперативных механизмов сотрудничества, в том числе на пространстве СНГ.

Ключевые слова: киберпреступления, киберхищения, противодействие, международные организации, ООН, СНГ.

Трансграничная угроза распространения корыстных преступлений против собственности, совершаемых с использованием информационных технологий, обусловила необходимость выработки мер противодействия на международном уровне.

Меры противодействия преступлениям против собственности, совершенным с использованием информационных технологий, разрабатываются множеством международных организаций: Организацией объединенных наций (далее-ООН), Североатлантическим альянсом (далее-НАТО), Шанхайской организацией сотрудничества (далее-ШОС), Советом Европы (далее-СЕ), Европейским союзом (далее-ЕС), Содружеством независимых государств (далее – СНГ) и т. д.

Первые шаги по нормативно-правовому регулированию были реализованы 13 сентября 1989 года. Совет Европы принял Рекомендацию №89 [1], которой был установлен перечень цифровых преступлений. К корыстным преступлениям против собственности, совершаемым в виртуальной среде, были отнесены:

- 1) компьютерное мошенничество;

2) компьютерный подлог.

В дальнейшем, в связи с увеличением фактов совершения вышеуказанных преступлений, список был дополнен рядом противоправных деяний, среди которых было и «противозаконное применение компьютера». Данное преступление имело уже более широкую трактовку. «Противозаконное применение компьютера» не конкретизирует объективную сторону противоправного деяния, определяя обязательный признак объективной стороны – применение компьютера.

В 2001 году была принята Резолюция Генеральной Ассамблеи ООН №55/63 «Борьба с использованием информационных технологий в преступных целях», указывает на необходимость международного сотрудничества в рамках борьбы в киберпреступностью, которая и на сегодняшний день остается ведущим документом в вопросах информационной безопасности [2].

На 20-ом Конгрессе ООН в 2010 году, была обозначена проблема дальнейшей разработки единой Глобальной Конвенции по борьбе киберпреступлениями.

В 2011 году Советом Европы была принята Конвенция «О преступности в сфере компьютерной информации» [3]. Указанная Конвенция включала в себе две наиболее значимые группы преступлений в исследуемой среде:

- 1) преступления, связанные с использованием компьютерных средств;
- 2) правонарушения, связанные с содержанием данных.

Но несмотря на то, что Конвенция объединила позиции ряда государственных систем, она по-прежнему включает в себя незначительный перечень преступлений, не отвечая объемам имеющейся угрозы.

В 2016 году был принят первый нормативный акт Европейского союза, регламентирующий вопросы безопасности сетей и информационных систем – *Директива ЕС о безопасности сетей и информационных систем (NIS Directive)* [4]. Директива призывает страны Европы к развитию устойчивости критической инфраструктуры, требует технического развития в области противодействия киберугрозам.

Как отмечает Н.О. Мороз, на сегодняшний день в международном сообществе все же отсутствует комплексный договор универсального характера, в сфере

неправомерного использования информационных технологий [5]. Отсутствие подобного нормативного документа обусловлено двумя проблемами: различия в национальных подходах к информационной безопасности; недостаток международного сотрудничества.

Важнейшим этапом в рамках противодействия киберпреступлениям стало принятие *Конвенция ООН против киберпреступности* [6]. Принятие Конвенции послужило основанием для:

- криминализации ряда противоправных деяний, совершаемых с использованием информационных технологий (перехват данных, легализация денежных средств, хищения и т. д.);
- закрепления универсальных методов работы с электронными следами;
- взаимной межгосударственной помощи при расследовании киберпреступлений;
- создания сети контактных центров, работающих 24/7, для оперативной помощи.

Однако даже принятие вышеуказанной Конвенции не устранило проблемы противодействия киберхищениям на международном уровне. По-прежнему различными остаются подходы к криминализации киберхищений [7], в ряде стран законодательные акты устанавливают уголовную ответственность в рамках специальных норм, в иных случаях присутствуют лишь общие нормы.

Трансграничный характер анализируемых преступлений создает сложности и для определения правовой юрисдикции, т.е. зачастую возникает вопрос в какой именно стране правоохранительные органы должны расследовать совершенное противоправное деяние.

Безусловно, механизм взаимопомощи при расследовании такого рода преступлений также является несовершенным. Процессуальные процедуры занимают много времени, что зачастую приводит к потере цифрового следа. К тому же особенности политической обстановки в отдельных странах и на международной арене непосредственно влияет на взаимодействие правоохранительных органов.

Таким образом, сфера международного сотрудничества в рамках противодействия киберхищениям регулярно совершенствуется, но несмотря на это, действующие механизмы имеют несовершенства. Рациональным видится дальнейшее совершенствование системы взаимопомощи при расследовании киберхищений. Меры взаимопомощи должны быть более универсальным, гибкими, реализовываться в кратчайшие сроки. В ближайшее время возможно достичь создания единого наднационального механизма противодействия киберхищениям для всех стран СНГ, достаточно устранить практические барьеры в обмене данными и цифровыми доказательствами.

Список литературы

1. О преступлениях, связанных с компьютерами: Рекомендация Совета Европы от 13.09.1989 №89 (9). – URL: [https://translated.turbopages.org/proxy_u/en-ru.ru.9cd68488-63d8e9b3-65be9571-74722d776562/https/itlaw.fandom.com/wiki/Recommendation_No._R\(89\)_9](https://translated.turbopages.org/proxy_u/en-ru.ru.9cd68488-63d8e9b3-65be9571-74722d776562/https/itlaw.fandom.com/wiki/Recommendation_No._R(89)_9) (дата обращения: 18.06.2023).
2. Резолюция Генеральной Ассамблеи ООН №55/63 «Борьба с использованием информационных технологий в преступных целях». – URL: <https://docs.cntd.ru/document/901941379?ysclid=mbtdksusd7728248658> (дата обращения: 18.06.2026).
3. О преступности в сфере компьютерной информации: Конвенция ETS №185 от 23.11.2001 г. – URL: <https://base.garant.ru/4089723/?ysclid=ldk2px5hk9362018531> (дата обращения: 20.06.2026).
4. Директива ЕС о безопасности сетей и информационных систем принята от 06.07.2016. – URL: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2020\)654198](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)654198) (дата обращения: 20.06.2026).
5. Мороз Н.О. Международно-правовые основы обеспечения международной информационной безопасности / Н.О. Мороз. – URL: <http://elib.mitso.by/bitstream/edoc/1799/1/2016%20%20-%201-079-083.pdf> (дата обращения: 22.06.2026).

6. Конвенция Организации Объединенных Наций против киберпреступности (принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 года). – URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243?ysclid=mraq3gq77x673440368> (дата обращения: 25.06.2026).

7. Чернякова А.В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации / А.В. Чернякова // Юридическая наука и правоохранительная практика. – 2018. – №4 (46). – URL: <https://cyberleninka.ru/article/n/mezhdunarodnyy-i-zarubezhnyy-opyt-ugolovno-pravovogo-protivodeystviya-hischeniyam-sovershaemym-s-ispolzovaniem-kompyuternoy> (дата обращения: 07.07.2026).

8. Солодовник В.В. Международная правовая помощь по уголовным делам: современное состояние, проблемы и перспективы развития / В.В. Солодовник // Международное право и международные организации / International Law and International Organizations. – 2026. – №1. – DOI: 10.7256/2454-0633.2026.1.78653. EDN BAIDGK