ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДИПЛОМАТИЧЕСКАЯ АКАДЕМИЯ
МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

На правах рукописи

Аббуд Руслан Ратебович

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

5.1.5. Международно-правовые науки

Диссертация на соискание ученой степени
кандидата юридических наук

Научный руководитель:
Нешатаева Татьяна Николаевна
доктор юридических наук, профессор

Москва – 2025

ОГЛАВЛЕНИЕ

Список сокращений

1) **ИКТ** – информационно-коммуникационные технологии.
2) **Конвенция СЕ** – конвенция Совета Европы о преступности в сфере компьютерной информации.
3) **Протокол № 1** – дополнительный протокол к конвенции по киберпреступлениям в отношении криминализации деяний расистского и ксенофобского характера, осуществляемых при помощи компьютерных систем.
4) **Конвенция АС** – конвенция Африканского союза о кибербезопасности и защите персональных данных.
5) **Конвенция ЛАГ** – конвенция Лиги Арабских Государств о борьбе с преступлениями в сфере информационных технологий.
6) **Протокол № 2** – второй дополнительный протокол к конвенции о киберпреступности о расширении сотрудничества и обнаружении электронных доказательств.
7) **Проект Конвенции ООН** – проект конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях от 27 июля 2021 года.
8) **Конвенция ООН против киберпреступности** – конвенция ООН против киберпреступности; Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям.
9) **Директива ЕС** – Директива № 2013/40/ЕС Европейского парламента и Совета Европейского Союза «Об атаках на информационные системы и о замене Рамочного решения 2005/222/ПВД Совета ЕС.
10) **Конвенция о выдаче** – Европейская Конвенция о выдаче 1957 года.
11) **УК РФ** – Уголовный Кодекс Российской Федерации.
12) **ЕСПЧ** – Европейский Суд по правам человека.

13) **Европейская Конвенция** - Конвенция о защите прав человека и основных свобод.

14) **ЕКПП** – Европейский комитет по проблемам преступности.

15) **Комитет** – Комитет Конвенции о киберпреступности.

16) **Офис по борьбе с киберпреступностью –** Офис Программы Совета Европы по борьбе с киберпреступностью.

17) **Рабочая группа СЕ** – Рабочая группа по доступу уголовного правосудия к доказательствам, хранящимся в облаке, в том числе в рамках взаимной правовой помощи.

18) **ООН** – Организация Объединенных Наций.

19) **ГА ООН** – Генеральная Ассамблея ООН.

20) **Комиссия ООН по правосудию** – Комиссия ООН по предупреждению преступности и уголовному правосудию.

21) **УНП ООН** – Управление ООН по наркотикам и преступности.

22) **Спецкомитет** – Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

23) **ГКИ** – Глобальный комплекс инноваций Интерпола.

24) **ЕС** – Европейский союз.

25) **Агентство ЕС по кибербезопасности** – Европейское агентство по сетевой и информационной безопасности.

26) **ЕАЭС** – Евразийский экономический союз.

27) **ЛАГ** – Лига арабских государств.

28) **АС** – Африканский союз.

29) **СНГ** – Содружество независимых государств.

30) **ШОС** – Шанхайская организация сотрудничества.

31) **ЭКОВАС** –Экономическое сообщество Западноафриканских государств.

32) **САДК** – Сообщество развития Юга Африки.

33) **ОЭСР** – Организация экономического сотрудничества и развития.

34) **ОАГ** – Организация американских государств.

35) **ОБСЕ** – Организации по безопасности и сотрудничеству в Европе.

36) **НАТО** – Североатлантический альянс.

37) **Киберцентр НАТО** – Центр передового опыта совместной киберзащиты НАТО.

38) **ММППК** – Международное многостороннее партнерство против киберугроз.

39) **МСЭ** – Международный союз электросвязи.

40) **ИИ** – Искусственный интеллект.

41) **ПО** – программное обеспечение.

42) **ОПГ** – оперативная преступная группа.

43) **ОРД** – оперативно-розыскная деятельность.

44) **ЕЦБК** – Европейского центра по борьбе с киберпреступностью.

45) **ЮНИКРИ** – центр искусственного интеллекта и робототехники при Межрегиональном научно-исследовательском институте Организации Объединенных Наций по вопросам преступности и правосудия.

46) **Комитет по ИИ** – специальным межправительственный комитет экспертов по ИИ Совета Европы.

47) **ЭД** – электронные доказательства.

48) **МУС** – международный уголовный суд.

49) **Европол** – агентство Европейского союза по сотрудничеству в правоохранительной сфере.

50) **АФРИПОЛ** – механизм Африканского союза по полицейскому сотрудничеству.

Введение

Актуальность темы исследования

Киберпреступление является современным вызовом и угрозой, которая исходит от негосударственных акторов. Эта проблема носит глобальный характер, которая будет возрастать по мере распространения и развития информационных технологий. В связи с этим эффективное международное сотрудничество, а также координация усилий мирового сообщества в сфере предупреждения и ликвидации последствий киберпреступлений имеет огромное значение, так как бороться с этим противоправным деянием в сфере информационно-коммуникационных технологий (далее – ИКТ) на уровне отдельного государства представляется практически невозможным.

В международном праве киберпреступление является преступлением международного характера, которое посягает как на внутригосударственный, так и на международный правопорядок. В узком смысле под киберпреступлением понимается любое противоправное деяние, осуществляемое посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных. Киберпреступление в широком смысле означает любое противоправное деяние, совершаемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное хранение, распространение информации посредством компьютерной системы или сети[1].

На сегодняшний день, в международном праве отсутствует консолидированный подход к пониманию термина киберпреступление. Вопрос понятийно-категориального аппарата является одним из существенных пунктов в международных договорах. Отсутствие единого подхода к пониманию самой сущности и несогласованности терминологии в

[1] Schjolberg, Stein. The history of cybercrime (third edition). 2020. P. 25.

международных документах, а также в доктринах свидетельствует о специфических особенностях данного криминального явления.

Такие виды киберпреступлений, как киберджетинг, кардинг и кибербуллинг требуют соответствующего нормативного регулирования. Для более четкого понимания проблемы необходимо выработать также легальную дефиницию для каждого вышеперечисленного киберпреступления.

Проблема киберпреступности является многогранной, требующей четкого и скоординированного принятия мер. Стоит отметить возрастание роли транснациональных и неправительственных организаций, которые превратились в важнейший инструмент по борьбе с киберпреступлениями и их расследованию. Постепенное интегрирование искусственного интеллекта, как превентивной меры, видится эффективным методом борьбы против киберпреступлений.

Вместе с тем актуальным и целесообразным видится потребность в необходимости выработки на международном уровне конвенции универсального характера, которая будет содержать определение термина киберпреступление, новые виды киберпреступлений, способы и методы взаимодействия межправительственных структур, а также национальных правоохранительных органов разных государств в части расследования и предотвращения киберпреступлений, и регламентировать сеть «Интернет».

Степень научной разработанности темы исследования

Вопрос международной информационной безопасности, которая включает в себя международно-правовое противодействие киберпреступлениям, является одним из самых неоднозначных и дискуссионных проблем со времени появления этого феномена. Отсутствие консолидированной концепции в отношении киберпреступлений порождает определенные сложности в части международно-правового противодействия киберпреступлениям. Состояние существующего международного права в отношении борьбы с киберпреступлениями вызван генезисом и определенными причинами развития киберпреступлений. В основу

диссертационного исследования заложен анализ ряда международных соглашений, национального законодательства, а также доктрин ученых в части киберпреступлений.

На сегодняшний день анализ проблемы международно-правового противодействия киберпреступлениям в научной отечественной литературе должным образом не уделено, многие вопросы ее остаются открытыми. Отечественные юристы, специализирующиеся в международном праве, ограничиваются небольшими статьями в части отдельных аспектов киберпреступлений, вследствие чего актуальность научного исследования увеличивается. Большая часть монографий, посвященных особенностям международно-правового противодействия киберпреступлениям, написаны иностранными учеными. На национальном уровне существует пробел в части диссертационных исследований, посвященных объекту данной работы.

В доктрине международного права феномен киберпреступления не имеет консолидированного подхода. Ряд концепций относительно определения понятия, сущности, международно-правового противодействия и классификации киберпреступлений продолжают являться предметом научных обсуждений. Анализ международных соглашений в части киберпреступлений, а также выработка новой универсальной конвенции, которая будет регулировать киберпреступления, видится необходимым для решения данной проблематики.

Актуальность исследования, недостаточная разработанность выбранной темы определили цели, задачи и структуру диссертационного исследования.

Целью диссертационного исследования является проведение подробного анализа теоретических и практических вопросов, коррелирующих с международно-правовым регулированием противодействия киберпреступлениям, а также выработка конкретных предложений для решения данной проблемы.

Для достижения указанной цели ниже приведены следующие **задачи**:

– раскрыть существенные характеристики содержания определения киберпреступления;

– привести существующие подходы в части определения термина киберпреступление и привести его понятие с позиции автора;

– провести сравнительно-правовой анализ международных соглашений, регулирующих киберпреступления;

– определить классификацию киберпреступлений, которая не закреплена в международных договорах;

– проанализировать алгоритм работы систем искусственного интеллекта в качестве противодействия киберпреступлениям;

– определение института международно-правовой ответственности государств за совершение киберпреступлений.

Объект диссертационного исследования – правоотношения, образующиеся в процессе международно-правового регулирования киберпреступлений.

Предмет исследования – принципы и нормы международного права, регламентирующие основы международно-правового регулирования киберпреступлений, а также судебная практика в сфере данного рода преступлений.

Методологические основы исследования

Применены такие методы научного познания как общественные, так и социальные явления и процессы, в том числе явления правовой действительности: общенаучные и частнонаучные методы. Приведем общенаучные методы:

1) Диалектический метод. Сыграл важную роль в части подробного изучения предмета диссертации в его постоянном прогрессе с учетом корреляции с иными юридическими явлениями.
2) Метод анализа. Благодаря методу анализа были достигнуты задачи и цели, содержащиеся в диссертации.

3) Метод синтеза. Использован при определении толкований основных понятий по теме диссертации комплексному рассмотрению вопросов данной проблематики.

Далее приведем частнонаучные методы:

1) Формально-юридический метод. Данный метод был применен при формулировании конкретного смысла терминов, использованных в научном исследовании, для понимания содержания положений Протокола Конвенции ООН об использовании ИКТ в противоправных целях, а также других международных соглашений.
2) Сравнительно-правовой метод. Использовался в целях соотношения международных соглашений и норм внутригосударственного права в части киберпреступлений для выявления и анализа особенностей регулирования данной области, а также решения конкретных задач.

Теоретическую основу диссертационного исследования составили основные идеи и выводы, отображенные в работах отечественных и иностранных исследователей, в которых освещаются аспекты теории международного права, киберпрестпулений и международной информационной безопасности: А.Х. Абашидзе, Бирюков, А. Г. Волеводз, А.Н. Вылегжанин, А.А. Ефремов, А.А. Данельян, Ю.Н. Жданов, Б.Л. Зимненко, Д.В. Красиков, А.В. Крутских, В.Д. Зорькин, М.Б. Касенова, Н.Н. Липкина, И.И. Лукашук, А.Б. Мезяев, А.В. Наумов, Т.Н. Нешатаева, А.Ю. Скуратова, Б. Р. Тузмухамедов, Г.И. Тункин, В.П. Талимончик, Т.Л. Тропина, В. Л. Толстых, Н. А. Чернядьева, А. В. Яковенко, М.Ч. Бассиуни, Томас Ж. Холт, Адам М. Босслер, Хусам аль-Таи, Самули Хаатажа, Д.Е. Деннинг, Габриэль Вейман, Мора Конвей, Али Джахангири, Д. Абрахам, Уильям А. Оуэнс, К. Уилсон, Штейн Шолберг и другие.

Правовой основой исследования послужили: проект Конвенции ООН, внесенный Российской Федерацией о противодействии использованию информационно - коммуникационных технологий в преступных целях от 27 июля 2021 года (далее – проект Конвенции ООН), Конвенция Совета Европы

о преступности в сфере компьютерной информации 2001 года (далее – Конвенция СЕ), Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 года (далее – Соглашение СНГ), Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности 2009 года (далее – Соглашение ШОС), Директива № 2013/40/ЕС Европейского парламента и Совета Европейского Союза об атаках на информационные системы и о замене Рамочного Решения 2005/222/ПВД (далее – Директива ЕС), Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 года (далее – Конвенция АС), Конвенция Лиги Арабских Государств о борьбе с преступлениями в сфере информационных технологий 2010 года (далее – Конвенция ЛАГ), Уголовный кодекс Российской Федерации (далее – УК РФ).

Эмпирическую основу составили доклады Группы правительственных экспертов ООН, резолюции Генеральной Ассамблеи ООН в части киберпреступлений, а также судебные решения национальных и международных судов.

Научная новизна диссертационного исследования состоит в том, что впервые в отечественной юридической науке осуществлен всесторонний анализ регулирования киберпреступлений. Диссертантом в комплексном виде осуществлен сравнительно-правовой анализ международных соглашений, регламентирующих киберпреступления. При изучении сущности киберпреступления, в диссертационном исследовании были не только выявлены характеристики данного противоправного деяния, но и сформулировано автором исследования его понятия, а также определена новая классификация киберпреступлений, не содержащаяся в международных договорах. В исследовании проанализированы институциональные и договорные формы сотрудничества между государствами в целях противодействия киберпреступлениям и аргументирована позиция в

отношении того, какие акты (*hard law vs soft law*) являются наиболее эффективными в части регулирования данной проблемы. Более того, исследование содержит анализ систем искусственного интеллекта (далее – ИИ), что позволило прийти к выводу о том, что посредством установления специального алгоритма, ИИ способен обеспечить надлежащую киберзащиту.

Положения, выносимые на защиту:

1. Киберпреступление является преступлением, обладающее трансграничным характером – происходит на территории двух и более государств. Трансграничность выражается в появлении иностранного элемента в правоотношениях и, как следствие, угрожает национальным правопорядкам двух или более государств. Более того, о трансграничном характере говорит то, что киберпреступление не ограничено территориальными границами одного государства. Таким образом, трансграничность киберпреступления характеризуется отсутствием каких-либо ограничений по субъектному составу и способам совершения, поскольку информационное пространство не имеет определенных границ, и его последствия выходят за пределы правопорядка отдельного государства в силу степени общественной опасности.

2. Имея ввиду отсутствие в международных соглашениях общепризнанного универсального определения киберпреступления, что связано с несогласованностью терминологии в международных документах, а также с отсутствием в доктринах единого понятия киберпреступления, предлагается определить киберпреступление – как виновно совершенный, несанкционированный доступ к информационно-коммуникационным технологиям при помощи компьютерных устройств и иных технических средств, с целью нанесения как материального, так и нематериального ущерба и влекущее негативные последствия трансграничного характера неограниченному круг лиц.

3. В настоящий момент, учитывая стремительное развитие технологий в эпоху цифровизации, классификация киберпреступлений, содержащаяся в

действующих международных соглашениях, теряет актуальность. Например, такие преступления в сфере информационных технологий, как криптоджекинг или кибербуллинг в международных соглашениях не закреплены.

Предлагается выделить дополнительную классификацию по следующему критерию объекта: «противоправное использование информационно-коммуникационных технологий в целях нарушения прав личности в части чести и достоинства, а также собственности в информационном пространстве». Из данного тезиса вытекают следующие виды киберпреступлений: а) кибербуллинг, б) дипфейк, в) криптоджекинг, г) вещевой кардинг.

4. Средством международно-правовой борьбы с киберпреступлениями может выступить искусственный интеллект (далее – ИИ), роль которого применимо к киберпреступлениям двойственна. Во-первых, постепенное интегрирование искусственного интеллекта, как превентивной меры и упреждающего удара, может быть эффективным методом борьбы против киберпреступлений и обеспечения международной информационной безопасности в целом. Во-вторых, ИИ также может нести угрозу международной информационной безопасности, если системы ИИ окажутся в распоряжении умелых киберпреступников, способных взламывать базы данных, осуществлять кибератаки на инфраструктуру, критически важные объекты и при этом оставаться латентными. В исследовании делается вывод о том, что обычные нормы международного права и механизмы международно-правовых институтов в части реализации ИИ не работают.

Предлагается противостоять киберпреступлениям при помощи ИИ путем разработки исходного кода внутреннего инструмента специального программного обеспечения (далее – ПО), посредством которого разработчики систем ИИ смогут находить риски и тем самым выявлять проблемы кибербезопасности.

5. В настоящее время современная множественность национальных правовых систем свидетельствует о невозможности координации

регулирования киберпреступлений на национальном уровне. В современном мире положения правовых норм, противоречащих друг другу, приводят к коллизиям национальных законов, и как следствие, к невозможности их регулирующего действия на территории разных государств, так и реализаций наказаний за их нарушение. Гармонизация и унификация уголовного права, уголовно-процессуального права является неотъемлемым требованием для усовершенствования международного сотрудничества в сфере противодействия киберпреступлениям[2].

Сделан вывод о том, что сближение национальных правовых систем в части криминализации во внутреннем законодательстве деяний, совершенных с использованием компьютерных технологий, а также включения в национальный уголовный процесс норм о процессуальных действиях, специфических для расследования и судебного разбирательства по делам о киберпреступлениях осуществимо через международные договоры универсального и регионального характера.

6. Особо значимо сотрудничество на региональном уровне. На сегодняшний день в рамках Евразийского экономического союза (далее – ЕАЭС) отсутствует многостороннее соглашение в части противодействия киберпреступлениям. Сотрудничество через двусторонние международные договоры между государствами-участниками оказалось малоэффективным, так как киберпреступления нарушают правопорядок более двух государств. В целях преодоления данной проблемы видится необходимым принятия договора под эгидой ЕАЭС, который сможет обеспечить безопасность информационного пространства путем обмена информацией, взаимной помощью в части расследования киберпреступлений, а также запросах о выдаче преступников.

Вышеперечисленные механизмы взаимодействия должны обеспечить эффективность в части сотрудничества между странами-участниками ЕАЭС, а

[2] Schjolberg, Stein. 2008. The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva. URL: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.

помощь их в реализации должен оказать специально созданный международный правоохранительный орган регионального характера.

7. Доказано, что принятие на универсальном уровне международного соглашения, регламентирующего усовершенствованные формы сотрудничества и усиление превентивных мер в части оказания противодействия киберпреступлениям, является актуальным. Резолюцией ГА ООН 79/243 от 24 декабря 2024 года принята Конвенция ООН против киберпреступности; Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (далее – Конвенции ООН против киберпреступности), разработанная Россией. Конвенции ООН предусматривает реализацию международного сотрудничества в сфере оперативно-розыскной деятельности, ареста и возврата активов. Закрепляется цифровой суверенитет государств над своим информационным пространством, в том числе посредством наращивания международного взаимодействия между компетентными ведомствами.

Сделан вывод о важности создания в будущем международной правоохранительной организации универсального характера, наделенной компетенцией в части осуществления международной оперативно-розыскной деятельности в целях выявления, пресечения или раскрытия наиболее тяжких киберпреступлений, а также международных расследований на досудебных стадиях уголовного судопроизводства. Кроме того, в целях осуществления международного уголовного правосудия возможно создание специального трибунала ad hoc по международным киберпреступлениям.

8. Подчёркивается, что экстрадиция по-прежнему остается одним из традиционных механизмов сотрудничества в части борьбы с киберпреступлениями. Однако, как показывает практика, государства отказывают в экстрадиции со ссылками на нормы внутригосударственного

законодательства[3]. Делается вывод, что если государство по каким-либо причинам отказывается в выдаче, то оно обязано само осуществить правосудие. Тем не менее, суды подчеркивают, что государства, которые берут на себя ответственность судить преступников из другого государства, должны соблюдать основополагающие принципы справедливого судебного разбирательства, а также обеспечивать гуманное обращение к таким преступникам[4].

Теоретическая значимость результатов диссертационного исследования состоит в том, что данные, полученные при проведении настоящего исследования, имеют ценность в связи с тем, что они дополняют теоретические представления о правовых аспектах регулирования киберпреступлений как преступлений международного характера. Сформированные в диссертации теоретические положения могут использоваться для дальнейших исследований в области регламентации киберпреступлений.

Практическая значимость результатов диссертационного исследования состоит в том, что полученные результаты исследования могут быть применены правоохранительными органами Российской Федерации в части уголовного преследования за совершение киберпреступлений. Более того, результаты проведенного исследования могут быть использованы в рамках разработки международного договора универсального характера под эгидой ООН.

Апробация результатов исследования

Основные положения и выводы диссертации обсуждались на заседании кафедры международного права Российского государственного университета правосудия, отражены в опубликованных статьях. Отдельные идеи

---

[3] See *Soering V the United Kingdom* (1989) European Court of Human Rights; *Othman (Abu Qatada) V United Kingdom* 8139/09 (2012) ECHR 56

[4] Bassiouni., M. C (1999). The Sources and Content of International Criminal Law: A Theoretical Framework *International Criminal Law* 3-126; *Cheng V Governor of Pentonville Prison* (1973) A.C. 931, 945 H.L.;*Ex Parte Schtraks* (1964) AC 556, at 583 HL; and *Schtraks V Government of Israel* (1964) AC 556, 582- 584.

диссертационного исследования были обсуждены на научно-практических конференциях:

1) Международная научно-практическая конференция «Международное право и глобальные вызовы современности», посвященная 80-летию профессора Р. М. Валеева в Казанском федеральном университете (г. Казань, 27-28 сентября 2018 г.);
2) X Всероссийская научно-практическая конференция аспирантов, соискателей и молодых ученых «Толкование и конкретизация права: проблемы теории и практики» в Российском государственном университете правосудия (г. Москва, 23 апреля 2019 г.);
3) V Международная научно-практическая конференция «Актуальные проблемы международных отношений и международного права» в Дипломатической академии МИД России (г. Москва, 16 марта 2021 г.);
4) XXVIII Международная конференция студентов, аспирантов и молодых ученых «Ломоносов» в Московском государственном университете имени М.В. Ломоносова (г. Москва, 12-23 апреля 2021 г.);
5) X Всероссийская научно-практическая конференция аспирантов, соискателей, магистрантов и молодых ученых «Регулирование правоотношений: проблемы теории и практики» в Российском государственном университете правосудия (г. Москва, 28 апреля 2022 г.);
6) Международная научно-практическая конференция «Действие международного права в пространстве (материковое, морское, воздушное, космическое, киберпространство)» посвященная 80-летию МГИМО МИД России (г. Москва, 23 мая 2024 г.).

По теме исследования опубликовано 10 научных работ, в том числе 6 статей в научных изданиях, рецензируемых Высшей аттестационной комиссией при Министерстве образования и науки Российской Федерации.

Структура работы. Диссертация состоит из введения, двух глав, включающих в себя шесть параграфов, заключения, а также списка использованной литературы.

Глава 1. Характеристика киберпреступления в международно-правовой науке

§ 1. Определение понятия киберпреступление в международном праве

Киберпреступления не знают территориальных границ, а внутригосударственные органы, наделенные полномочиями в сфере борьбы с преступлениями в сфере компьютерной информации строго ограничены юрисдикцией своего государства. В связи с этим международное сотрудничество является необходимым, для того чтобы пресекать, выявлять, а также раскрывать киберпреступления, так как противостоять преступлениям в сфере информационных технологий на уровне отдельного государства представляется невозможным.

На протяжении последних десятилетий в ряде регионов были воплощены разные подходы, направленные на международно-правовое регулирование борьбы в отношении киберпреступлений и приняты соответствующие международные соглашения регионального характера. Большинство действующих международных соглашений в части киберпреступлений не содержат данного понятия.

На сегодняшний день, в международном праве отсутствует единый подход к пониманию термина киберпреступление. Вопрос понятийно-категориального аппарата является одним из существенных пунктов в международных договорах. Отсутствие единого подхода к пониманию самой сущности и несогласованности терминологии в международных документах, а также в доктринах свидетельствует о специфических особенностях данного криминального явления.

Конвенция о преступности в сфере компьютерной информации (далее – Конвенция СЕ) является первым международным договором, направленным на борьбу с киберпреступлениями путем гармонизации национальных законов, совершенствования метод расследования и расширения

сотрудничества между странами. Она была разработана Советом Европы в Страсбурге. Конвенция и Пояснительный доклад к ней были приняты Комитетом министров Совета Европы на его 109-й сессии 8 ноября 2001 года. Она была открыта для подписания в Будапеште 23 ноября 2001 года и вступила в силу 1 июля 2004 года.

В Конвенции СЕ приведен лишь перечень киберпреступлений и их содержание[5]. Определение термина киберпреступление Конвенция СЕ не содержит.

Однако в Конвенцией Африканского союза о кибербезопасности и защите персональных данных от 2014 года, а именно в Главе 3 «Обеспечение кибербезопасности и борьба с киберпреступностью» в ст. 25 «Законодательство против киберпреступности» указано, что под киберпреступлениями понимаются такие противоправные деяния с использованием информационно-коммуникационных телекоммуникаций в отношении целостности, доступности и конфиденциальности, а также сохранности компьютерных систем[6].

Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий содержит положения об усилении сотрудничества между странами-участницами Конвенции ЛАГ в части противодействию киберпреступлениям в целях обеспечения безопасности государств-участниц Конвенции ЛАГ. Конвенция ЛАГ была принята 21 декабря 2010 года в Каире, Египет. В данном международном соглашении регионального характера описываются охватываемые им преступления в области информационных технологий, процессуальные нормы, механизмы правового и судебного сотрудничества между странами-участницами[7]. Конвенция ЛАГ содержит такие киберпреступления, как

---

[5] Convention on Cybercrime (Budapest, 23.XI.2001). URL: https://www.europarl.europa.eu/. Доступ из СПС «Гарант».

[6] African Union Convention on Cyber Security and Personal Data Protection. 2014. URL: https://au.int/. Доступ из СПС «Гарант».

[7] Arab Convention on Combating Information Technology Offences. 2010. URL: https://www.asianlaws.org/. Доступ из СПС «Гарант».

несанкционированный доступ к персональным данным, кибертерроризм, нарушение авторских и смежных прав, а также хищение с использованием ИКТ. Кроме того, Конвенция ЛАГ включает положения о процессуальном праве, юрисдикции и взаимной правовой помощи. Однако определение понятия киберпреступление в Конвенции ЛАГ отсутствует.

На Десятом Конгрессе ООН по предупреждению преступности и обращению с правонарушителями (Вена, 10–17 апреля 2000 года), одобренной резолюцией 53/110 от 9 декабря 1998 года ГА ООН, в соответствии с пунктом 14 киберпреступление было определено с двух точек зрения.

В узком смысле под киберпреступлением понимается любое незаконное действие, реализуемое через информационные ресурсы для того, чтобы рассекретить защиту систем ЭВМ и обрабатываемых им информации. В широком смысле под киберпреступлением понимается любое незаконное действие, реализуемое через системы ЭВМ, включая также такие противоправные деяния, как противоправное распространение и хранение данных через системы ЭВМ или сети[8].

Существуют международные соглашения, содержащие синоним понятия киберпреступление. Так, например, в Соглашении о сотрудничестве государств – участников Содружества Независимых Государств (далее – СНГ) в борьбе с преступлениями в сфере компьютерной информации от 2001 года не содержится понятие киберпреступление, а дается термин преступления в сфере компьютерной информации. В соответствии с пунктом а статьи 1 под преступлением в сфере компьютерной информации понимается «уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация»[9]. Однако вышеприведенное соглашение утратило силу. Под эгидой СНГ было заключен новый договор в части противодействия киберпреступлениям: Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018

[8] Schjolberg, Stein. The history of cybercrime (third edition). 2020. P. 25.

[9] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 года). Доступ из СПС «Гарант».

года[10]. В 2021 году Российская Федерация приняла Федеральный закон о ратификации Соглашения СНГ (далее – Соглашение СНГ)[11]. В данном соглашении преступления в сфере компьютерной информации стали трактоваться, как преступления в сфере информационных технологий. Более того, в данном договоре прописаны виды уголовно наказуемых деяний в сфере информационных технологий, а также формы сотрудничества. Определение понятия преступления в сфере информационных технологий в данном соглашении отсутствует.

Под эгидой ШОС было принято соглашение о сотрудничестве в области обеспечения международной информационной безопасности (далее – Соглашение ШОС) (Екатеринбург, 16 июня 2009 года) и вступило в силу с 5 января 2012 года. Данный документ содержит следующие киберпреступления: кибертерроризм; разработка кибероружия; распространение данных, наносящих урон системам инфраструктуры. Всего в Соглашении ШОС перечислено 6 угроз, которые можно приравнять к киберпреступлениям. В Соглашении ШОС под киберпреступлениями понимается термин информационная преступность, и определяется, как использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях (статья 1, основные понятия)[12].

Таким образом, определение понятия киберпреступление дается слишком лаконичным и не отображает всей сущности данного преступления международного характера.

Если мы обратимся к национальному законодательству, то в главе 28 Уголовного Кодекса Российской Федерации (далее – УК РФ) под

---

[10] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018г.). Доступ «СПС Гарант».
[11] Федеральный закон "О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий" от 01.07.2021 N 237-ФЗ (последняя редакция). Доступ «СПС Гарант».
[12]СОГЛАШЕНИЕ между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2019 года). Доступ из СПС «Гарант».

киберпреступлением понимаются преступления в сфере компьютерной информации, где приведены виды данного рода преступления и не разъяснено понятие[13]. В статьях 272–274.2 главы 28 УК РФ приведен перечень преступлений в сфере компьютерной информации:

1) неправомерный доступ к компьютерной информации;
2) создание, использование и распространение вредоносных компьютерных программ;
3) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
4) неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации;
5) нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.

В июле 2021 года Российская Федерация внесла в Спецкомитет ООН проект Конвенции о противодействии использовании информационно-коммуникационных технологий в преступных целях (далее – проект Конвенции ООН). В проекте Конвенции ООН под киберпреступлениями понимаются преступления в сфере информационно-коммуникационных технологий. Само понятие преступления в сфере информационно-коммуникационных технологий в документе отсутствует. Однако в пункте f статьи 4 проекта Конвенции ООН дается ответ на вопрос, что представляют из себя информационно-коммуникационные технологии (далее – ИКТ). ИКТ – это процессы и методы создания, обработки, распространения информации, а также способы и средства их осуществления[14].

---

[13] Уголовный Кодекс Российской Федерации. Доступ СПС «ГАРАНТ»

[14] Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (29.06.2021). Доступ из СПС «Гарант».

Таким образом, определение ИКТ в соответствии с проектом Конвенции ООН описывает техническую часть понятия киберпреступление, а именно, реализацию механизмов в информационной сети. На наш взгляд, чтобы определить киберпреступление, необходимо подчеркнуть трансграничный характер и противоправную общественно опасную направленность данного деяния, совершаемого частными акторами в целях квалификации киберпреступления в качестве преступления международного характера. В данном контексте трансграничность киберпреступления характеризуется в отсутствии каких-либо ограничений по субъектному составу и способам совершения, поскольку информационное пространство не имеет границ, и его последствия выходят за пределы правопорядка отдельного государства в силу степени общественной опасности.

Для работы над проектом Конвенции ООН был учрежден ad hoc комитет – Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (далее – Спецкомитет). Это межправительственный комитет экспертов открытого состава, представляющий все регионы, который и будет заниматься разработкой текста Проекта ООН. Спецкомитет должен провести не менее шести сессий. Первая сессия комитета проходила с 28 февраля по 11 марта 2022 года. Результатом работы комитета должен стать проект Конвенции ООН. 21 апреля 2023 года завершилась пятая сессия Спецкомитета по киберпреступности в Вене. Всего Спецкомитету поручено провести шесть сессий с августа 2021 года по конец июня 2024 года и заключительную сессию в 2024 году. Резолюцией ГА ООН 79/243 от 24 декабря 2024 года принята Конвенция ООН против киберпреступности.

В предложенном Российской Федерацией проекте Конвенции ООН отсутствует определение понятия киберпреступление. Тем не менее проект Конвенции ООН соответствует современным вызовам и угрозам в сфере международной информационной безопасности, а также создает

благоприятные условия для сотрудничества в части выявления, расследования и преследования злоумышленников за совершенные киберпреступления. России и тем государствам, которые поддерживают принятие вышеназванного документа, видится проект Конвенции ООН, как универсальный международный уголовно-правовой механизм, который способен сфокусироваться на киберпреступлениях, бороться с противоправным применением ИКТ и носящий по своему содержанию всеобъемлющий характер[15].

С точки зрения уголовного права любое преступление может быть определено во внутреннем законодательстве государств. Преступление в глобальной сети «Интернет» трактуется, как противоправное деяние против информационных технологий и компьютерной информации[16]. Это любое деяние, которое государство квалифицирует как преступление и налагает на него санкции[17]. Традиционно правонарушения и санкции за них устанавливаются независимо от средств, использованных для совершения такого правонарушения. Рост числа разнообразных форм преступлений обусловил необходимость классификации некоторых преступлений, создания законодательной базы и наказания за них[18].

В научной литературе также отсутствует единая позиция относительно понятия киберпреступление. Зарубежные ученые используют термин cybercrime (киберпреступление), который внесен в оригинальное название Конвенции СЕ – (Convention on Cybercrime).

Следует отметить, что проблема киберпреступлений стала объектом научных исследований в зарубежных странах с прошлого века. Данный термин был введен в оборот в научных кругах в начале 1960-х гг. в США

---

[15] Кибермафия. Мировые тенденции и международное противодействие: монография / Ю.Н. Жданов, С.К. Кузнецов, В.С. Овчинский; вступ. ст. О.В. Храмова. – Москва: Норма, 2022. – 175 с.
[16] Black's Law Dictionary, 9th Ed., p.427.
[17] The life of criminal law begins with criminalization; to criminalise an act-type is to make it a crime to commit tokens of that type. See Stanford Encyclopedia of Philosophy. (2018). Theories of Criminal Law**.** URL: https://plato.stanford.edu/entries/criminal-law/ (дата обращения: 18.07.2024). – Текст: электронный.
[18] Aaron, A. (2019). *A legal Analysis of Cybercrime and Cyber Torts: Lessons for Nigeria*. [LL. B Thesis, University of Lagos], p.6.

исследователем Д.Б. Паркер. Исследователь отмечает, что «электронно-вычислительная машина (ЭВМ) является как объектом преступления, так и орудием, используемым для получения политических или деловых преимуществ»[19].

По мнению К. Уилсона киберпреступление – это противоправное деяние, которое осуществляется посредством ЭВМ. К киберпреступлениям относятся такие противоправные действия, как кража интеллектуальной собственности, нарушения коммерческой тайны или авторских прав; хакерские атаки на сети ЭВМ с целью преднамеренного нарушения обработки данных или шпионаж с целью получения доступа к секретным данным. Террористические атаки на сети ЭВМ, использование сети «Интернет» с целью распространения террористической идеологии, пропаганда терроризма и иные преступления, связанные с террористической деятельностью, также относятся к киберпреступлениям[20].

Уильям А. Оуэнс определяет киберпреступление, как противоправное деяние с использованием ЭВМ, с целью уничтожения компьютерной системы, информации или программного обеспечения. Киберпреступления направлены на то, чтобы поставить под угрозу компьютерную безопасность путем уничтожения информации, подрыва работы компьютерных систем, а также нарушая потока обмена информации в сети «Интернет»[21].

Ажетунмоби Р.Л. отмечает, что непрерывное развитие технологий затрудняет дать точное определение киберпреступления[22]. Он также отмечает, что определение должно включать в себя знание или использование компьютерного преступления[23].

---

[19] Parker D.B. 1989. *Computer crime Criminal Justice Resource Manual.* Cambridge, Mass.; Department of Justice. 223 p.
[20] Clay Wilson. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, p. 4. 2008.
[21] William A Owens and others (eds), Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities (National Academies Press 2009) 10–11.
[22] Ajetunmobi, R.L. (2015). Cybercrimes (Prohibition, Prevention, etc. Act 2015: A Review" (2014-2015) *NIALS Journal of Intellectual Property, 17* p.171.
[23] Ajetunmobi, R.L. (2015). Cybercrimes (Prohibition, Prevention, etc. Act 2015: A Review" (2014-2015) *NIALS Journal of Intellectual Property, 17* p.171.

Профессор Ладан описывает киберпреступление, как преступление, которое использует современные технологические сети, где электронно-вычислительные машины используются для противоправной деятельности[24].

Иной подход постулирует о том, что киберпреступление – это преступление, где ЭВМ представляют собой цель этого преступления или используются в качестве инструмента для совершения правонарушения[25].

Самули Хаатаджа под киберпреступлением понимает противоправное деяние, выраженное в нанесения ущерба посредством информационно-коммуникационных технологий государству как информационному объекту, вызывая увеличение энтропии[26].

Таким образом, доктринальные позиции зарубежных ученых, касающиеся определения термина «киберпреступление» сводятся к тому, что данное деяние направлено на подрыв информационной безопасности через противоправное использование ИКТ, и носит экстерриториальный характер.

Отечественные ученые в большей степени используют терминологию, соответствующую официальному подходу, закрепленному в УК РФ, где данный вид преступлений определен через родовой объект как «преступления в сфере компьютерной информации».

В России научное обсуждение проблемы борьбы с киберпреступлениями началось в начале 90-х годов, с момента создания межведомственного семинара «Криминалистика и компьютерная преступность», который был организован НИИ Проблем укрепления законности и правопорядка при Генеральной прокуратуре РФ и ЭКЦ МВД России. На занятии семинара в марте 1993 года, когда обсуждался вопрос о состоятельности термина «компьютерные преступления», ему было дано следующее определение: «предусмотренные уголовным законом общественно опасные действия, в

---

[24] Ladan, M.T. (2015). Overview of the 2015 Legal and Policy Strategy on Cybercrime and Cybersecurity in Nigeria.*Prof. M.T. Ladan's Law and Policy Review Research Working Papers, Faculty of Law,* Ahmadu Bello University, p. 2.

[25] Techopedia. Cybercrime" URL: https://www.techopedia.com/definition/2387/cybercrime/.

[26] Haataja, Samuli. Cyber Attacks and International Law on the Use of Force (Emerging Technologies, Ethics and International Affairs). 2020. p. 2.

которых машинная информация является либо объектом, либо средством преступного посягательства»[27]. Указанное понятие не содержало указание ни на виновный характер посягательства, ни на последствия или возможность их наступления в результате совершения общественно опасного деяния.

И.А. Петрова определяет преступления в сфере компьютерной информации, как противоправное виновно-совершенное общественно-опасное деяние, наказуемое в уголовном порядке, посягающее на общественные отношения по безопасному производству, хранению, передаче, поиску, использованию, распространению или защите компьютерной информации, причинившее или создающее угрозу причинения вреда охраняемым законом права и интересам физических и (или) юридических лиц, общества, государства[28].

И.Н. Васильева трактует преступления в сфере компьютерной информации, как запрещенное УК РФ под угрозой наказания виновно совершенное общественно опасное деяние, посягающее на общественные отношения, связанные с правомерным и безопасным использованием охраняемой законом компьютерной информации[29].

По мнению А.Н. Попова, преступления в сфере компьютерной информации – это законодательное определение преступлений, предусмотренных главой 28 УК РФ.

А.Н. Попов в своей монографии обращает внимание на определение компьютерное преступление, у которого отсутствует четкий и единый термин. Компьютерное преступление может трактоваться в качестве синонима преступления в сфере компьютерной информации. Автор полагает, что

---

[27] Селиванов, Н. А. Проблемы борьбы с компьютерной преступностью / Н. А. Селиванов // Законность. – 1993. – No 8.

[28] Петрова И.А., Лобачев И.А. 2020. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств. – *Журнал прикладных исследований.* No1. С.52–62.

[29] Расследование инцидентов информационной безопасности: учебное пособие / И. Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 5 с.

преступления в сфере компьютерной информации – это нормативное определение преступлений, закрепленное в УК РФ[30].

А.В. Суслопаров трактует киберпреступления, как информационные преступления, и понимает под ними общественно-опасные противоправные деяния, причиняющие вред общественным отношениям по обеспечению информационной безопасности личности, общества и государства, способом совершения которых является информационное воздействие или (и) предметом которых является информация как особый нематериальный объект[31].

С.И. Буз определяет киберпреступление, как любое противоправное деяние, совершенное в информационном пространстве, либо при помощи информационных технологий[32].

Перед тем, как дать собственное определение киберпреступления, автор считает целесообразным раскрыть объект, объективную сторону, субъект и субъективную сторону киберпреступлений.

Исходя из анализа действующих на сегодняшний день международных соглашений в части противодействия киберпреступлениям, объектом киберпреступлений являются различного рода общественные отношения, блага, а также социальные ценности (человек, его права и свободы; собственность; государственный строй; мир и безопасность человечества и т.д..), которые появляются при реализации компьютерных процессов в части обработки компьютерных данных. Под объективной стороной киберпреступления понимается общественно опасное деяние, связанное с несанкционированным доступом к компьютерным системам, и причинением вреда в части прав и свобод человека или национальным интересам государства. Под субъект киберпреступлений может подпадать, как

---

[30] Попов А. Н. *Преступления в сфере компьютерной информации. Учебное пособие.* Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. С. 4–11.

[31] Суслопаров А. В. Компьютерные преступления как разновидность преступлений информационного характера. Дисс. ... канд. юрид. наук. Владивосток. 2010. С. 32–56.

[32] Буз С. И. 2019. Киберпреступления: понятие, сущность и общая характеристика. – Юрист-Правоведъ. No4. С.78–82.

отдельный индивид, так и организованные преступные группы, находящиеся в разных территориальных юрисдикциях. Под субъективной стороной понимаются киберпреступления, влекущие наступление ответственности только в случае их совершения умышленно.

Резюмируя вышесказанное, можно сделать вывод о том, что трансграничный характер киберпреступления позволит максимально эффективно защитить публичные интересы и задействовать международно-правовые механизмы в поимке преступника, а также предотвратить последствия этого противоправного деяния. Несмотря на то, что в каждом национальном законодательстве существует регулирование киберпреступлений, механизмы противодействия будет затруднительно задействовать, если это будет только внутригосударственное регулирование. Международные механизмы борьбы против киберпреступлений осуществимы на основе международных соглашений и в рамках деятельности международных органов, организаций. Более того, последствиями киберпреступлений является причинение ущерба как материального, так и нематериального характера. К первой категории отнесем такой вид «киберпреступления» как кибертерроризм, который может привести к разрушению экономической инфраструктуры. Ко второй категории отнесем кибербуллинг, который может наступить вследствие посягательства на честь и достоинство граждан и в дальнейшем привести к фатальным последствиям. Выработка консолидированной позиции в отношении определения киберпреступление остается открытым. Вышеперечисленные международные соглашения не содержат единообразно понимаемого и применяемого нормативно-закрепленного определения киберпреступление. На внутригосударственном уровне больше принято говорить о преступлениях в сфере компьютерной информации, однако, УК РФ не содержит определение данного понятия. Плюрализм доктринальных взглядов, как у отечественных, так и у зарубежных исследователей в части определения термина киберпреступление говорит нам о сложности данного феномена. Однако стоит

отметить тот факт, что киберпреступления направлены на подрыв информационной безопасности. В этом концепции ученых совпадают. На международном уровне отсутствует универсальная новая Конвенция, которая внесла бы ясность в то, что из себя представляет киберпреступление, определила полный перечень видов киберпреступлений и какое наказание предусмотрено за то или иное правонарушение в сети «Интернет». На наш взгляд, выработка четкого определения является необходимым фактором для дальнейшей квалификации данного рода правонарушений в сети «Интернет». Считаем, что термин «киберпреступление» в международном праве можно определить следующим образом. Киберпреступление – это виновно совершенный, несанкционированный доступ к информационно-коммуникационным технологиям при помощи компьютерных устройств и иных технических средств, с целью нанесения как материального, так и нематериального ущерба и влекущее негативные последствия трансграничного характера неограниченному круг лиц.

§ 2. Виды киберпреступлений согласно современным международно-правовым актам

Перечень киберпреступлений зафиксирован практически во всех международных соглашениях в части преступлений в сфере информационных технологий. Наибольший интерес для целей работы представляет сравнительно-правовой анализ Конвенции СЕ с Директивой N 2013/40/ЕС Европейского парламента и Совета Европейского Союза об атаках на информационные системы и о замене Рамочного Решения 2005/222/ПВД (далее – Директива ЕС), Соглашением СНГ, Соглашением ШОС, Конвенцией АС, а также проектом Конвенции ООН и УК РФ. Европейский опыт правового регулирования данного вопроса является наиболее наработанным и практически апробированным.

Киберпреступления, содержащиеся в Конвенции СЕ, в общей сложности образуют 10 видов. В свою очередь компьютерные преступления поделены на 4 раздела:

1) Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;
2) Правонарушения, связанные с использованием компьютерных средств (подлог, мошенничество);
3) Правонарушения, связанные с содержанием данных (детская порнография);
4) Правонарушения, связанные с нарушением авторского права и смежных прав.

В свою очередь, Директива ЕС содержит 4 вида киберпреступления.

Конвенция СЕ и Директива ЕС содержат схожие положения. Оба документа имеют общую основу, состоящую из трех уголовных преступлений относительно конфиденциальности, целостности и доступности компьютерных данных и систем. Первый – противозаконный доступ (ст. 2 Будапештская Конвенция СЕ) и незаконный доступ к информационным системам (ст. 2 Директивы ЕС), заключается в преднамеренном доступе к компьютерной системе без права на это.

Оба соглашения позволяют государствам требовать, чтобы такие деяния считались преступными, если они совершены с нарушениями мер безопасности[33]. Эти положения должны предоставить гибкость национальным правовым системам. Они также учитывают компромисс между чрезмерной криминализацией (и, таким образом, стремлением наказать все незаконные доступы) и конкретным отбором преступных незаконных доступов (тем самым стимулируя граждан к защите компьютерных данных и системы). Требование, чтобы такие деяния считались преступными, если они совершены

[33] Weyembergh, Anne. 2005. Approximation of criminal laws, the Constitutional Treaty and The Hague Programme. Common Market Law Review, p. 42.

с нарушениями мер безопасности, является, пожалуй, наиболее разумным и эффективным подходом к криминализации незаконного доступа[34].

Другое противоправное деяние с использованием ИКТ– воздействие на функционирование системы (ст. 5 Будапештской Конвенции СЕ) и нарушение неприкосновенности системы (ст. 3 Директивы ЕС). Системное вмешательство происходит, когда кто-то намеренно мешает или прерывает работу компьютера путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения, подавления или делает недоступными компьютерные данные.

Третьим общеуголовным преступлением является воздействие на данные (ст. 4 Будапештской Конвенции СЕ) и нарушение неприкосновенности данных (ст. 4 Директивы ЕС). Данный вид киберпреступления заключается в самых разнообразных формах противоправного деяния с использованием ИКТ (нанесение ущерба, удаление, повреждение, изменение, подавление), влияющие на компьютерные данные.

Определения трех основных противоправных деяний с использованием ИКТ, содержащихся в двух международных соглашениях, во многом совпадают[35]. В действительности гармонизация уголовного права не должна быть направлена на унификацию или точное соответствие национальному законодательству, а скорее устранять трения и несоответствия между национальными законами[36].

Помимо вышеописанных противоправных деяний с использованием ИКТ, Конвенция СЕ имеет в своем перечне иные киберпреступления, такие как незаконный перехват, неправомерное использование устройств, преступления,

[34] Brenner, Susan W., and Leo L. Clarke. 2005. Distributed Security: Preventing Cybercrime. John Marshall Journal of Computer & Information Law, 23, no. 4: 659-709.
[35] Mercado Kierkegaard, Sylvia. 2006. Here comes the «cybernators!». Computer Law & Security Report, 22, no. 5: 381-391.
[36] Calderoni, Francesco. 2008. A Definition that Could not Work: The EU Framework Decision on the Fight against Organised Crime. European Journal of Crime, Criminal Law and Criminal Justice, 16: 265-82.

связанные с компьютером (подделка документов и мошенничество) и преступления, связанные с контентом (детская порнография)[37].

Согласно позициям деятелей науки в сфере ИКТ и международного права, вышеназванный документ малоэффективен и несовершенен. Конвенция СЕ охватывает неполный перечень киберпреступлений. По словам бывшего Генерального секретаря МСЭ Х. Туре, Конвенция СЕ «немного запылилась». За время после появления данного соглашения появились новые киберпреступления. Причем киберпреступления более масштабные и направленные на большие группы людей и сами государства. Например, реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности.

Анализ юридической техники положений Конвенции СЕ позволяет сделать следующий вывод. Составители данного международного соглашения в большинстве своем европейские государства, где страны связаны между собой тесными политико-правовыми отношениями, культурой и историей. Поэтому для них естественен свободный доступ к киберпространству друг с другом. Остальные страны, в том числе Российской Федерации, имеющие конкурирующие политические и экономические интересы в региональном и общемировом масштабе, положение о полной прозрачности собственного киберпространства может быть критичным и маловероятным[38].

Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 года является значимым договором регионального характера в данной сфере, в том числе для Российской Федерации. Статья 3 (уголовно наказуемые деяния) перечисляет 8 видов киберпреступлений. Среди неосвещенного в Конвенции СЕ киберпреступления можно выделить следующее преступление в сфере

---

[37] Downing, Richard W. 2005. Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime. Columbia Journal of Transnational Law, 43, no. 3: 705-711.

[38] 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.

информационных технологий: распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма. Остальные преступления в сфере информационных технологий совпадают с теми киберпреступлениями, что закреплены в Конвенции СЕ.

В статье 2 (основные угрозы в области обеспечения международной информационной безопасности) Соглашения ШОС о сотрудничестве в области обеспечения международной информационной безопасности перечислены угрозы, которые можно приравнять к киберпреступлениям. Среди неосвещенных таких угроз, которые не обозначены в Конвенции СЕ, можно выделить, например, информационный терроризм, а также разработку и применение информационного оружия, подготовку и ведение информационной войны. Стоит также отметить, что вышеприведенное соглашение регионального характера содержит подробное писание форм и механизмов сотрудничества в части противодействия киберпреступлениям.

Перечень киберпреступлений перечислен в статье 29 (правонарушения, связанные с ИКТ) Главы 2 (уголовные положения) Конвенции Африканского союза о кибербезопасности и защите персональных данных от 2014 года. Данная статья содержит 4 пункта. Четвертый пункт конвенции Африканского союза о кибербезопасности гласит, что цифровые доказательства должны быть представлены в ходе судебного разбирательства и обсуждаться в присутствии судьи. Таким образом, заключительный пункт статьи 29 конвенции не раскрывает сущность данного вида киберпреступления, а указывает на гармонизацию национальных законодательств государств-участников в части уголовно-процессуальной деятельности. Данное положение не закреплено в Конвенции СЕ. Первые три пункта конвенции Африканского союза совпадают с теми киберпреступлениями, которые закреплены в Конвенции СЕ.

В свою очередь, проект Конвенции ООН охватывает 22 вида киберпреступлений. Проект Конвенции ООН дублирует 10 видов киберпреступлений, содержащиеся в Конвенции СЕ, а также вводит новые 12 видов преступлений в сфере ИКТ, которые в Конвенции СЕ не освещены. Также в вышеназванном проекте прописан порядок взаимодействия государств в вопросах выдачи киберпреступников и оказания правовой помощи уголовным делам, включая выявление, арест, конфискацию и возврат активов. Перед тем как приступить к анализу видов киберпреступлений, прописанных в проекте Конвенции ООН, считаем необходимым осветить такой вид киберпреступления, как кибербуллинг, который не закреплен в международных договорах.

Изначально само определение кибербуллинга было дано Биллом Белсеем, который обозначил его как применение ИКТ в целях недружественного поведения и нанесения вреда пользователям[39].

В Российской Федерации понятийно-категориальный аппарат в отношении кибербуллинга не установлен, так как отсутствует легальная дефиниция. С. И. Ковалева считает, что кибербуллинг является одной из форм киберпреступления и определяет его, как перманентное направление сообщений, которые содержат информацию, содержащую унижающий достоинства контент. Отличительной особенностью кибербуллинга по мнению С.И. Ковалевой является так называемая онлайн-агрессия, когда пользователь может пострадать как в эмоциональном, так и в физическом плане. Последствия из-за онлайн-агрессии у потерпевшего могут быть следующими: апатия, суицидальные мысли и замыкание в себе. Прежде всего это касается лиц, не достигших совершеннолетнего возраста, чья психика еще не до конца сформировалась. Самый действенный и эффективный способ защиты от такого рода противоправного деяния посредством ИКТ является установление настроек конфиденциальности своей страницы в социальных сетях,

[39] Belsey B. Cyberbullying: An emerging threat to the «always on» generation. URL: http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf (дата обращения: 18.07.2024). – Текст: электронный.

блокирование нежелательных пользователей и внесение их в черный список. Таким образом можно обезопасить себя от кибербуллинга[40].

В качестве примера можно привести Ирландию, где в 2021 году приняли так называемый «Закон Коко», предусматривающий лишение свободы на срок до 7 лет для тех, кто выставляет на всеобщее обозрение в сети «Интернет» интимные изображения человека без его согласия. Николь Фокс повесилась в возрасте 21 года после того, как в течение 3 лет подвергалась физическому и виртуальному насилию. После смерти, затравленной в соцсетях гражданки Ирландии, в ЕС готовится закон против кибербуллинга.

В деле Geoffrey Andare v Attorney general & 2 others (2016) Высокий суд Кении признал неконституционным положение, предусматривающее уголовную ответственность за оскорбительные высказывания, а также клевету, которые вызывают раздражение и причиняют беспокойство, поскольку оно является расплывчатым и неоправданно ограничивает свободу выражения мнения. Дело возникло из-за сообщения Джеффри Андаре в социальной группе Facebook (запрещенный на территории РФ), в котором он обвинил Титуса Куриа, представителя стипендиального фонда, в использовании своего служебного положения для того, чтобы проводить ночи с девушками, претендующими на стипендии. Курия подал жалобу на Андаре в соответствии с разделом 29 кенийского Закона об информации и связи, который предусматривает уголовную ответственность за порочащую честь или ложную информацию. Пока дело рассматривалось в уголовном суде, Андаре подал петицию с целью оспорить конституционность раздела 29. Высокий суд постановил, что раздел 29 является неконституционным, поскольку он необоснованно ограничивает свободу выражения мнений, а также потому, что он сформулирован нечетко[41].

---

[40] Ковалева С. Е. О некоторых актуальных социально-психологических проблемах виртуальной коммуникации в информационную эпоху // XXI век: итоги прошлого и проблемы настоящего плюс. 2017. No 5-6. С. 122–127.

[41] Republic of Kenya in The High Court of Kenya at Nairobi Milimani Law Courts Constitutional and Human Rights Division Petition № 149 of 2015. (Geoffrey Andare v Attorney general & 2 others).

В Российской Федерации кибербуллинг на законодательном уровне не закреплен. Однако в Объединенных Арабских Эмиратах на национальном уровне существует Федеральный Закон № 5 от 2012 года о борьбе с киберпреступностью, который содержит положения об оскорблениях в сети «Интернет» и предусматривает достаточно серьезное наказание в виде реального тюремного срока и депортацией для экспатов. В 2018 году Президент Объединенных Арабских Эмиратов Халифа ибн Зайд аль-Нахайян издал указ о принятии ряда поправок к Федеральному Закону № 5 от 2012 года о борьбе с киберпреступностью, которые в значительной степени смягчили санкции за кибербуллинг. Реальный тюремный срок и обязательная депортации для экспатов заменились на запрет пользоваться «Интернетом» в течение определенного периода времени и денежным штрафом[42].

Таким образом, кибербуллинг – это оскорбления в сети «Интернет» с использованием цифровых технологий. Кибербуллинг может происходить в социальных сетях, на платформах обмена сообщениями, игровых платформах и в мобильных устройствах. Это киберпреступление представляет собой угрозы, диффамации, намеренные оскорбления и осуществляется в информационном пространстве через информационно-коммуникационные каналы и средства ЭВМ[43].

Важно понимать, что кибербуллинг может осуществляться как одним лицом, так и группой, и направлен на определённого человека при помощи ИКТ в целях унижения его чести и достоинства, запугивания или причинения иного морального вреда. Однако последствия данного противоправного деяния посредством ЭВМ носит публичный характер. Потерпевшими от кибербуллинга могут быть как лица, не достигшие совершеннолетнего возраста, так и совершеннолетние лица[44]. Кибербуллинг в отсутствие

---

[42] Federal Decree-Law no. (5) of 2012 ON COMBATING CYBERCRIMES. United Arabic States. Issued on 25 Ramadan 1433 AH. Corresponding to 13 August 2012.

[43] Аббуд Р.Р. Актуальные проблемы международного права в части киберпреступлений – «Актуальные проблемы международных отношений и международного права», Сборник статей под редакцией Т.В. Кашириной, С.А. Агуреева, Воробьева С.В., Москва, 2021, Дипломатическая академия МИД России.

[44] *Duggan M.* Online harassment // URL: http://www.pewinternet.org/2014/10/22/part-1-experiencing-online- harassment/ (дата обращения: 18.07.2024). – Текст: электронный.

юридического регулирования является проблемой моральных и культурных ценностей, выражением отрицательного мнения в безнравственной форме. Так как на данный момент отсутствуют юридические механизмы защиты против кибербуллинга, то наилучшим способом защититься является самозащита. Например, установка настроек конфиденциальности в приложениях, а также коллективная защита, когда пользователи становятся на защиту потерпевшего.

Более того, к одному из современных видов киберпреступлений можно отнести дипфейки. Дипфейк – это генерация изображения или голоса, которая основана на ИИ. Киберпреступники посредством ИИ переделывают фотографии или видеозаписи своей жертвы в порнографические ролики. Во многом ИИ облегчил задачу преступникам. Злоумышленники обнаруживают такие механизмы в области ИИ, которые доступны и просты в эксплуатации и не требуют специального обучения. Дипфейк-порно осуществляется путем перемещения фотографии лица в видео эротического характера. Далее видео размещается на разных платформах. Преступники совершают данное противоправное деяние при использовании ИКТ из-за корыстных побуждений в целях мести, выкупа, дискредитации или, например, в целях развлечения. В основном жертвами преступников становятся лица, не достигшие совершеннолетнего возраста. Кроме того, с помощью ИИ можно сгенерировать голос любого человека. Например, возможно сымитировать голос человека посредством использования модифицированного алгоритма трансформации текстового содержания в речь и обработкой нейросетью аудиозаписей речи любого человека.

Другим видом киберпреступления, который не отображён ни в одном из международных соглашений является криптоджекинг. Криптоджекинг – это противоправное использование технических средств преступниками в целях получения криптовалюты. Особенность криптоджекинга заключается в трудности обнаружения, так как он скрыт от жертвы. Данный вид киберпреступления представляет собой угрозу, которая интегрируется в компьютерные системы или мобильные гаджеты, и в дальнейшем использует

данные девайса в целях получения криптовалюты. Криптовалюта – это электронные деньги. Биткойн является самой известной криптовалютой. Криптовалюты используют для работы блокчейн (распределенная база данных). В целях создания нового блокчейна необходима добыча вычислительной мощности, и криптовалюта является платой за вычислительные ресурсы, а тех, кто занимается обменом, называют майнерами. Большие компании по майнингу криптовалюты нанимают майнеров в целях управления майнинг-фермами, которые осуществляют вычислительные расчеты. Соответственно преступники, которые совершают криптоджекинг, хотят получить прибыль от майнинга криптовалюты, не неся убытков. Больше всего преступников интересует криптовалюта Monero, которую затруднительно отследить, так как добывается на персональных компьютерах. Таким образом, криптоджекинг помогает преступникам получать криптовалюты, не неся при этом видимых расходов: не оплачивать огромные счета за электроэнергию и специальное оборудование для майнинга.

Другим противоправным деянием, направленным в отношении личной собственности, является кардинг. Кардинг – это форма кражи личных данных, при которой человек использует информацию о чужой кредитной карте для оплаты покупок или снятия средств со счета. Мошенничество с кредитными картами также включает мошенническое использование дебетовой карты и может быть совершено путем кражи самой карты или незаконного получения учетной и личной информации владельца карты, включая номер карты, пароль карты, имя и адрес владельца карты.

По данному виду киберпреступления, содержащемуся в проекте Конвенции ООН, существует внутригосударственная судебная практика. Национальные суды с такого рода преступлениями уже столкнулись.

Впервые о кардинге заговорили в 1994 году, когда Левин В. Л., находясь в России смог перевести несколько миллионов долларов со счетов банка США Citibank. Данный кейс стал первым в истории, когда киберпрестпуление обрело трансграничный характер. Левин В. Л. был арестован в

Великобритании, а затем экстрадирован в США, где его приговорили к 36 месяцам заключения под стражу.

Так, в деле США против Романа Селезнева, 21 апреля 2017 года Окружной Суд Соединенных Штатов по Западному Округу Вашингтона в Сиэтле приговорил к 30 годам тюремного заключения ответчика[45]. Сторона обвинения заявляла, что г-н Селезнев путем мошеннических действий с использованием ИКТ украл личную информацию американских граждан с банковских карт. Вследствие чего обвиняемый получил незаконную прибыль в размере 2-ух миллионов долларов США. Г-н Селезнев был задержан в международном аэропорту Мальдив. Стоит отметить, что между Мальдивами и США отсутствует договор об экстрадиции иностранных граждан.

В марте 2021 года, в деле США против Сергея Медведева, американский суд штата Невады приговорил россиянина к 10 годам тюремного заключения. Сергей Медведев являлся соучредителем преступной транснациональной организации хакеров под названием Infraud Organization и занимал должность администратора. Члены данной преступной организации занимались кражей личной информации с банковских карт, а также финансовым мошенничеством. По данным Минюста США, жертвами транснациональной организацией хакеров Infraud Organisation стали более миллиона людей со всех 50 штатов США, а финансовые убытки, связанные с деятельностью организации, превысили 586 миллионов долларов США[46].

Как видим, данные преступления по своему характеру могут не ограничиваться территорией одного государства. Более того, существует вещевой кардинг, который является разновидностью кардинг. По сравнению с реальным кардингом, вещевой кардинг является менее масштабным. Он направлен на приобретение товаров в онлайн-магазинах, посредством оплаты с чужой кредитной карты. Одним из способа совершения такого рода

---

[45] UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON AT SEATTLE NO. CR11-0070RAJ SENTENCING MEMORANDUM. April 14, 2017.

[46] UNITED STATES DISTRICT COURT CLARK COUNTY, NEVADA. Case No. 2:17-cr-00306-JCM-VCF. 2nd day of April, 2021.

киберпреступления – совершить взлом онлайн-магазина, где клиенты совершают покупку в сети «Интернет».

Проект Конвенции ООН содержит следующие виды киберпреступлений.

1) *Неправомерный доступ к цифровой информации.*

Является одним из первых видов киберпреступлений и больше трактуется как незаконный доступ к компьютерной системе[47].

Под неправомерным доступом к цифровой информации понимается противоправный доступ к компьютерной информации с целью ее блокирования, копирования, модификации или уничтожения.

Растущее число незаконного доступа к цифровой информации обусловлена тремя аспектами:

– созданием программных инструментов, которые автоматизируют атаки;

– слабой защитой компьютерных систем;

– возрастанием роли персональных компьютеров, как цели атак киберзлоумышленников.

2) *Неправомерный перехват.*

Данный вид киберпреступления представляет из себя противоправное деяние в киберпространстве и осуществляется без соответствующих прав или с нарушением установленных норм, в том числе с использованием технических устройств перехвата технических параметров трафика и данных, обрабатываемых с использованием ИКТ и не предназначенных для массового использования.

3) *Неправомерное воздействие на цифровую информацию.*

Неправомерное воздействие на цифровую информацию включает в себя ее умышленное повреждение, изменение, удаление, модификацию, блокирование либо копирование информации в цифровой форме.

---

[47] Понимание киберпреступности: явление, задачи и законодательный ответ: отчет Международного Союза Электросвязи (МСЭ), 2014. URL: http://www.itu.int/ (дата обращения: 18.07.2024). – Текст: электронный.

4) *Нарушение функционирования информационно-коммуникационных сетей.*

Данный вид киберпреступления направлен на умышленное нарушение функционирования информационно-коммуникационных сетей, путем ввода, удаления, блокирования или модификации компьютерных данных.

Анализируя 4 вышеприведенных киберпреступления, можно сделать вывод, что они направлены против трех ключевых постулатов международной информационной безопасности: конфиденциальности, целостности и доступности информации. Исследователи в области информационной безопасности именуют ее как триаду CIA (confidentially, integrity, availability)[48].

5) *Создание, использование и распространение вредоносных программ.*

Данное киберпреступление направлено на разработку или реализацию бот-сети (сеть компьютеров, зараженных вредоносным ПО) в целях совершения несанкционированного воздействия на электронные данные; хищение электронных данных посредством ИКТ; противозаконный доступ к персональным данным[49]. Кроме того, данное противоправное деяние в сфере компьютерной информации направлено на удаление электронных данных, а также модификации и блокированию.

Вредоносность программ обуславливается тем, что все действия осуществляются в отсутствии уведомления непродвинутого пользователя, который может не подозревать о существовании таких программ.[50]

Вредоносная программа используется для заражения компьютерных систем с целью модификации работы системы, а также уничтожения системы или их данных. Статья 3(б) Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями

[48]Актуальные вопросы защиты информации: монография / А.В. Бабаш, Е. К. Баранова. – М.: РИОР: ИНФРА-М, 2017. 87 с.

[49] Hogben, G. (ed.) 2011. Botnets: Detection, Measurement, Disinfection and Defence. European Network and Information Security Agency (ENISA).

[50] Ефремова М. А. К вопросу об уголовной ответственности за создание, распространение и использование вредоносных компьютерных программ // Информационное право. 2015. No 3. С. 12.

в сфере компьютерной информации 2001 года запрещает «создание, использование или распространение вредоносных программ»[51]. Приведем перечень актуальных видов вредоносных программ, которые используют киберпреступники:

а) *Червь*. Относится к вредоносной программе, которая реплицирует себя, автоматически распространяясь по сети.

б) *Компьютерный вирус*. Компьютерный вирус – это тип вредоносного программного обеспечения, который распространяется между компьютерными устройствами и наносит урон информационным данным и программному обеспечению.

в) *Троянский конь*. Вредоносная программа, намеренно разработанная для уничтожения информации или для того, чтобы можно было ее украсть.

г) *Шпионская программа*. Шпионская программа — это вредоносное программное обеспечение, которое проникает в компьютер пользователя, собирает данные с устройства и пользователя, и отправляет их третьим лицам без их согласия.

д) *Вирус-вымогатель*. Является особым типом вредоносных программ, которые удерживают данные в обмен на выкуп. Угрожает опубликовать, заблокировать, испортить данные или лишить пользователя возможности работать или получать доступ к своему компьютеру, если он не выполнит требования злоумышленника[52].

6) *Неправомерное воздействие на критическую информационную инфраструктура.*

Данный вид киберпреступления представляет из себя противоправное воздействие на системы ИКТ, которые являются критическими инфраструктурами или необходимы объектами для функционирования критических инфраструктур. Например: телекоммуникации, транспорт, ЭВМ,

---

[51] СОГЛАШЕНИЕ о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 года). Доступ из СПС «Гарант».
[52] Maras, Marie-Helen. (2014). *Computer Forensics: Cybercriminals, Laws and Evidence*, second edition. Jones and Bartlett.

программное обеспечение, сеть «Интернет», промышленные системы, используемые для управления производством и распределением энергии, процессами химического производства и переработки[53].

7) *Несанкционированный доступ к персональным данным.*

Защита персональных данных осуществляется в соответствии с правом на неприкосновенность частной жизни, предусмотренном в международных договорах в области прав человека.

Проект Конвенции ООН гарантирует основные права и свободы человека. В подтверждении можно привести статью 7 (несанкционированный доступ к персональным данным). Защита персональных данных осуществляется в соответствии с правом на неприкосновенность частной жизни, предусмотренном в международных договорах в области прав человека.

8) *Незаконный оборот устройств.*

Похожее наименование и содержание данного вида киберпреступления можно найти в статье 6 Конвенции Совета Европы под названием – противозаконное использование устройств. Незаконный оборот устройств представляет из себя неправомерный доступ и воздействие на цифровую информацию; хищение цифровой информации с использованием информационно-коммуникационных технологий; несанкционированного доступа к персональным данным; нарушение функционирования информационно-коммуникационных сетей.

9) *Хищение с использованием информационно-коммуникационных телекоммуникаций.*

Одним из самых распространенных хищений посредством использования ИКТ является фишинг. Фишинг (phishing) – это тип угрозы кибербезопасности, направленный непосредственно на пользователей через электронную почту, текстовые или прямые сообщения. Во время одной из таких атак киберзлоумышленник выдает себя за доверенное лицо, чтобы

[53] Директива Совета Европейского Союза 2008/114/ЕС от 8 декабря 2008 г. о европейских критических инфраструктурах и мерах по их защите. Доступ из СПС «Гарант».

украсть данные, например логины, номера счетов и информацию о кредитных картах. Мотивы такого противоправного поведения в основном финансовые.

В отношении коммерческих организаций фишинг может привести к очень серьезным последствиям. Если киберпреступник получит доступ к корпоративной сети, то может произойти утечка данных и тем самым будет нанесен значительный ущерб как организации, так и ее сотрудникам.

Электронная почта является уязвимым компонентом, посредством которого киберпреступники осуществляют фишинг. Однако электронная почта остается наиболее важным средством коммуникации для бизнеса. Таким образом, коммерческим организациям необходимо обеспечить в первую очередь свою электронную почту надежной киберзащитой, чтобы гарантировать себе информационную безопасность от такого вида киберпреступления, как фишинг.

Также к разновидности фишинга относится телефонное мошенничество или голосовой фишинг. В настоящее время является одним из самых распространенных киберпреступлений. Преступники путем уловок, играя роль сотрудника компетентных органов или банка, под разными предлогами выманивают у жертвы денежные средства с их лицевых счетов в банках. Методы существуют следующие. Например: банковское мошенничество, шантаж или непосредственное выманивание денег.

10) *Преступления, связанные с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием ИКТ.*

Данное киберпреступление является распространенным явлением. Статья 15 Конвенции ООН дает подробное описание данного вида киберпреступления, а также определяет понятие «детская порнография» и возрастной ценз «несовершеннолетнего». Положение о преступлении, связанном с детской порнографией также закреплено в Конвенции Совета Европы (ст. 9).

Выявление преступников существенно снизилось благодаря интегрированию средств шифрования, а также приложений со сквозным шифрованием[54]. Более того, преступники используют услуги анонимности, например, виртуальную частную сеть (VPN). К сожалению, растет количество преступлений, связанных с детской порнографией при использовании ИКТ. Пандемия COVID-19 усугубила это противозаконное явление, так как введения рядом стран всеобщего карантина с целью остановить распространение пандемии COVID-19, дети стали проводить больше времени в сети «Интернет» без присмотра родителей и тем самым подвергая себя опасности.

Для того чтобы совершить противоправное деяние с использованием ИКТ в отношении несовершеннолетних онлайн-преступники используют поддельные личные данные и метод груминга (grooming – уход за детьми), чтобы установить дружеские отношения и эмоциональную связь с несовершеннолетними.

Детская порнография обычно создается в домашних условиях и по большей части теми, кто входит в доверительный и близкий круг ребенка[55].

В настоящее время дети имеют свободный и неконтролируемый со стороны родителей доступ к сети «Интернет». В силу отсутствия надлежащего опыта у несовершеннолетних они не способны адекватно оценить противоправные намерения, которое оказывает киберпреступник по другую сторону монитора[56].

Европол располагает более чем 40 миллионами порнографическими изображениями несовершеннолетних со всего мира. В июне 2020 года

---

[54] Eurojust and Europol 2019, Common challenges in combating cybercrime. //URL: https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf. (дата обращения: 18.07.2024). – Текст: электронный.

[55] Australian Institute of Family Studies 2015, Conceptualising the prevention of child sexual abuse,accessibleathttps://acuresearchbank.acu.edu.au/download/5bb2f7760724b150faee97eef3bf9afcfd4cb50e87d7fbab4096c71055c5c82c/1704205/OA_Quadara_2015_Conceptualising_the_prevention_of_child_sexual.pdf (дата обращения: 18.07.2024). – Текст: электронный.

[56] European Union. 2021 – serious and organized crime threat assessment. A CORRUPTING INFLUENCE:THE INFILTRATION AND UNDERMINING OF EUROPE’S ECONOMY AND SOCIETY BY ORGANISED CRIME. P. 39.

полицейская служба Европейского Союза запустила краудсорсинговую кампанию под названием «Остановите жестокое обращение в отношении детей». Материалы с противозаконным контентом регулярно публикуются на официальном веб-сайте Европола. Эти вещественные доказательства в дальнейшем используются для информирования правоохранительных органов и дальнейшего расследования, а также оказания помощи в установлении личности киберпреступников и их жертв[57].

11) *Склонение к самоубийству или доведение до его совершения.*

Данный вид киберпреступления не содержится в Конвенции Совета Европы, однако похожая статья есть в УК РФ (110.1. Склонение к совершению самоубийства или содействие совершению самоубийства). Склонения к самоубийству или доведения до самоубийства, в том числе несовершеннолетних, совершенных посредством оказания психологического и иных видов воздействия в информационно-телекоммуникационных сетях, включая сеть «Интернет».

По данным социальной сети «Вконтакте», за 2021 год было сгенерировано более 3 миллионов сообщений с хештегами, возможно, призывающими к самоубийству от так называемых «групп смерти». Так, 18 июля 2017 года Тобольским районным судом Тюменской области был приговорен Будейкин Филипп (Филипп Лис – под этим именем он был известен в социальных сетях) за доведение несовершеннолетних до самоубийства при помощи социальных сетей к трем годам и четырем месяцам в колонии-поселении. Суд признал виновность и причастность киберпреступника по двум эпизодам, в которых он склонял девочек-подростков к суицидальным мыслям.

[57] Europol 2020, Exploiting isolation – Offenders and victims of online child sexual abuse during the COVID 19 pandemic. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/europol_covid_reportcse_jun2020v.3_0.pdf. (дата обращения: 18.07.2024). – Текст: электронный.

12) *Преступления, связанные с вовлечением несовершеннолетних к совершению противоправных действий, опасных для его жизни и здоровья.*

Вовлечение несовершеннолетних посредством использования ИКТ в совершение противоправных деяний, представляющих опасность для его жизни, является новым видом киберпреступления, которое не зафиксировано в Конвенции Совета Европы, однако существует похожая статья в УК РФ (150. Вовлечение несовершеннолетнего в совершение преступления). В данный вид киберпреступления подпадают такие деяния, как использование ИКТ в противоправных целях, которое может привести к совершению противоправных действий, опасных для жизни и здоровья несовершеннолетнего или в отношении других лиц[58].

Комитет по правам ребенка в своем Замечании общего порядка № 13 о праве ребенка на свободу от всех форм насилия признает, что дети могут быть вовлечены в «создание неподобающих материалов сексуального характера, предоставление вводящей в заблуждение информации или рекомендаций и/или незаконное скачивание, хакерство, азартные игры, финансовое мошенничество и/или терроризм»[59].

Специальный докладчик ООН по вопросу о торговле детьми, детской проституции и детской порнографии также обращает внимание на тревожную тенденцию создания самими детьми откровенных изображений сексуального характера[60].

Проблема остается открытой. На сегодняшний день киберпресупники вовлекают несовершеннолетних детей к совершению преступной деятельности через сеть «Интернет». Чаще всего киберпреступники завлекают несовершеннолетних путем обещаний в финансовом вознаграждении или

---

[58] Information provided by Steven Malby, Senior Expert, Division of Treaty Affairs, Organized Crime and Illicit Trafficking Branch, UNODC, 23 May, 2014.
[59] UN Committee on the Rights of the Child, General Comment No. 13 (2011). The right of the child to freedom from all forms of violence, CRC/C/GC/13, 18 April 2011, §31(c) (iii).
[60] United Nations special representative of the secretary-general on violence against children. Releasing children's potential and minimizing risks. ICTs, the Internet and violence against children. P. 27.

принуждая угрозами к совершению противозаконных действий, опасных для его жизни и здоровья посредством ИКТ.

13) *Создание и использование цифровой информации для введения пользователя в заблуждение.*

Вышеназванное киберпреступление является умышленным противозаконным образованием и применением электронных данных, похожими с уже известными и вызывающими определенное доверие у пользователя данными, которые повлекли за собой причинение существенного урона.

14) *Подстрекательство к подрывной или вооруженной деятельности.*

Согласно Проекту ООН, данный вид киберпреступления представляет из себя противоправное деяние с использованием компьютерных сетей агитации к совершению вооруженной или подрывной деятельности и направленное на насильственное изменение конституционного строя другого государства. В УК РФ существует целая глава, посвященная преступления против основ конституционного строя и безопасности государства. В частности, статья 279 УК РФ трактует о вооруженном мятеже.

15) *Преступления, связанные с террористической деятельностью.*

Информационно-коммуникационные технологии (ИКТ) могут использоваться для способствования совершению преступлений, связанных с терроризмом, или могут быть целью террористов. Например, ИКТ могут использоваться для поощрения, поддержки террористических актов, содействия в их совершении и/или участия в них[61].

Отличие кибертерроризма от традиционного терроризма заключается в использование компьютерных сетей[62]. По сути, это использование электронных связей для осуществления террористических атак, обычно с

---

[61] *UNODC. (2012). The Use of the Internet for Terrorist Purposes. P.3.*

[62] S.S. Raghay, Cyber Security in India's Counter Terrorism Strategy, INTEGRATED DEFENSE STAFF 2 (Sept. 15, 2012), ids.nic.in/art_by_offids/Cyber security in india by Col SS Raghav.pdf дата обращения: 18.07.2024). – Текст: электронный.

использованием программ, созданных для этой цели. Эти программы могут быть доставлены по назначению либо через сеть «Интернет», либо через портативные устройства хранения данных (например, USB-карты), беспроводные радиосигналы или другие подобные средства[63].

Кибертерроризм следует рассматривать отдельно от использования террористами сети «Интернет», которое включает в себя такие аспекты, как коммуникация, вербовка, финансирование, организацию, пропаганду, подстрекательство к терроризму и апологии терроризма[64]. В то же время некоторые кибероперации (например, вторжения в базы данных критической инфраструктуры для сбора информации об уязвимых объектах) могут способствовать деятельности киберэкстремистов, но сами по себе не являются актами кибертерроризма[65]. Исследователь Конвей предлагает разделить кибератаки на «использование» сети Интернет (выражение идей и общение), «неправильное использование» (разрушение или компрометация веб-сайтов или инфраструктуры), «наступательное использовании» (использование сети «Интернет» для нанесения ущерба или совершения кражи) и «кибертерроризм»[66].

Термин «кибертерроризм» появился еще до событий 11 сентября 2000 года. Отсутствие нормативного определения «кибератака» привело к тому, что каждый эксперт понимает этот термин по-своему[67]. Неясность в терминологии усугубляется средствами массовой информации, которые характеризуют незначительные кибератаки, как «кибертерроризм».

---

[63] James A. Lewis, *The Internet and Terrorism*, 99 AM. SOC'Y INT'L L. 112, 114 (2005) ("One of the characteristics of terrorist websites is their ability to manage rapid changes of Internet addresses. When authorities force a site to move, informal networks based on chatrooms or e-mail inform the group's supporters of the new network address."); *see also* TIMOTHY F. O'HARA, CYBER WARFARE: CYBER TERRORISM 114 (2004).

[64] Elina Noor, *The Problem with Cyber Terrorism*, 2 SOUTHEAST ASIA REGIONAL CTR. FOR COUNTER-TERRORISM 51, 52 (2011).

[65] Varvara Mitliaga, *Cyber-terrorism: A Call for Governmental Action?*, BRITISH AND IRISH LAW, EDUCATION & TECHNOLOGY ASSOCIATION 5 (2001), http://www. bileta.ac.uk/01papers/mitliaga.html (describing hacktivism as "using hacking techniques to disrupt normal functions of systems, without causing serious damage, aiming at dissemination of propaganda and expression of political opinions").

[66] Maura Conway, *Terrorism and IT: Cyberterrorism and Terrorist Organisations Online* 6 (2003) (paper prepared for presentation at the International Studies Association Annual International Convention in Portland, Oregon).

[67] Ali Jahangiri, *Cyberspace, Cyberterrorism and Information Warfare: A Perfect Recipe for Confusion*, WORLDWIDE SECURITY CONFERENCE 6: BACKGROUND MATERIALS AND SELECTED SPEAKERS NOTES 29 (2009).

Как и в случае с «терроризмом», ученые предложили широкий спектр возможных определений, которые могли бы охватить это понятие. Некоторые из них сосредоточены на разрушительном и дестабилизирующем характере «кибертерроризма», определяя его как преступление международного характера и совершаемое отдельными физическими лицами. Особое внимание уделяется психологическим эффектам (например, страху), процессу написания вредоносных программ, включая атаки на критические национальные инфраструктуры и атаки, наносящие ущерб самим компьютерным сетям[68]. Более того существует ряд мнений о том, что концепция «кибертерроризма» не имеет права на существование, поскольку «терроризм» требует физического нападения[69].

Многие из этих определений являются слишком широкими или узкими. Стэнфордский проект Международной конвенции об усилении защиты от киберпреступности и терроризма 2000 года определяет кибертерроризм, как неправомерное вмешательство в компьютерные сети с целью причинения существенного ущерба критической инфраструктуре государства, распространение террористической идеологии, а также нанесения ущерба военно-политическим объектам[70].

Принимая во внимание все эти факторы, с юридической точки зрения, наилучшим определением, описывающим понятие (конвенционального) кибертерроризма является: противоправное использование электронных сетей для совершения акта терроризма в сети «Интернет» в целях нанесения ущерба международной информационной безопасности[71].

---

[68] Gabriel Weimann, *Cyberterrorsim: The Sum of All Fears?*, 28 STUD. IN CONFLICT & TERRORISM 129, 130 (2005), *cited in* Clive Walker, *Cyber-Terrorism: Legal Principle and Law in the United Kingdom*, 110 PENN ST. L. REV., 625, 634 (2006).

[69] J. P. I. A. G. Charvat, *Cyber Terrorism: A New Dimension in Battlespace*, CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM 7 (2009)*, available at* http:// www.ccdcoe.org/publications/virtualbattlefield/05_CHARVAT_Cyber%20Terrorism.pdf. (дата обращения: 18.07.2024). – Текст: электронный.

[70] Abraham D. Sofaer et al., *A Proposal for an International Convention on Cyber Crime and Terrorism* 26 (Aug. 2000) (paper presented at the Stanford Conference at Stanford University), *available at* http://iis-db.stanford.edu/pubs/11912/sofaer goodman.pdf дата обращения: 18.07.2024). – Текст: электронный.

[71] YAROSLAV SHIRYAEV. Ph.D. Candidate at University Warwick. Cyberterrorism in the Context of Contemporary International Law. 2012. P. 167.

Кибертерроризм относится к конвергенции киберпространства и терроризма. Барри Коллин является одним из первых кто сформулировал определение кибертерроризма в 1980-х годах. Деннинг определяет кибертерроризм, как «незаконные нападения и угрозы нападений на компьютеры, сети и хранящуюся в них информацию, когда они совершаются с целью запугивания государства и его населения для достижения политических или социальных целей.» Кроме того, чтобы квалифицировать данное противоправное деяние как кибертерроризм, кибератака должна чтобы вызвать страх, посеять панику среди населения и повлиять на дестабилизацию внутри страны. Серьезные атаки на критически важные объекты инфраструктуры могут быть актами кибертерроризма, в зависимости от их последствий[72].

Группировка интернет-террористов – Киберхалифат, которая является подразделением «Исламского государства» (запрещенная в Российской Федерации террористическая организация), взломала аккаунт центрального командования вооруженных сил США в социальной сети «Twitter» и популярном видеохостинге «Youtube». Кибертеррористы выложили в открытый доступ секретные сведения о военнослужащих армии США, включая их позывные и телефонные номера. Спустя некоторое время злоумышленники совершили террористическую атаку на запись издания «Newsweek» в «Twitter». На странице портала в сети микроблогов появилось несколько сообщений с угрозами, одно из которых было адресовано первой леди США, ее дочерям и мужу. «КиберХалифат объявляет киберджихад в виртуальном пространстве Интернет. В то время как США и их союзники убивают наших братьев в Сирии, Ираке и Афганистане, мы намерены уничтожить их системы кибербезопасности. Мы и дальше намерены

[72] Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Networks and netwars: The future of terror, crime, and militancy, 239, 288.

продолжать атаку на сеть Пентагона» − говорится в оставленных кибертеррористами посланиях[73].

Данное преступление можно квалифицировать по части 1 статьи 2 (Противозаконный доступ), Главы II Конвенции Совета Европы « О преступности в сфере компьютерной информации» (ETS No 185) (Будапешт, 23.11.2001) (далее – Конвенция от 23.11.2001), статья 3 (Распространение расистских и ксенофобских материалов посредством компьютерных систем), статья 4 (Мотивированная угроза расизма и ксенофобии), Главы II Дополнительного Протокола No 1 к Конвенции от 23.11.2001. Помимо взлома базы данных и незаконного доступа к персональной информации, террористы-хакеры Киберхалифата используют стремительно развивающиеся технологии, информационные инструменты для пропаганды деструктивных идеологий, инструменты рекрутинга и насаждения насилия для усиления восприятия их действий. Они демонстративно показывают свои действия для того, чтобы посеять страх у своих оппонентов и обеспечить себе поддержку. Они используют специальные кибер-инструменты для распространения террора. Агитация и вербовка в свои ряды является подстрекательством к насильственным действиям и распространением экстремистской̆ информации и подпадает под статью 7 (Пособничество и подстрекательство), Главы II Дополнительного протокола к Конвенции по киберпреступлениям в отношении криминализации деяний расистского и ксенофобского характера, осуществляемых при помощи компьютерных систем (г. Страсбург, 28.01.2003). Также путем обмена информацией̆ через всемирную паутину и сети связи, координируются и осуществляются террористические акты. Одна из основных идей Конвенции от 23.11.2001 является определение единообразных составов компьютерных преступлений, которые государства должны включить в свои национальные законодательства, а также разработка мер борьбы с ними. Террористы «ДАИШ» (запрещенная в Российской

[73] Голубев В.А. Кибертерроризм-угроза национальной безопасности. URL: http://www.crime-research.ru/ articles/Golubev_Cyber_Terrorism/ дата обращения: 18.07.2024). – Текст: электронный.

Федерации террористическая организация) стараются вербовать в свои ряды молодых людей (средний возраст 23 года), а также военных специалистов, лингвистов и переводчиков. Через сайты это им сделать на территории нашей страны затруднительно, так как Роскомнадзор сразу блокирует их и вносит в чёрный список. Поэтому кибертеррористы используют социальные сети и чаты. В течение 2001–2005 года Российская Федерация активно участвовала в разработке проекта Конвенции Совета Европы о предупреждении терроризма[74] (CETS No 196) (Варшава, 15.05.2005) (далее – Конвенция от 16.05.2005) и первым ратифицировала его 21.04.2006. Согласно Конвенции от 16.05.2005 впервые в мировой практике подстрекательство к терактам (статья 5), а также вербовка (статья 6) и подготовка террористов (статья 7) признаны уголовными преступлениями.

В своей резолюции от 17.12.2015 Совет Безопасности ООН,[75] выражая озабоченность по поводу того, что в глобализированном обществе террористы и их сторонники все шире используют новые информационно-коммуникационные технологии, в частности сеть «Интернет», для содействия террористическим актам, и осуждая использование этих технологий в целях подстрекательства, вербовки, финансирования или планирования террористических актов, выражая озабоченность по поводу международной вербовки новых членов в ряды «ИГИЛ» (запрещенная в Российской Федерации террористическая организация), «Аль-Каиды» и связанных с ними групп и масштабов этого явления и ссылаясь на свою резолюцию 2178 (2014), в которой Совет Безопасности ООН постановил, что государства-члены должны в соответствии с международными стандартами в области прав человека и нормами международного беженского права и международного гуманитарного права предотвращать и пресекать вербовку, организацию, перевозку и экипировку иностранных боевиков-террористов и

[74] Конвенция Совета Европы «О предупреждении терроризма» (CETS No196), (Варшава, 16 мая 2005 г.). Доступ СПС «ГАРАНТ».
[75] Резолюция Совета Безопасности ООН 2253 от 17 декабря 2015 г. «Угрозы международному миру и безопасности, создаваемые террористическими актами». Доступ СПС «ГАРАНТ».

финансирование деятельности[76]. Предотвращение международной вербовки новых членов в ряды террористов является на сегодняшний день актуальным вопросом для всего мирового сообщества. Террористы настолько активно используют интернет для коммуникации, рекрутирования, пропаганды и сбора средств, что нанесение упреждающего удара является просто необходимой мерой для предотвращения кибертерроризма.

Стремительные темпы освоения цифрового пространства и внедрение новых технологий привели к тому, что Конвенция СЕ перестала быть актуальной. В период ее разработки (1997–2001 г.) о многих угрозах в сфере информационной безопасности, включая некоторые уголовные преступления, не было известно, либо им не придавалось должного значения. На сегодняшний день появились новые виды преступлений в сфере информационных технологий, в частности использование злоумышленниками так называемых «ботнетов» – сетей компьютеров, зараженных вредоносной программой, которая позволяет удаленно выполнять различные противоправные действия. Также в качестве примера можно привести отсутствие ссылок в Конвенции СЕ на принятие антиспамовских мер, «фишинг» и др. Сложно эффективно вести борьбу с новыми проявлениями терроризма в информационном пространстве без его юридического определения и, соответственно, криминализации как самого понятия, так и его составляющих[77]. Таким образом, необходим документ глобального охвата по борьбе с преступностью в информационной сфере, который гарантировал бы суверенитет и невмешательство во внутренние дела государств посредством ЭВМ.

До сих пор как в национальном, так и в международном праве отсутствует легальное определение кибертерроризма. В отечественной юридической литературе ряд авторов дали кибертерроризму дефиницию. Например,

---

[76] Иванов С.М. Международно-правовое регулирование борьбы с кибертерроризмом // Право и безопасность. 2013. No 3-4. С. 82-87.

[77] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры: автореф. дис. ... канд. юр. наук. Владивосток, 2005. 19 с.

Голубев В. А. понимает под кибертерроризмом: «преднамеренную, политически мотивированную атаку на информацию обрабатываемою компьютером, компьютерную систему и сети, которая создает опасность для жизни или здоровья людей или наступления других тяжких последствий, если такие действия были содеянные с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта». А что представляет из себя Киберхалифат, который выступает субъектом вышеупомянутого кибертерроризма? Организованная преступная группировка, совершающая преступления в сфере компьютерной информации? Внося собственный вклад в дефиницию рассматриваемого понятия, автор считает возможным определить Киберхалифат – как террористов, взламывающих информационные системы для создания эффекта опасности, которую можно использовать для политического воздействия. Своими кибератаками они пытаются посеять страх, хаос и дестабилизировать обстановку в стране[78].

Для успешного противодействия киберпреступности, в частности, кибертерроризму, необходимо принять следующие меры:

1) Установить эффективное международное сотрудничество с иностранными государствами, их спецслужбами и правоохранительными органами, а также организовать тесный контакт с международными организациями для скорейшего разрешения данной проблемы.

2) Принять на национальном уровне законы о защите компьютерной безопасности в соответствии с действующими международными соглашениями

3) Создать универсальный орган оперативного характера, который будет наделен оперативно-разыскными полномочиями в целях выявления, пресечения и раскрытия киберпреступлений.

---

[78] Аббуд Р.Р. Киберхалифат: нормативное определение и криминологическая характеристика в национальном и международном информационном праве // Вопросы российского и международного права. 2018 Том 8 № 8А. С. 195.

16) *Преступления, связанные с экстремистской деятельностью.*

Проект Конвенции ООН определяет преступления, связанные с экстремистской деятельностью, как распространение контента, содержащего текст агитационного характера к склонению совершению неправомерных деяний по мотивам идеологической, социальной, национальной, политической и религиозной вражды, оправдания или пропаганды таких деяний, совершенных с использованием компьютерных сетей.

Так, в деле США против Закари Чессер, американец Закари Адам Чессер, осужденный в 2010 году за пособничество «Аш-Шабааб», которая связана с «Аль-Каидой» и была признана правительством США террористической организацией. Обвиняемый признался в размещении онлайн-угроз в адрес создателей мультсериала «Южный парк» и был приговорен к 25 годам тюремного заключения. Согласно материалам дела, Закари Адам Чессер призвал джихадистов напасть на сценаристов «Южного парка» за эпизод, в котором был изображен пророк Мухаммед в костюме медведя. Чессер размещал онлайн-сообщения, в которых указывались домашние адреса авторов. Чессер признал себя виновным в оказании материальной поддержки террористам и подстрекательстве применения насилия. Максимальное наказание по этим трем обвинениям составляло 30 лет тюремного заключения. Чессер также признался, что пытался отправиться в Сомали, чтобы присоединиться к «Аш-Шабааб», исламской военизированной группировке, которую Соединенные Штаты считают террористической организацией. После признания вины Чессер был приговорен федеральным судом США 24 февраля 2011 года к 25 годам тюремного заключения. Данное противоправное деяние в сети «Интернет» суд США квалифицировал как киберэкстремизм[79].

17) *Преступления, связанные с распространением наркотических средств и психотропных веществ.*

[79] U.S. v. Zachary Chesser (October 20, 2010).

В последние годы онлайновая торговля наркотическими средствами продолжает расти и имеет все основания для дальнейшего расширения. Однако поставки наркотиков через онлайн-платформы остаются ограниченными по сравнению с традиционными офлайн-поставками. Онлайновая торговля наркотиками, как правило, осуществляется на уровне розничной торговли, с частыми, но небольшими индивидуальными поставками[80]. Киберпреступники, занимающиеся оптовой торговлей наркотическими средствами, по-прежнему полагаются на офлайновую логистику.

Исследования в области использования ИКТ в противоправных целях выяснили, что *онлайн-платформы,* представляющие собой разновидность различных веб-сайтов, используют передовой стандарт шифрования для защиты анонимности пользователей[81]. Например, прекративший свое существование веб-сайт Silk Road, все чаще используются киберпреступниками для расширения своей деятельности за счет охвата клиентов во всем мире[82]. Онлайн-платформы сводят к минимуму риски быть обнаруженными правоохранительными органами, которые существуют при незаконном обороте наркотических средств офлайн.[83] Онлайн-платформы также уменьшают факторы нестабильности, связанные с рынками наркотических средств, расширяют доступ покупателей к информации о продавцах и отзывам покупателей о качестве товаров, предлагаемых продавцами, и их надежности (в форме рейтингов), а также расширяют доступ продавцов к клиентам и доступ покупателей к наркотическим средствам.[84]

---

[80] EMCDDA and Europol 2019, EU Drug Markets Report 2019. // URL: https://www.emcdda.europa.eu/system/files/publications/12078/20192630_TD0319332ENN_PDF.pdf дата обращения: 18.07.2024). – Текст: электронный.

[81] Broseus, Julian, Damien Rhumorbarbe, Caroline Mireault, Vincent Ouellette, Frank Crispino, and David Decary-Hetu. (2016). Studying illicit drug trafficking on Darknet markets: Structure and organization from a Canadian Perspective. *Forensic Science International*, Vol. 264, 7-14.

[82] Martin, James. (2014). Lost on the Silk Road: online drug distribution and the «cryptomarket». *Criminology and Criminal Justice*, Vol. 14(3), 351-367.

[83] Norbutas, Lukas. (2018). Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network. *International Journal of Drug Policy*, Vol. 56, pp.92-100.

[84] Przepiorka, Wojtek, Lukas Norbutas, and Rense Corten. (2017). Order without law: Reputation promotes cooperation in a cryptomarket for illegal drugs. *European Sociological Review*, Vol. 33(6), 752-764.

18) *Преступления, связанные с незаконным оборотом оружия.*

Оружие можно приобрести через сеть «Интернет» или так называемую «теневую сеть» (англ. DarkNet; рус. Даркнет). Онлайновая торговля оружием является незаконным и, вероятно, будет расти в будущем, причем для доставки огнестрельного оружия или его составных частей используется почтовая служба или операторы быстрых посылок. Ограничения, введенные пандемией Covid-19, повлияли на то, что получение оружия путем онлайн стал более доступным.

Доступность оружия в «теневой сети» вызывает озабоченность у правоохранительных органов, поскольку это позволяет лицам, не имеющим криминальных связей, находить и приобретать незаконно оружие. Использование криптовалют и наличие бесплатных анонимизирующих программных средств, обеспечивающих легкий доступ к даркнету, также делают ее источником незаконного приобретения оружия. Учитывая длительный срок службы оружия, после утечки с легального рынка оно может представлять опасность в течение десятилетий, причем преступники в европейских регионах, где трудно достать огнестрельное оружие, прибегают к использованию антикварного огнестрельного оружия. Распространение незаконного огнестрельного оружия в ЕС повышает риск его использования в террористических атаках и организованной преступности, поэтому ЕС предпринимает последовательные усилия по устранению риска, связанного с незаконным оборотом оружия[85].

Объявления о незаконной продаже огнестрельного оружия размещаются в социальных сетях, на аукционных и коммерческих сайтах, а также на сайтах даркнета[86]. Например, в Соединенных Штатах Америки законно приобретаемое огнестрельное оружие затем незаконно перепродается

[85] European Parliamentary Research Service. P. 7.
[86] GAO. (2017). *Internet Firearm Sales.*

торговцами оружием на сайтах даркнета и отправляется во многие страны Европы в нарушение законов штатов[87].

19) *Реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности.*

Новый вид киберпреступления, который пока что не зафиксирован ни в одном международном документе. Представляет из себя умышленное распространения материалов, в которых отрицаются факты, одобряются или оправдываются действия таких международных преступлений, как геноцид или преступлениями против мира и человечности, установленные приговором Международного военного трибунала, образованного в соответствии с Лондонским соглашением от 8 августа 1945 года. Стоит подчеркнуть, что военные преступления и агрессия, установленные Римским статутом не подпадают под данный вид киберпреступления[88].

20) *Незаконное распространение фальсифицированных лекарственных средств и медицинских изделий.*

Данный вид «киберпреступления» получил свое глобальное распространение в эпоху пандемии COVID-19, когда киберзлоумышленники начали активно регистрировать доменные имена, содержащие такие обозначения, как «coronavirus» или «COVID». В результате чего многие потребители были введены в заблуждение и приобрели медицинские маски, дезинфицирующие средства для рук, а также поддельные лекарства, которые якобы предотвращают или лечат от COVID-19[89]. Вышеприведенный вид «киберпреступления» является также новым и не зафиксирован ни в одном действующем международном соглашении.

21) *Использование ИКТ для совершения деяний, признанных преступлениями в соответствии с международным правом.*

---

[87] US Department of Justice. (2017). *Gun traffickers arrested for allegedly using the Dark Net to export guns across the world.* US Attorney's Office, Northern District of Georgia.
[88] The Rome Statute of the International Criminal Court. Доступ СПС «ГАРАНТ».
[89] COVID-19 Cybercrime Analysis Report-August 2020 (Interpol).

В Приложении к Конвенции ООН перечислены международные договоры, которые охватывают использование ИКТ с целью совершения какого-либо деяния, представляющего собой преступление. К таким противоправным деяниям относятся преступления международного характера. К ним можно отнести:

1) преступления, совершаемых на борту воздушных судов;
2) незаконный захват воздушных судов;
3) незаконного оборота наркотических средств и психотропных веществ;
4) финансированием терроризма и т.д.

22) *Нарушение авторских и смежных прав с использованием ИКТ.*

Конвенция ООН дает довольно лаконичное определение в отношении данного вида киберпреступления. Нарушение авторских прав с использованием ИКТ представляет противоправное использование программ для систем ЭВМ и баз данных, представляющих из себя объекты авторского права. Авторское право в информационном пространстве достаточно подробно описано в праве Европейского Союза, которое гармонизирует и унифицирует авторские и смежные права государств-членов ЕС на данном этапе развития.

Если мы обратимся к праву Европейского Союза, то обнаружим ряд директив, регулирующих вопросы авторского права с использованием ИКТ.

Например, Директива Европейского Союза 91/250/ЕЕС от 14 мая 1991 года «О правовой охране программ для ЭВМ» обеспечивает правовую защиту компьютерных программ и гармонизирует защиту авторских прав на всей территории ЕС[90]. Эта директива была впервые введена в действие в 1991 году и предоставляла авторско-правовую защиту компьютерным программам так же, как и литературным произведениям, таким как книги или стихи. Директива также предоставляет владельцу авторского права право на временное или

[90]Директива Европейского Союза 91/250/ЕЕС от 14 мая 1991 года «О правовой охране программ для ЭВМ». Доступ СПС «ГАРАНТ».

постоянное копирование программы, любые переводы программы или право на ее распространение любым способом.

Аналогичная защита также предоставляется базам данных отдельной информации в соответствии с Директивой 96/9/ЕС от 11 марта 1996 года «О правовой охране базе данных»[91].

Директива Европейского Союза 2001/29/ЕС от 22 мая 2001 года «О гармонизации срока действия охраны авторского права и некоторых смежных прав в информационном обществе» устанавливает руководящие принципы, касающиеся правовой защиты материалов, защищенных авторским правом, с помощью технических средств[92]. Эта Директива определяет права владельцев авторских прав, включая право воспроизводить свои материалы и делать их доступными для общественности посредством публикации и передачи продуктов через сеть «Интернет», включая музыку, медиа и программное обеспечение. Данная Директива также требует от всех государств-членов обеспечить правовую защиту от попыток обхода технологий, предотвращающих копирование интеллектуальной собственности и баз данных. Кроме того, государства-члены должны обеспечить защиту от продуктов и услуг, предназначенных для обхода защитных мер на интеллектуальную собственность в незаконных целях или ограниченных коммерческих целях.

Обращаясь к судебной практике целесообразно будет осветить дело A&M Records, Inc. vs Napster, Inc., 239 F.3d 1004 (2001), которое является знаковым в части интеллектуальной собственности, в котором Апелляционный суд Соединенных Штатов по Девятому округу подтвердил решение Окружного суда Соединенных Штатов по Северному округу Калифорнии, решение о том, что ответчик, одноранговый сервис обмена файлами Napster, может быть привлечен к ответственности за нарушение авторских прав и косвенное

[91]Директива 96/9/ЕС от 11 марта 1996 года «О правовой охране базе данных». Доступ СПС «ГАРАНТ».
[92]Директива Европейского Союза 2001/29/ЕС от 22 мая 2001 года «О гармонизации срока действия охраны авторского права и некоторых смежных прав в информационном обществе». Доступ СПС «ГАРАНТ».

нарушение авторских прав истцов. Это было первое крупное дело, касающееся применения законов об авторском праве к одноранговому обмену файлами[93].

Подводя итоги вышесказанному, проект Конвенции ООН видится по настоящему уникальным и универсальным международно-правовым документом, носящим по своему содержанию всеобъемлющий характер. Несмотря на то, что Проект Конвенции ООН еще не принят, он не учитывает новые виды киберпреступлений. Такой вид киберпреступления, как кибербуллинг (оскорбление в сети «Интернет») в проекте Конвенции ООН не освещен. Помимо этого, деление перечня классификации киберпреступлений на разделы, как в Конвенции СЕ, видится целесообразным.

Тем не менее, проанализировав 22 вида киберпреступления, содержащиеся в проекте Конвенции ООН, можно сделать вывод о том, что перечень является практически исчерпывающим, отвечает современным международно-правовым реалиям и направлен на противодействие противоправного применения и использования ИКТ.

Таким образом, проект Конвенции ООН дублирует 10 видов киберпреступлений, содержащиеся в Конвенции СЕ, а также вводит новые 12 видов преступлений в сфере ИКТ, которые в Конвенции СЕ не освещены. Среди неосвещенных в Конвенции СЕ киберпреступлений можно выделить следующие: склонение к самоубийству или доведение до его совершения, оправдание геноцида, незаконное распространение фальсифицированных лекарственных средств и медицинских изделий и т.д. Более того, проект Конвенции ООН содержит такие виды киберпреступлений, который закреплены на национальном законодательном уровне в офлайн формате в УК РФ. Например: преступления, связанные с вовлечением несовершеннолетних к совершению противоправных действий, опасных для его жизни и здоровья; склонение к самоубийству или доведение до его совершения; незаконное производство, сбыт или пересылка наркотических средств, психотропных

[93] *A&M Records, Inc. v. Napster, Inc.*, 239 F. 3d 1004 (2001).

веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества. Помимо этого, деление перечня классификации киберпреступлений на разделы, как в Конвенции СЕ, видится целесообразным.

Кроме того, проект Конвенции ООН является существенно прогрессивнее ныне действующих международных соглашений, в котором заложены эффективные механизмы сотрудничества, в частности, в вопросах выдачи и оказания правовой помощи по уголовным делам, включая выявление, арест, конфискацию и возврат активов. Предложенный Российской Федерацией подход фактически закрепляет цифровой суверенитет государств над своим информационным пространством и открывает новую страницу в истории глобального противодействия киберпреступлениям.

Международные договоры в части противодействия киберпреступлениям не акцентируют внимание на территории конкретного государства. Ни в части субъекта, находящегося на территории данного государства, ни то, что противоправное деяние совершено на территории определенной страны, ни то, что последствия противоправного деяния возникают на территории данного государства. Квалифицирующие признаки данного рода преступления, вышеприведенные международные соглашения не содержат.

На сегодняшний день происходит только начальный этап формирования международно-правовой системы противодействия киберпреступлениям. Международное сообщество только приближается к созданию действительно универсального и эффективного международно-правового инструмента. Конвенция СЕ демонстрирует себя как неспособной адекватно отвечать новейшим угрозам в сфере преступного использования ИКТ в силу отсутствия положений, которые могли бы обеспечить правовую регламентацию новых киберпреступлений. Более того, на данный момент отсутствует устоявшаяся, однозначная и унифицированная правовая

терминология в части киберпреступления, которую можно было бы использовать в дальнейшем правотворчестве. Тем не менее, отрицать или не замечать серьезную угрозу со стороны развивающихся киберпреступлений невозможно.

Исходя из анализа международных документов в области регулирования преступлений в сфере информационных технологий, и, учитывая, что такой вид киберпреступления, как кибербуллинг в международных соглашениях не закреплен, предлагается выделить дополнительную классификацию по следующему критерию объекта: «противоправное использование информационно-коммуникационных технологий в целях нарушения прав личности в части чести и достоинства, а также собственности в информационном пространстве». Из данного тезиса вытекают следующие виды киберпреступлений: а) кибербуллинг, б) дипфейк, в) криптоджекинг, г) вещевой кардинг.

§ 3. Киберпреступление как новый вид международного преступления

В данном параграфе автор считает важным затронуть вопрос в части того, будет ли кибератака одного государства в отношении другого государства являться актом применения силы и возможно ли в данном случае квалифицировать киберпреступление в качестве международного преступления. Кроме того, целесообразно создание международной правоохранительной организации универсального характера, наделенной компетенцией в части осуществления международной оперативно-розыскной деятельности в целях выявления, пресечения или раскрытия наиболее тяжких киберпреступлений, а также международных расследований на досудебных стадиях уголовного судопроизводства. Кроме того, в целях осуществления международного уголовного правосудия возможно создание специального трибуна ad hoc по международным киберпреступлениям.

Международно-правовой режим применения силы состоит из двух частей: основания обращения к силе определяются правом войны (jus ad bellum); отношения между воюющими определяются правом воюющих, т. е. международным гуманитарным правом (jus in bello). Обе части содержат нормы, призванные сдерживать насилие, однако, основываются на разных идеях: *jus ad bellum* — на идее международной безопасности; *jus in bello* — на идее гуманности[94].

По мнению Dr. Samuli Haataja, преступления в сфере информационных технологий, направленные в отношении государств, представляют собой новую форму насилия в эпоху цифровизации[95].

Согласно статьей 2 (4) Устава ООН, все Члены Организации Объединенных Наций воздерживаются в их международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями ООН[96]. Данное положение Устава ООН запрещает государствам прибегать к определенным формам насилия в международных отношениях. В связи с этим возникает вопрос, можно ли отнести кибератаку одного государства в отношении другого государства, как к акту применения силы?

На сегодняшний день ведутся серьезные дебаты по поводу того, будут ли кибератаки, направленные одним государством в отношении другого, приравниваться к акту применения силы в нарушение статьи 2 (4) Устава ООН. Таллинское Руководство 2.0 предусматривает, что кибератака представляет собой применение силы в том случае, когда ее масштабы и последствия сопоставимы с традиционным «применением силы»[97]. Руководство также уделяет внимание разрушительным кибернетическим

---

[94] В. Л. Толстых. «Курс международного права». 2019. с. 453.
[95] Haataja, Samuli. Cyber Attacks and International Law on the Use of Force (Emerging Technologies, Ethics and International Affairs). 2020. p. 2.
[96] Устав Организации Объединенных Наций (Сан-Франциско, 26 июня 1945 г.). Доступ из СПС «ГАРАНТ».
[97] Michael N Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd edn, Cambridge University Press 2017). P. 330.

операциям, которые квалифицируются как «вооруженные нападения» и дают право государствам реагировать в порядке самообороны. Стоит отметить, что вышеприведенный документ относится к актам мягкого права и не имеет обязательной юридической силы. По мнению автора, Таллиннское руководство можно отнести к доктрине. В соответствии со статьей 38 Статута Международного Суда ООН, доктрина является вспомогательным источником международного права. Многие положения Таллинского руководства, в частности вопросы суверенитета, юрисдикции и международно-правовой ответственности подробно проработаны и являются возможным ориентиром для создания международных соглашений в части регулирования киберпреступлений, которые будут содержать нормы jus cogens.

Таким образом, в Таллинском руководстве отображены два главных элемента:

1) *jus ad bellum,* которое устанавливает основания осуществления государством силы в международных отношениях.
2) *jus in bello* направлено на установление причин конфликта и определяет по совей сути гуманитарные функции.

Основным источником права *jus ad bellum* является Устав ООН, в то время как к источникам *jus in bello* относятся Гаагские конвенции, Женевские конвенции иные международные соглашения.

Вопросам применения международного гуманитарного права к киберпространству посвящены научные работы в отечественной и иностранной доктринах. Как отмечает А. Стрельцов «ст. 41 и ст. 42 Устава ООН, выделяют два основных вида «силы» — сила, связанная с использованием вооруженных сил (оружия) и сила, не связанная с использованием оружия. Международные отношения в области злонамеренного использования ИКТ в основном урегулированы нормами ст. 2 (4) Устава ООН, предъявляющими к государствам требование

воздерживаться от угрозы силой или ее применения в международных отношениях, в том числе и в киберпространстве»[98].

Нельзя не учесть, что согласно консультативному заключению МС ООН «О законности применения ядерного оружия» реализация права на самооборону не зависит от вида оружия, направленного в целях нападения, достаточно самого факта применения силы.

W.M. Stahl отмечает, что «… Устав ООН не позволяет четко определить равнозначность кибератаки, совершенной одним государством против другого, вооруженному нападению, дающему государству право на ответные силовые действия[99].

Исходя из вышеуказанной сентенции, ученые в целях правовой определенности пытаются установить, что под собой подразумевает вооруженный конфликт в информационном пространстве; какими нормами права регулируется правовой статус комбатантов и не комбатантов в таких случаях; каков круг субъектов, защищаемых нормами права в таких ситуациях[100].

Резюмируя вышесказанное, на взгляд автора, кибератаку, направленную одним государством против другого, можно отнести к акту применения силы, если данная кибератака нарушает цифровой суверенитет государств и тем самым угрожает международной информационной безопасности в целом. В практическом плане в контексте права на самооборону по ст. 51 Устава ООН международному сообществу следовало бы выработать определенные границы, позволяющие квалифицировать кибератаку как «применение силы» или «акт агрессии», и соответственно, приравнять к международному преступлению, а также соответствующие критерии для квалификации ИКТ в качестве оружия.

---

[98] Крутских А.В., Стрельцов А.А. Проблемы применения международного права к злонамеренному использованию ИКТ. Международная жизнь. 2014. № 11.

[99] Stahl W.M. [Электронный ресурс]. http://interlaws.ru/kiberbezopasnost-i-mezhdunarodnoe-pravo/ (дата обращения: 18.07.2024). – Текст: электронный.

[100] Козик А.Л. Развитие информационных технологий и правовое регулирование общественных отношений // Studii Juridice Universitare. 2008. № 3-4. С. 122–123.

Важно, чтобы в отношении киберпреступлений было проведено расследование в соответствие с международным правом. Широкомасштабные и систематические кибератаки будут оставаться безнаказанными без специального международного судебного органа и универсального оперативного органа в действии. Учреждение вышеупомянутых институтов приведет к всеобщему применению принципа индивидуальной уголовной ответственности[101]. Легитимность создания универсальной международной правоохранительной организации будет обусловлено принятием межправительственного соглашения, которое наделит данный силовой институт всеми необходимыми полномочиями в части уголовного преследования. Этот шаг станет сигналом для ООН и всего мирового сообщества в той части, что широкомасштабные и систематические кибератаки больше недопустимы[102].

Одним из наиболее реализуемых сценариев развития видится в создании Конференции по Обзору Римского Статута МУС, на которой будет обсуждаться вопрос в части определения киберпреступления, как международного преступления, а также условий осуществления юрисдикции в отношении использования ИКТ в противоправных целях. Внесение данного положения в вышеприведенный международный акт будет способствовать укреплению правовых основ международной информационной безопасности, а также укреплению такого правопорядка, где мир и правосудие являются глобальными ценностями.

Альтернативным сценарием является образование самостоятельного международного силового и судебного института. Действующие международно-правовые институты на мировой арене являются недостаточными. Международный союз электросвязи является специализированным учреждением ООН и выполняет по большей части

---

[101] Stein, J. (2012). *Recommendations for Potential New Global Legal Mechanisms Against Global Cyber Attacks and Other Global Cybercrimes*. A Paper for the East West Institute (EWI) Cybercrime Legal Working Group 2012. P. 127.

[102] Stein, J. (2012). *Recommendations for Potential New Global Legal Mechanisms Against Global Cyber Attacks and Other Global Cybercrimes*. A Paper for the East West Institute (EWI) Cybercrime Legal Working Group 2012. P. 58.

политико-консультативные функции в области информационной безопасности. Международная универсальная организация уголовной полиции – Интерпол координирует сотрудничество в части противодействия в отношении киберпреступлений, а его оперативно-розыскные полномочия ограничены рамками информационного содействия. Однако, современные тенденции преступности, их международная составляющая требуют не только информацию, но и совместных действий по пресечению и раскрытию готовящихся и совершенных преступлений путем проведения в необходимых случаях международных оперативно-розыскных мероприятий. Решение данного вопроса реализуемо с помощью принятия международного межправительственного соглашения, в котором будет определена компетенция международного силового органа. Необходимо формирование международной правоохранительной организации универсального характера, наделенного компетенцией в части осуществления международной оперативно-розыскной деятельности в целях выявления, пресечения или раскрытия наиболее тяжких киберпреступлений, а также международных расследований на досудебных стадиях уголовного судопроизводства. Кроме того, в целях осуществления международного уголовного правосудия возможно создание специального трибуна ad hoc по международным киберпреступлениям.

Глава II. Международно-правовое противодействие киберпреступлениям.

§1. Международные соглашения в части противодействия киберпреступлениям.

Революция в информационных технологиях коренным образом изменила общество и, вероятно, продолжит это делать в обозримом будущем. Информационные технологии так или иначе проникли почти во все аспекты человеческой деятельности. По мнению М. Б. Касеновой, за достаточно короткий исторический промежуток времени интернет превратился в глобальный коммуникационный ресурс, позволяющий объединять в рамках одной сети – сети интернет – множество разнообразных сетей, предоставляя возможность универсального доступа и взаимодействия в интернете неограниченному кругу лиц, включая лиц, находящихся в разных юрисдикциях[103]. Иными словами, научно-технический прогресс не стоит на месте, и вместе с тем влияние информационных технологий на эволюционирование телекоммуникационных технологий будет неуклонно возрастать. Например, появились голосовые сообщения, обмен которыми стал возможен не только между пользователями, но и между пользователями и самими устройствами, например компьютером, а также между самими устройствами. Тем самым появился новый метод передачи информации наряду с установлением прямого соединения между пользователями, например по сотовой связи.

Под противодействием (предупреждением или борьбой) понимаются усилия, которые прямо или косвенно связаны с борьбой с киберпреступлениями, такие как меры реагирования, принимаемые правоохранительными органами, и содействие национальному и

[103] Касенова М. Б. Правовое регулирование трансграничного функционирования и использования интернета: дис. … д-ра юрид. Наук / Касенова М. Б. – Москва., 2016. – 511.

международному сотрудничеству между правительствами, деловыми кругами, научно-образовательными учреждениями, организациями и общественностью в целях контроля и/или снижения уровня киберпреступности. Иными словами, противодействие киберпреступлениям сосредоточено на мерах политики, программах и практике в области уголовного правосудия и предупреждения преступности. Противодействие киберпреступлениям достигается как криминализацией деяний в данной сфере, так и применением мер, направленных на обнаружение киберпреступлений, их расследование, судебное преследование лиц, совершивших такие преступления[104].

Согласно позиции Т. Н. Нешатаевой, в западной правовой доктрине «сформировалась концепция о делении международного публичного права на «мягкое» право (soft law) – рекомендательные нормы и «твердое» право (hard law) – обязательные нормы». Кроме того, Т. Н. Нешатаева отмечает, что «резолюции-рекомендации межправительственных организаций системы ООН, формулирующие новые правила поведения государств-членов, выполняют двоякую роль: во-первых, они могут выступать в качестве стадии в правотворческом процессе, ведущем к оформлению нормы международного публичного права, и, во-вторых, они являются регулятором межгосударственных отношений, оставаясь при этом рекомендательными, а не обязательными нормами»[105].

Согласно позиции Г.И. Тункина, резолюции ГА ООН нередко выступают также как средство констатации или толкования действующих принципов и норм международного права[106].

На сегодняшний день правовые механизмы противодействия киберпреступлениям предусмотрены преимущественно в многосторонних

---

[104] Международное право: учебник / отв. ред. В. И. Кузнецов, Б. Р. Тузмухамедов. — 3-е изд., перераб. — М.: Норма: Инфра-М, 2010. — 720 с.

[105] Нешатаева Т.Н. Международные организации и право: Новые тенденции в международно-правовом регулировании / Т. Н. Нешатаева. - Москва: Дело, 1998. - 270,[1] с.; 21 см.; ISBN 5-7749-0058-4: Б. ц.

[106] Тункин Г.И. Теория международного права. Под общей ред. Проф. Л. Н. Шестакова. – М.: ИКД «Зерцало-М», 2019–416 с.

международных соглашениях регионального характера. По большей части эти региональные соглашения содержат нормы jus cogens и являются обязательными для исполнения. В рамках ООН приняты резолюции в части противодействия киберпреступлениям и обеспечению международной информационной безопасности Генеральной Ассамблеей, но они относятся к мягкому праву и не являются юридически обязательными. Вместе с тем такие нормы имеют важное значение в складывающемся блоке международных норм об информационной безопасности.

В данном параграфе проводится анализ документов с целью выявления методов международно-правового сотрудничества в сфере противодействия использованию ИКТ в преступных целях, а также выяснить, является ли регулирование данного вопроса универсальным или региональным. Более того, в рамках данного исследования предпринимается попытка определить, акты обязательного характера или мягкого права являются наиболее эффективными в части регулирования данной проблемы.

В основу данного параграфа заложен анализ правовых документов, разработанных в контексте 16 международных организаций. Стоит отметить, что документы различаются по юридической силе и соответствующим правовым последствиям. Исходя из критерия обязательности, данные документы разделены на две группы: обязательные и рекомендательного характера.

Так, ряд документов (Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 г., Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г., Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 г., Конвенция Совета Европы о киберпреступности 2001г. и др.) имеют характер межгосударственных соглашений, что влечет наложение определенных юридических обязательств на государство-участника в соответствии с

принципом добросовестного выполнения обязательств, принятых на себя в соответствии с международным соглашением[107].

Другие документы (Резолюции ГА ООН, Рекомендации Организации экономического сотрудничества и развития (ОЭСР), Типовые законы Содружества Наций о компьютерных преступлениях и электронных доказательствах 2002 г., Типовой закон о компьютерных преступлениях и киберпреступности Сообщества развития Юга Африки (САДК) 2012 г., и др.) носят рекомендательный характер и выступают в качестве общих правовых рамок и типовых моделей законодательства в сфере противодействия киберпреступности, что, в свою очередь, не предполагает установление каких-либо юридических обязательств для государств.

Анализ данных документов выявил следующие цели:

1) улучшение эффективности в части международного-правового регулирования в данной сфере;

2) сближение и унификация внутригосударственного права государств в соответствии с международными нормами (jus cogens) и рекомендациями (soft law);

3) консолидация стран в лице компетентных внутригосударственных органов при раскрытии и пресечении киберпреступлений.

Сквозь призму международных соглашений, а также международных организаций происходит процесс кооперации стран в части борьбы с киберпреступлениями.

Организация Объединенных Наций

Организация Объединенных Наций (далее – ООН) является международной организацией, которая решает вопросы глобального характера

---

[107] Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций, принята Резолюцией Генеральной Ассамблеи ООН 1970 г. Доступ: https://www.un.org/ru/documents/decl_conv/declarations/intlaw_principles.shtml (дата обращения: 18.07.2024). – Текст: электронный.

и действует на основании Устава ООН 1945 года. На данный момент, в рамках ООН отсутствует юридически обязательное международное соглашение о борьбе с киберпреступлениями. Под эгидой ООН приняты акты рекомендательного характера о противодействии киберпреступлениям.

Генеральная Ассамблея ООН 14 декабря 1990 г. приняла Резолюцию по предупреждению преступности и обращению с правонарушителями[108]. Резолюция, в том числе, затронула вопросы борьбы с компьютерными преступлениями. Так, в пункте 10 данной Резолюции настоятельно призывается оказывать всемирную поддержку проектам технической помощи, в частности, развивающимся странам, и области предупреждения преступности и уголовного правосудия, а также содействовать техническому сотрудничеству между развивающимися странами. На основе этой резолюции ООН опубликовала в 1994 году Руководство по предупреждению компьютерных преступлений и борьбе с ними[109]. Данное руководство было разработано с целью оказания помощи государствам-членам ООН в борьбе с киберпреступлениями. Руководство отражает усовершенствованный технический и оперативный подход ООН к предупреждению преступности и уголовному правосудию. В качестве компьютерных преступлений в соответствии с пунктом Е параграфом I Руководства понимаются: мошенничество, подделка документов, компьютерный саботаж, несанкционированный доступ и копирование компьютерных программ.

В 2005 году состоялся всемирный саммит по информационному обществу, проводившийся под эгидой ООН в Тунисе, в ходе которого была утверждена Тунисская программа развития информационного общества. Тунисская программа развития информационного сообщества предусматривает разработку государствами необходимого внутригосударственного правового регулирования в части расследования и судебного преследования за

---

[108] UN General Assembly, A/RES/45/121, (14 December 1990) URL: http://www.un.org/documents/ga/res/45/a45r121.html/ (дата обращения: 18.07.2024). – Текст: электронный.

[109] United Nations. *UN Manual on the Prevention and Control of Computer-Related Crime* (United Nations publication, Sales No. E.94.IV.5) URL: http://www.uncjin.org/Documents/EighthCongress.html/ (дата обращения: 18.07.2024). – Текст: электронный.

совершение киберпреступлений при учете существующих международных стандартов в данной области (например, Конвенция СЕ)[110].

Необходимость проведения переговоров по глобальной конвенции о борьбе с киберпреступлениями возникла в 2010 году во время двенадцатого конгресса ООН по предупреждению преступности и уголовному правосудию, проходившего в Сальвадоре, Бразилия. Мнения по этому вопросу разделились[111].

Российская Федерация призывала к переговорам по глобальной конвенции. Также высказались в поддержку обсуждения в части принятия универсального соглашения страны Латинской Америки, страны Африки, Китайская Народная Республика. Соединенные Штаты Америки, страны Европейского Союза и Великобритания не поддержали на том основании, что в настоящий момент необходимое международно-правовое регулирование вопросов киберпреступлений в полной мере осуществляется в рамках Конвенции СЕ[112].

Необходимость создания всемирной конвенции о регулировании киберпреступлений обсуждался на заседании Комиссии ООН по предупреждению преступности и уголовному правосудию (далее – Комиссия ООН по правосудию), которое состоялось в апреле 2013 года. Комиссия ООН по правосудию подготовила проект резолюции, в котором предложила государствам-членам «продолжить рассмотрение ... пути и средства укрепления международного сотрудничества в борьбе с киберпреступлениями» и просила созвать межправительственную рабочую

---

[110] International Telecommunication Union, World Summit on the Information Society, *'Tunis Agenda for the Information Society'*, WSIS-05/TUNIS/DOC/6 (Rev. 1) - E, (18 November 2005) 40. URL: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html/ (дата обращения: 18.07.2024). – Текст: электронный.

[111] Rep. of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, UN Doc A/CONF.213/18 at 56 – 7 [202] – [204] (18 May 2010). URL: https://www.un.org/ru/conf/crimecongress2010/ (дата обращения: 18.07.2024). – Текст: электронный.

[112] Masters Op.cit., note 22. The Quintet of Attorneys-General from Australia, Canada, New Zealand, the United Kingdom and the United States have resolved to «promote the Convention as the key international instrument for dealing with cybercrime and use the Convention as a basis for delivering capacity building and awareness raising activities»: US Reference Service, Communiqué – Quintet of Attorneys General: Action Plan to Fight Cyber Crime (18 August 2011) URL: http://usrsaustralia.state.gov/us-oz/2011/07/15/aag2.html/ (дата обращения: 18.07.2024). – Текст: электронный.

группу открытого состава для дальнейшего изучения проблемы киберпреступлений и мер реагирования государств на них[113].

Наряду с разработкой положений, регламентирующих вопросы процессуального характера, возникающие при обнаружении, расследовании и привлечении лиц к ответственности за совершение киберпреступлений, в рамках ООН разрабатываются организационные основы взаимодействия государств и национальных отраслевых компетентных органов по вопросам международной правовой помощи. Так, составлен проект резолюции Комиссии ООН по правосудию, который содержит положения, призывающие Управление ООН по наркотикам и преступности (далее - УНП ООН) укреплять партнерские отношения для оказания технической помощи и наращивания потенциала с государствами-членами, соответствующими организациями, частным сектором и гражданским обществом» и «служить центральным хранилищем законов и передовой практики в области противодействия киберпреступлениям[114].

В рамках системы ООН были приняты и другие меры для решения проблем, связанных с противодействием киберпреступлениям. Например, в 2007 году ЭКОСОС принял резолюцию о международном сотрудничестве в предотвращении, расследовании, судебном преследовании и наказании за экономическое мошенничество и преступления, связанные с использованием личных данных[115]. Хотя эта резолюция конкретно не касается регулирования киберпреступлений, УНП ООН опиралось на нее и при создании основной группы экспертов для обмена мнениями о наилучшем курсе действий по

---

[113] Commission on Crime Prevention and Criminal Justice, Strengthening International Cooperation to Combat Cybercrime, UN ESCOR, 22nd sess, Agenda Item 7, UN Doc d E/CN.15/2013/L.14 (2 April 2013) para 3. URL: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-NGO1/E-CN15-2013-NGO1_E.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

[114] Commission on Crime Prevention and Criminal Justice, Enabling International Cooperation against Cybercrime through Technical Assistance and Capacity-Building, UN ESCOR, 22nd sess, Agenda Item d 7, UN Doc E/CN.15/2013/L.16 (2 April 2013) paras 3–4. URL: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP11/E-CN15-2013-CRP11_E.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

[115] ECOSOC Resolution 2007/20, *International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime*. URL: https://www.un.org/ecosoc/en/docs/2007/Resolution%202007-20.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

борьбе с экономическим мошенничеством и преступлениями, связанными с использованием личных данных, и основная группа провела ряд исследований, которые, в частности, включали аспекты киберпреступлений[116].

18 декабря 2019 года ГА ООН приняла резолюцию, в которой призвала государства осуществлять меры, которые: обеспечат расследование киберпреступлений и судебное преследование за них; посодействуют международному сотрудничеству; организуют тренинги для сотрудников правоохранительных и судебных органов; улучшат техническую поддержку[117].

Стоит отметить, что Российская Федерация (далее – РФ) внесла существенный вклад в части разработки глобальной конвенции о противодействии киберпреступлениям.

Так, проект Конвенции ООН, внесенный Российской Федерацией, был одобрен в ходе 74-й сессии Генеральной Ассамблеи ООН в 2021 году. 21 апреля 2023 года завершилась пятая сессия Спецкомитета по киберпреступности в Вене. Всего Спецкомитету поручено провести шесть сессий с августа 2021 года по конец июня 2024 года и заключительную сессию в 2024 году. Работа по вышеназванному документу будет завершена, как только Спецкомитет представит Проект ООН ГА ООН на ее 78-й сессии в сентябре 2024 года. Резолюцией ГА ООН 79/243 от 24 декабря 2024 года принята Конвенция ООН против киберпреступности

Кроме того, Спецкомитет позволяет ООН оценивать и учитывать мнения государств-членов об усилиях, предпринимаемых отдельными государствами для укрепления международной информационной безопасности и дальнейшего международного сотрудничества в борьбе с

---

[116] *Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice,* 2009, E/CN.15/2009/CRP.13. URL: https://www.unodc.org/documents/treaties/organized_crime/ECN152009_CRP10.pdf (дата обращения: 18.07.2024). – Текст: электронный.

[117] Резолюция ГА ООН от 18 декабря 2019 года. A/RES/74/177. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/431/57/PDF/N1943157.pdf?OpenElementhttps://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/431/57/PDF/N1943157.pdf?OpenElement/ (дата обращения: 18.07.2024). – Текст: электронный.

киберпреступлениями[118]. Спецкомитет также уполномочен проводить консультации с региональными организациями, такими как Африканский союз, Европейский союз, Организация американских государств по вопросам, касающимся противодействию киберпреступлениям и международной информационной безопасности.

В рамках ООН создано Контртеррористическое управление, реализующее Программу по кибербезопасности и новым технологиям, предусматривающую борьбу против киберпреступлений, которые совершаются террористами в отношении критически важной инфраструктуры. Кроме того, использование социальных сетей в части сбора данных и электронных доказательств для того, чтобы оказать борьбу против терроризма во всемирной сети, а также насильственному экстремизму.

Кроме того, в рамках СБ ООН разработаны Мадридские руководящие принципы для пресечения потока иностранных боевиков-террористов. В частности, Руководящие принципы 25 и 26 постулируют о том, что странам-участникам необходимо пересмотреть внутригосударственное законодательство в целях установления того, чтобы доказательства, которые были собранные посредством механизмов расследования, а также доказательства, полученные посредством ИКТ. Образовать во внутригосударственных компетентных органах информационно-коммуникационную и экспертно-криминалистическую базу. Данные принципы могут быть полезными в части оперативно-розыскной деятельности, а именно, в части обнаружения и собирания доказательственной базы.

21 декабря 2010 года на Двенадцатом Конгрессе ООН по предупреждению преступности и уголовному правосудию принята Салвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире. В соответствии с пунктом 9 резолюции 65/230 ГА от 21

[118] Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: note / by the Secretary-General. 2021. URL: https://digitallibrary.un.org/record/3934214/ (дата обращения: 18.07.2024). – Текст: электронный.

декабря 2010 года, ГА просит Комиссию по предупреждению преступности и уголовному правосудию учредить межправительственную группу экспертов в целях реализации всеобъемлющего анализа феномена киберпреступности. Более того, осуществить кооперацию для того, чтобы выяснить методы совершенствования в части новых внутригосударственных и международных юридических или иных механизмов по борьбе с киберпреступлениями. Также в пункте 12 резолюции ГА просит Управление Организации Объединенных Наций по наркотикам и преступности, при разработке и осуществлении своих программ технической помощи, стремиться к достижению устойчивых и долгосрочных результатов в области предупреждения преступности, уголовного преследования и наказания за совершение различных видов преступлений, в том числе киберпреступлений.

18 декабря 2019 года принята резолюция ГА 74/173 о содействие оказанию технической помощи и наращиванию потенциала для усиления национальных мер и укрепления международного сотрудничества в целях борьбы с киберпреступностью, включая обмен информацией. В данном акте говорится об обязательности совершенствования кооперации между странами-участниками в части противодействия киберпреступлениям, посредством помощи технического характера в части улучшения их внутригосударственного законодательства и укрепления внутригосударственных органов в целях оказания борьбы киберпреступлениям. Оперативно-розыскные мероприятия, а также в дальнейшем судебный процесс над преступниками должен быть произведен в соответствии с принципом соблюдения основных прав и свобод человека. Данный принцип также подтверждается ООН при использовании ИКТ.

Резолюция 74/27, принятая Генеральной Ассамблеей от 27 декабря 2019 года о противодействие использованию ИКТ в противозаконных целях дублирует тезисы в вышеприведенных резолюциях, а также делает акцент на усилении кооперации национальных правоохранительных органов и всего международного сообщества в части борьбы с киберпреступлениями,

Подчеркивает необходимость работы Межправительственной группы специалистов над осуществлением всеобщего анализа феномена киберпреступности.

Таким образом, деятельность ООН направлена на проведение мер организационного характера в виде международной правовой помощи, в том числе, по сбору информации о способах и методах совершения киберпреступлений, консолидации технических ресурсов государств в целях предупреждения киберпреступлений. Выявлена тенденция к необходимости международной унификации отношений по выявлению, фиксации, расследованию, а также судебных процедур применительно к киберпреступлениям.

Правовое регулирование вопросов ответственности в сфере киберпреступлений, в настоящий момент рассматривается ООН исключительно как вопросы внутригосударственного характера. Вместе с тем, признается, что национальное регулирование должно осуществляться при соблюдении международно-правовых гарантий, среди которых положения резолюций Совета по правам человека 20/08 и 26/13 о поощрении, защите и осуществлении прав человека в сети «Интернет» и резолюций ГА 68/167 и 69/166 о праве на неприкосновенность личной жизни в эпоху цифровизации.

При этом, отметим, что в рамках деятельности ООН подтверждается важнейшая роль государств в предупреждении и предотвращении киберпреступлений. Государства обязаны гарантировать безопасность ИКТ на своей территории. Государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ[119]. Особая роль государств в защите и сохранении объектов критически важной инфраструктуры возлагается на государства, под юрисдикцией которых данные объекты находятся.

[119] Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности 14.07.2021. Доступ из СПС «Гарант».

Таким образом, в рамках ООН можно найти правовые ориентиры для правотворческой и организационной деятельности государств в отношении киберпреступлений. В условиях, когда национальное правовое регулирование данных вопросов развивается, такой подход является оправданным, поскольку позволяет создать схожие правовые механизмы предупреждения и расследования данного вида преступлений международного характера.

БРИКС

Объединение, начало которому было положено в июне 2006 года в рамках Петербургского экономического форума, включало Бразилию, Россию, Индию и Китай (БРИК). В феврале 2011 года к БРИК присоединилась Южно-Африканская Республика, после чего объединение получило название БРИКС. На август 2023 года 40 стран выразили заинтересованность в присоединении к БРИКС, около 20 из них официально обратились с просьбой о приёме. На саммите в августе 2023 было сообщено, что Аргентина, Иран, Саудовская Аравия, Египет, Эфиопия и ОАЭ приглашены к вступлению в БРИКС в качестве полноправных членов с 1 января 2024 года.

25–27 июля 2018 г. на Десятом Саммите стран – членов БРИКС в г. Йоханнесбурге Южно-Африканской Республики главами государств и правительств, представляющих Федеративную Республику Бразилию, Российскую Федерацию, Республику Индия, Китайскую Народную Республику и Южно-Африканскую Республику, была принята Йоханнесбургская Декларация[120]. Она принята в целях реализации новой стратегии БРИКС по расширению взаимодействия стран – членов БРИКС со странами Африки, инклюзивного роста и процветания сотрудничающих государств в связи с начавшейся Четвертой промышленной революцией.

---

[120] Йоханнесбургская Декларация Десятого Саммита БРИКС от 26.07.2018 г. БРИКС в Африке: Сотрудничество для достижения инклюзивного роста и всеобщего процветания в эпоху Четвертой промышленной революции». http://www.kremlin.ru/ supplement/5323/ (дата обращения: 18.07.2024). – Текст: электронный.

Итогом саммита стало понимание необходимости образования юридических конструкций в целях кооперации между членами БРИКС в сфере установления безопасности в области применения ИКТ. Кроме того, страны данной организации договорились о проведении дальнейшей работы в части создания межгосударственного договора о кооперации в данной сфере.

Таким образом, государства ШОС и БРИКС разделили с Россией соавторство проекта Конвенции ООН, над которой ведется на данный момент субстантивная работа в части принятия текста, и по праву стали лидерами мирового сообщества на пути построения глобальной системы международной информационной безопасности.

Сообщество развития Юга Африки

Торгово-экономический союз стран Юга Африки под названием Сообщество развития Юга Африки (далее – САДК), образованный на основании подписания Договора о САДК в Виндхуке (Намибия) в августе 1992 года на базе Конференции по координации развития Юга Африки[121]. В рамках САДК был разработал в 2012 году Типовой закон о компьютерных преступлениях и киберпреступности САДК (далее – Типовой закон САДК)[122]. Данный правовой документ можно отнести к мягкому праву, поскольку он является типовым, а следовательно, носит рекомендательный характер и не обязывает государств-участниц в реализации сотрудничества в части борьбы против киберпреступлений. Типовой закон является скорее методическим пособием для стран-членов САДК для выработки норм процессуального и материального права в сфере противодействия киберпреступлениям.

Организация экономического сотрудничества и развития

Международная экономическая организация под названием Организация экономического сотрудничества и развития (далее – ОЭСР),

---

[121] SADC Treaty. URL: http://www.sadc.int/documents-publications/sadc-treaty/ (дата обращения: 18.07.2024). – Текст: электронный.

[122] Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime. 2012. URL: https:// www.itu.int/en/ITU/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

правосубъектность которой определена в Конвенции о создании ОЭСР, вступившая в силу 30 сентября 1961 года. В рамках ОЭСР были разработаны ряд актов рекомендательного характера в части противодействия киберпреступлениям:

1) «Рекомендация ОЭСР 2015 г. по управлению рисками цифровой безопасности для экономического и социального процветания», заменившая действовавшие ранее «Руководящие принципы ОЭСР по обеспечению безопасности информационных систем и сетей: на пути к культуре безопасности» 2002 г.;
2) «Рекомендация по цифровой̆ безопасности критически важных видов деятельности была принята Советом ОЭСР 2019 г.», заменившая «Рекомендацию ОЭСР о защите критической информационной инфраструктуры 2008 г.»;
3) «Рекомендации о принципах формирования политики в области Интернета 2011 г.»[123];
4) «Рекомендация Совета по цифровой безопасности критически важных видов деятельности 2019 г.», заменившая «Рекомендации Совета по защите критически важных информационных инфраструктур 2008 г.»[124];
5) Декларация о цифровой экономике: инновации, экономический рост и социальное процветание (Канкунская декларация) 2016 г[125].

Проведенный анализ вышеперечисленных актов ОЭСР показал, что цели и задачи направлены на сотрудничество в области обеспечения безопасности сетей и информационных систем; обмен информацией между участвующими сторонами в части осуществления мер, процедур и практики в сфере безопасности; создание единой основы, при помощи которой станет ясна конкретная проблема в области безопасности систем.

---

[123]Рекомендация Совета по принципам формирования интернет-политики 2011 г. (OECD/LEGAL/0387 Recommendation of the Council on Principles for Internet Policy Making).

[124] URL: https://unece.org/DAM/trade/Publications/WP6_ECE_TRADE_390R.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

[125] Декларация о цифровой экономике: инновации, рост и социальное благополучие 2016 г. (OECD/LEGAL/0426 Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration) Доступ из СПС «Гарант».

В актах ОЭСР также сформированы принципы, которые взаимодополняют друг друга и распространяются на участвующие стороны на всех уровнях. К таким принципам относятся: ответственность (за обеспечение безопасности сетей и информационных сетей отвечают все участвующие стороны), осведомленность (осознание в потребности обеспечения безопасности сетей и информационных систем), этика (уважение интересов других организаций и лиц), принятие ответных мер (принятие действий для предотвращения киберпреступлений), оценка рисков, демократия, разработка сетей и систем с целью обеспечения безопасности.

Кроме того, ОЭСР первая проанализировала возможности гармонизации норм, предусматривающих уголовную ответственность за киберпреступления, а также представила криминологическое определение компьютерного преступления[126].

Организация американских государств

Организация американских государств (дале – ОАГ) создана в 1948 году. Учредительным документом ОАГ является Устав, вступивший в силу в 1951 году. В рамках ОАГ были разработаны следующие акты в части киберпреступлений:

1) Рекомендации, принимаемые по итогам совещаний Министров юстиции и Генеральных прокуроров Америки (REMJA) 1999–2016;
2) Рекомендации Межправительственной группы экспертов по киберпреступности 1999–2016 г.;
3) Глобальная межамериканская стратегия по кибербезопасности, утверждена резолюцией AG/RES 2004 (XXXIV-O / 04) Генеральной Ассамблеи ОАГ (далее – межамериканская стратегия).

В частности, межамериканская стратегия предусматривает создание так называемых групп реагирования на компьютерные преступления, которые отвечали бы за своевременное распространение информации о

[126] Computer-Related Crime: Analysis of Legal Policy. Paris: OECD. 1986.

киберпреступлениях, а также оказание технической поддержки в сфере кибербезопасности[127].

В рамках ОАГ также действует Межамериканская конвенция об экстрадиции 1981 года. В соответствии с данным документом возможна выдача преступника за совершение киберпреступления одним государством-участником другому. Кроме того, в данном соглашении установлены положения, в соответствии с которыми, экстрадиция не осуществляется. В соответствии с вышеназванном документов, отказ в экстрадиции возможен, в случае такого наказания, как смертная казнь. Более того, унижающее и бесчеловечное обращение с лицом, которое подлежит экстрадиции, является легитимным основание отказа.

Организации по безопасности и сотрудничеству в Европе

Организации по безопасности и сотрудничеству в Европе (далее – ОБСЕ) имеет несколько учредительным документов, например: Заключительный акт Совещания по безопасности и сотрудничеству в Европе 1975 года (Хельсинские соглашения)[128], где закреплены основные принципы международного права; а также Парижская хартия для новой Европы 1970 года[129]. В рамках ОБСЕ – крупнейшей в мире региональной организации, занимающейся вопросами безопасности были разработаны и приняты следующие акты в части противодействия киберпреступлениям:

1) Решение Постоянного совета ОБСЕ № 1039 от 26 апреля 2012 г. «Разработка мер укрепления доверия с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий»[130];
2) Решение Постоянного совета ОБСЕ № 1202 от 10 марта 2016 г. «Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков

---

[127] The History of Cybercrime by Stein Schjolberg. 2020. P. 51.
[128] URL: https://docs.cntd.ru/document/1901862?ysclid=lgb6btdz6q110793886/ (дата обращения: 18.07.2024). – Текст: электронный.
[129] URL: https://www.osce.org/files/f/documents/3/4/39520.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.
[130] URL: https://www.osce.org/ru/pc/228521/ (дата обращения: 18.07.2024). – Текст: электронный.

возникновения конфликтов в результате использования информационных и коммуникационных технологий»[131];

3) Постановление Совета министров No 5 / 16 «Усилия ОБСЕ по сокращению рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий»[132] от 9 декабря 2016 г.;
4) Постановление Совета министров No 5 / 17 «Наращивание усилий ОБСЕ по сокращению рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий»[133] от 8 декабря 2017 г.

Вышеназванные акты направлены на активизацию, как самостоятельных, так и коллективных усилий государств-членов ОБСЕ в части обеспечения безопасности при использовании информационных и коммуникационных технологий в соответствии с договоренностями в рамках ОБСЕ и в кооперации с международными организациями. Документы ОБСЭ также предусматривают на добровольной основе проведения консультаций, обмена информацией, сотрудничеству между внутригосударственными компетентными органами по вопросам безопасности при применении ИКТ. Резюмируя вышесказанное, те пункты, которые были одобрены на основании документов ОБСЕ нацелены на избежание коллизий в результате применения ИКТ и на установления применения ИКТ в мирных целях.

Интерпол

Интерпол был создан в далеком 1923 году и был известен как Международная комиссия уголовной полиции[134].

Интерпол оказывает противодействие в отношении киберпреступлений, анализируя, исследуя новые механизмы и алгоритмы обучения, а также

---

[131] URL: https://www.osce.org/files/f/documents/e/4/228521.pdf (дата обращения: 18.07.2024). – Текст: электронный.
[132] URL: https://www.osce.org/files/f/documents/e/8/364011.pdf (дата обращения: 18.07.2024). – Текст: электронный.
[133] https://www.osce.org/files/f/documents/e/8/364011.pdf (дата обращения: 18.07.2024). – Текст: электронный.
[134] Deflem, International Police Co/operation – History of, in The Encyclopedia of Criminology, New York, 2005 pp. 795-798.

создавая современные методы работы правоохранительных органов. Интерпол разработал Национальные центральные справочные центры по компьютерным преступлениям, которые представляют собой систему раннего предупреждения между подразделениями по расследованию преступлений в сфере информационных технологий в целях обеспечения безопасных и надлежащих каналов Интерпола для использования специализированными подразделениями по расследованию преступлений в сфере информационных технологий и в целях передачи данных с минимизированными опозданиями[135].

Необходимость кооперации Интерпола для решения проблем в части противодействия преступлениям в сфере информационных технологий заключается в том, что отличительной киберпреступлений особенностью есть трансграничный характер. Национальные центры бюро Интерпола существуют во всех странах-участниках, для оперативной и плотной кооперации[136].

Одной из инициатив Интерпола является образование в 2014 году Глобального комплекса инноваций (далее – ГКИ). ГКИ – это глобальный координационный орган, расположенный в Сингапуре. Главная цель ГКИ – оказании помощи в предупреждении в отношении киберпреступлений, главный образом акцентируя внимание на анализах и изучении этого криминального явления. ГКИ консолидирует мировой опыт в сфере информационной безопасности компетентных органов и стратегически важных партнерах.

Кроме того, вышеназванная международная организация установила кодификатор киберпреступлений, а также методов их реализации, присвоив каждому киберпреступлению уникальный алфавитный индекс[137].

---

[135] INTERPOL's contribution to the elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. URL:https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/IGOs/21COM1175-SRIUN_UseInformation_CriminalPurposes_complet.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

[136] Kenichi, T. (2008). *The Role of INTERPOL in the Fight against Cybercrime INTERPOL NCRP for Computer Related Crime,* being a paper presented at 3rd Facilitation Meeting for WSIS Action Line C5 Geneva.

[137] Русскевич Е.А. 2018. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий. – *Международное уголовное право и международная юстиция.* No 3. С. 10–13.

НАТО

Североатлантический альянс (далее – НАТО) создана на основе Североатлантического договора[138] в 1949 году. Под эгидой НАТО– военно-политического блока, объединяющего страны Европы в большей части, приняты следующие документы в части борьбы с «киберпреступлениями»:

1) Таллиннское руководство по международному праву, применимому к кибервойне (далее – Таллинское руководство), 2013 г.[139];
2) Таллиннское руководство по международному праву, применимому к кибервойне 2.0, обновленная версия 2017 (Таллинское руководство 2.0) г[140].

Таллинское руководство было опубликована в марте 2013 года группой независимых международных экспертов. Цель данного документа состоится в том, чтобы изучить, как существующие нормы международного права применимы к кибервойне. Отчет был подготовлен Центром передового опыта совместной киберзащиты НАТО (далее – Киберцентр НАТО), но не предназначен для отражения доктрины НАТО, а только доктрины группы экспертов.

Таллиннское руководство долгое время было ведущей исследовательской инициативой Киберцентра НАТО в Таллинне. Таллиннское руководство (опубликованное в 2013 году) освещает наиболее серьезные действия в киберпространстве – те, которые нарушают запрет на применение силы, дают государствам право осуществлять свое право на самооборону или происходят во время вооруженного конфликта.

Таллиннское руководство 2.0, опубликованное в 2017 году, основывается на вышеназванном документе, рассматривая нормы международного права, регулирующие противоправные деяния в киберпространстве, с которыми

---

[138] Североатлантический пакт (Вашингтон, 4 апреля 1949 г.). Доступ из СПС «ГАРАНТ»
[139] Tallinn Manual on the International Law Applicable to Cyber Warfare& Prepared by International Group Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. General editor N. Schmitt. Cambridge University Press 2013.
[140] Tallinn Manual 2 on the International Law Applicable to Cyber Operations Second Edition Prepared by the International Groups of Experts at the Invitation of NATO Cooperative Cyber Defense Centre of Excellence General Editor: Michael N. Schmitt. Cambridge University Press 2017.

государства сталкиваются изо дня в день, но которые опускаются ниже пороговых значений применения силы или вооруженного конфликта.

Таллинское руководство 2.0 является важным источником для юристов, консультантов и экспертов, занимающихся проблемами кибербезопасности. Формирующаяся государственная практика и принятие публичных решений по международному информационному праву многими государствами после опубликования вышеназванного документа обусловили необходимость обновления этого руководства. Соответственно, в 2021 году Киберцентр НАТО запустил проект под названием «Таллиннское руководство 3.0» (далее – Таллинское Руководство 3.0), рассчитанный на пять лет, который будет включать пересмотр существующих глав и изучение новых тем, важных для государств. В дополнение к практике и официальным заявлениям государств по международному праву будут рассмотрены заявления на международных форумах, таких как форумы в рамках ООН и форумы регионального уровня, например, в рамках Совета Европы[141].

Киберцентр НАТО обеспечивает управление проектами и исследовательскую поддержку, а также предлагает технические консультации и консультации по вопросам политики.

Таким образом, Таллинское руководство – это академическое исследование того, как международное право (в частности, jus ad bellum и международное гуманитарное право) применяется к конфликтам и войнам в международном информационном пространстве.

СНГ

Содружество независимых государств (далее – СНГ) было образовано в результате подписания Соглашения о создании СНГ (Беловежское соглашение) 8 декабря 1991 года в Беловежской пуще[142]. Под эгидой СНГ было заключено следующее соглашение в части противодействия киберпреступлениям: Соглашение о сотрудничестве государств-участников

---

[141] URL: https://ccdcoe.org/research/tallinn-manual/ (дата обращения: 18.07.2024). – Текст: электронный.

[142] Соглашение о создании Содружества Независимых Государств (Минск, 8 декабря 1991 г.). Доступ «СПС Гарант».

Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г. (далее – Соглашение СНГ)[143]. В 2021 году Российская Федерация приняла Федеральный закон о ратификации Соглашения СНГ[144]. Киберпреступления в Соглашении СНГ трактуются, как преступления в сфере информационных технологий. Соглашение СНГ направлено на укрепление связей и сотрудничества между государствами-участниками, а также гармонизации и сближении внутригосударственных законодательств в целях оказания эффективного противодействия киберпреступлениям. Основной целью вышеназванного документа является обеспечение эффективной борьбы с преступлениями в сфере информационных технологий. Взаимодействие между государствами-участницами Соглашения СНГ реализуется посредством компетентных органов непосредственно. Формы сотрудничества компетентные органы государств-участниц данного соглашения осуществляют следующим образом:

1) обмен информацией:

   a) о способах совершения, формах и методах раскрытия, предупреждения, выявления, пресечения и расследования преступлений в сфере информационных технологий;

   b) о готовящихся или совершенных преступлениях в указанной сфере и причастных к ним физических и юридических лицах;

   c) о внутригосударственном законодательстве и международных соглашениях государств-участниц, регламентирующих вопросы раскрытия, расследования, предупреждения, выявления, пресечения преступлений в сфере информационных технологий.

2) реализация запросов об оказании содействия в получении информации, которая может помочь в раскрытии и расследовании киберпреступления, совершенного в отношении гражданина запрашивающей стороны либо

---

[143] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г.). Доступ «СПС Гарант».
[144] Федеральный закон "О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий" от 01.07.2021 N 237-ФЗ (последняя редакция). Доступ «СПС Гарант».

на территории запрашивающей стороны, о проведении оперативно-разыскных мероприятий.

3) обмен результатами научных исследований, нормативными правовыми актами, программными продуктами с целью обеспечение эффективной борьбы с преступлениями в сфере информационных технологий.

Сотрудничество осуществляется на основании запросов от компетентных органов государств-участниц об оказании содействия в соответствии с Соглашением СНГ. Если информация является необходимой для компетентного органа государства-участника, то она может быть передана без запроса об оказании содействия. Запрос направляется в письменной форме. Запросы об оказании содействия могут передаваться с использованием технических средств связи или устно, однако после этого в течение 3 суток они должны быть подтверждены письменно.

Запрос и материалы исполненного запроса могут передаваться по техническим каналам связи в случае, если об этом есть двусторонняя договоренность между компетентными органами Сторон либо эти каналы определены иными международными договорами, участниками которых являются стороны.

Исполнение запроса об оказании содействия осуществляет компетентный орган запрашиваемого государства-участника Соглашения СНГ. При исполнении запроса об оказании содействия применяется законодательство запрашиваемого государства-участника. Отказ в исполнении запроса об оказании содействия в соответствии с Соглашением СНГ возможен, если компетентный орган запрашиваемого государства-участника полагает, что реализация запроса об оказании содействия противоречит внутригосударственному законодательству или международным обязательствам, а также может нанести ущерб суверенитету или национальной безопасности государства.

Сам запрос об оказании содействия содержит следующую информацию:

1) наименование компетентного органа запрашивающего государства-участника и компетентного органа запрашиваемого государства-участника;

2) изложение существа дела;

3) указание цели и обоснование запроса;

4) содержание запрашиваемого содействия;

5) желательные сроки исполнения запроса;

6) любую другую информацию, которая может быть полезна для исполнения запроса, включая соответствующие документы или их заверенные копии;

7) ссылку на Соглашение СНГ.

В соответствии со статьей 11 в исполнении запроса в рамках Соглашения СНГ может быть отказано полностью или частично, если компетентный орган запрашиваемой стороны полагает, что исполнение запроса: может нанести ущерб суверенитету, безопасности или национальным интересам его государства, общественному порядку, а также правам и законным интересам граждан; противоречит национальному законодательству или международным обязательствам запрашиваемой стороны. В случае принятия решения об отказе в исполнении запроса компетентный орган запрашиваемой стороны незамедлительно письменно информирует компетентный орган запрашивающей стороны о своем решении.

Шанхайская организация сотрудничества

Шанхайская организация сотрудничества (далее – ШОС) была основана 15 июня 2001 года в результате подписания Хартии 6 июня 2002 года на заседании Совета глав государств-членов ШОС в Санкт-Петербурге. Под эгидой ШОС было принято соглашение о сотрудничестве в области обеспечения международной информационной безопасности (далее – Соглашение ШОС) (Екатеринбург, 16 июня 2009 года) и вступило в силу с 5 января 2012 года. Соглашение ШОС содержит такие виды угроз, направленные на причинение урона международной информационной безопасности, как информационный терроризм; разработка информационного

оружия; распространение информации, наносящей вред общественно-политической и социально-экономической системам. Всего в Соглашении ШОС перечислено 6 угроз, которые можно приравнять к киберпреступлениям. В целом, Соглашение ШОС направлено на сотрудничество в таких направлениях, как борьба с использованием ИКТ в террористических целях; выработка консолидированных мер в части обеспечения международной информационной безопасности; содействие в надлежащей работе сети «Интернет»; противодействии киберпреступлениям; обмен информацией, опытом, проведение рабочих встреч, конференций, подготовке специалистов; разработка, а также реализация мер доверия в целях обеспечения международной информационной безопасности.

Основным механизмом сотрудничества в соответствии с Соглашением ШОС являются консультации уполномоченных представителей участников и компетентных органов государств участниц. На этих консультациях происходит обмен информацией, анализ возникающих угроз информационной безопасности, а также определения, согласования и координации совместных мер реагирования на такие угрозы. Представление информации не является обязательным в рамках сотрудничества в соответствии с Соглашением ШОС, если раскрытие такой информации может нанести ущерб национальным интересам. Государства-участники данного соглашения реализуют свое сотрудничество в международном информационном пространстве таким образом, чтобы такое сотрудничество способствовало социальному и экономическому развитию и была совместимой с задачами поддержания международной безопасности и стабильности, соответствовала общепризнанным принципам и нормам международного права.

Европейский Союз

В рамках Европейского Союза, учрежденного на основании Маастрихтского договора 1992 года и вступившего в силу 1 ноября 1993 года (далее – ЕС) была разработана Директива 2013/40/ЕС (далее – Директива ЕС) совместно Европейским парламентом и Советом от 12 августа 2013 г. об

атаках на информационные системы и замене Рамочного решения 2005/222/ПВД Совета ЕС[145]. Целями Директивы ЕС являются укрепление сотрудничества между правоохранительными органами государств-членов ЕС, а также сближения уголовного законодательства государств-членов ЕС в части противодействия киберпреступлениям с помощью установления критериев по квалификации преступлений в сфере информационных технологий и назначения соответствующих наказаний[146].

Способом взаимодействия в целях предотвращения и пресечения согласно Директиве ЕС, является обмен информацией о киберпреступлениях между государствами-членами ЕС. Реализуя вышеназванный метод сотрудничества, государства-члены ЕС должны обеспечить наличие внутригосударственного контактного пункта, а также обеспечить доступность существующей сети контактных пунктов 24/7. Государства-члены ЕС должны информировать Европейскую комиссию о назначенном контактном пункте. Европейская комиссия должна передать данную информацию другим государствам-членам ЕС, а также уполномоченным специализированным агентствам и органам ЕС.

В рамках ЕС также существует иной механизм взаимодействия, например арест и выдача преступника. Данный метод закреплен в Рамочном решение Совета ЕС 2002/584//ПВД от 13 июня 2002 года «О европейском ордере на арест и о процедура передачи лиц между государствами-членами» (далее – Рамочное решение)[147]. Европейский ордер на арест обеспечивает возможность для ареста преступников за киберпреступления. В соответствии со статьей 2 вышеприведенного документа, европейский ордер на арест может выдаваться применительно к деяниям, в отношении которых закон выдающего ордер государства-члена предусматривает наказание или меру безопасности,

---

[145] «Договор о Европейском Союзе» (Подписан в г. Маастрихте 07.02.1992) (с изм. и доп. от 13.12.2007). Доступ «СПС Гарант».

[146] Директива N 2013/40/ЕС Европейского парламента и Совета Европейского Союза «Об атаках на информационные системы и о замене Рамочного решения 2005/222/ПВД Совета ЕС» (Принята в г. Брюсселе 12.08.2013). Доступ «СПС Гарант».

[147] Рамочное решение Совета ЕС 2002/584//ПВД от 13 июня 2002 года «О европейском ордере на арест и о процедура передачи лиц между государствами-членами». Доступ «СПС Гарант».

связанные с лишением свободы с верхним пределом не менее двенадцати месяцев, либо – когда уже было назначено наказание или уже была наложена мера безопасности – применительно к обвинительным приговорам, предусматривающим осуждение к лишению свободы не менее, чем на четыре месяца. Если преступления, как они определены в праве выдающего ордер государства-члена, караются в этом государстве наказанием или мерой безопасности, связанными с лишением свободы с верхним пределом не менее трех лет, то применительно к данным преступлениям передача лица на основании европейского ордера на арест согласно условиям настоящего Рамочного решения должна выполняться без проведения проверки на предмет двойной преступности деяния. Киберпреступление, в соответствии с данным документом, к таким преступлениям относится.

В 2004 г. в ЕС было создано Европейское агентство по сетевой и информационной безопасности (*далее – агентство ЕС по кибербезопасности*) с целью достижения в нем высокого общего уровня кибербезопасности. В 2016 г. Европарламент принял Директиву 2016/1148 «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза», в которой закреплены вопросы обеспечения кибербезопасности критической информационной инфраструктуры ЕС. Штаб-квартира агентства ЕС по кибербезопасности расположено в Афинах и функционирует с 1 сентября 2005 года. Агентство ЕС по кибербезопасности повышает надежность услуг и процессов ИКТ с помощью схем сертификации кибербезопасности, вносит вклад в политику ЕС, сотрудничает с государствами-членами ЕС, способствует повышению устойчивой инфраструктуры ЕС. Агентство ЕС по кибербезопасности управляется исполнительным директором и экспертами, а контролируется исполнительным советом и правлением, которые состоят из представителей государств-членов ЕС и Комиссии ЕС.

Кроме того, в рамках ЕС действует полицейская служба под названием Европол, находящаяся в городе Гаага. В компетенцию Европола наряду с

такими преступлениями международного характера, как терроризм и отмывание денег, входит борьба с киберпреступностью. Европол отвечает за работу координирующего характера полицейских служб 27 стран-членов ЕС[148]. Европол полностью интегрирован в организационный механизм ЕС и финансируется из общего бюджета ЕС, а не за счет взносов государств-членов[149]. Что касается организационной структуры Европола, то туда входят: административный совет, директор, финансовый контролер, бюджетная комиссия. Согласно праву ЕС директивы имеют приоритет над национальным правом и являются юридически обязательными для выполнения в соответствии с принципом верховенства права ЕС. Принцип верховенства является продолжением принципа прямого действия права ЕС и означает, что в случае коллизии норм права ЕС и норм национального права государств-членов приоритетом обладают нормы права ЕС[150].

ЕАЭС

В рамках Евразийского экономического союза отсутствует многостороннее соглашение между странами-участниками, которое регламентирует цифровое пространство, обеспечивает информационную безопасность, а также противодействует киберпреступлениям. Кибератакам, например, может подвергнуться платежно-расчетные инфраструктуры стран ЕАЭС[151]. В связи с этим необходимо тесное сотрудничество между странами-участниками ЕАЭС. На данный момент существуют двусторонние соглашения между государствами-участниками ЕАЭС в части усиления координации и укрепления взаимодействия в борьбе с киберпреступлениями.

В начале 2021 г. между Правительством Российской Федерации и Правительством Киргизской Республики было подписано Соглашение о

---

[148] URL: https://www.europol.europa.eu (дата обращения: 18.07.2024). – Текст: электронный.

[149] Скуратова А. Ю. Новый Европол: основные изменения в статусе Европейского полицейского ведомства // Международное право - International Law. - М.: Юрис Пруденс, 2010, № 3 (43). - С. 55–59.

[150] Право Европейского Союза: учебник и практикум для бакалавриата и магистратуры / под ред. А. Х. Абашидзе, А. О. Иншаковой. — М.: Издательство Юрайт, 2016. — 482 с. — Серия: Бакалавр и магистр. Академический курс. С. 33.

[151] Пищик В.Я., Алексеев П. В. Киберпреступность как ключевой операционный риск платежно-расчетной инфраструктуры глобальной финансовой системы и подходы к его регулированию в ЕАЭС // Финансовый журнал. № 3 2021. С. 54–66.

сотрудничестве в области обеспечения международной информационной безопасности[152].

Аналогичное соглашение есть между Россией и Беларусью, которое было подписано в 2013 г[153].

Договор между Россией и Беларусью в сфере кибербезопасности содержит положения, направленные на стремление государств установить юридическую и структурированную основы кооперации участников в части обеспечения кибербезопасности и юридических методов осуществления взаимных действий в целях обеспечения кибербезопасности.

Двусторонний договор между Россией и Кыргызстаном в части кибербезопасности отражает укрепление сотрудничества правоохранительных органов участников по линии международной информационной безопасности. Кроме того, осуществление перманентных консультаций по данной проблематике и обмену данными.

Таким образом, вышеприведенные договоры направлены на укрепление скоординированного сотрудничества в части обеспечения международной информационной безопасности.

По мнению А. А. Ефремова, в последние годы информационное пространство все больше выступает в качестве основной сферы геополитической и экономической конкуренции государств, что несет новые угрозы информационной безопасности как для самих государств, так и для личности и общества. Значение обеспечения и защиты государственного суверенитета возрастает и в связи с процессами цифровой интеграции в рамках региональных международных организаций[154].

---

[152] Соглашение между Правительством Российской Федерации и Правительством Киргизской Республики о сотрудничестве в области обеспечения международной информационной безопасности (Москва, 25 февраля 2021 г.). Доступ «СПС ГАРАНТ».

[153] Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности (Москва, 25 декабря 2013 г.). Доступ «СПС ГАРАНТ».

[154] Ефремов А.А. Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации: дис. … д-ра юрид. наук. / Ефремов А.А. – Москва, 2021. – 418 с.

10 февраля 2022 г. между Россией и Арменией по итогам консультаций на экспертном уровне был согласован проект двустороннего межправительственного Соглашения о сотрудничестве в области обеспечения информационной безопасности.

На данном этапе юридические документы стран-участников ЕАЭС отображают неодинаковый характер заинтересованности в вопросах кибербезопасности[155]. Отсутствие единообразных идей и целей в части кооперации государств ЕАЭС приводит к запаздыванию в реагировании на информационные угрозы в правовой, экономической и идеологической плоскостях интеграции[156].

Таким образом, в целях эффективного выявления, расследования, пресечения киберпреступлений целесообразно на уровне ЕАЭС разработать соглашение регионального характера, которое будет распространяться на все государства-участницы. Данное соглашение в обозримом будущем поспособствует странам-участникам ЕАЭС в обеспечение кибербезопасности и противодействии киберпреступлениям путем обмена информацией, взаимной помощью в части расследования киберпреступлений (например, сбор доказательств), а также запросах о выдаче преступников. Вышеперечисленные механизмы взаимодействия должны обеспечить эффективность в части оперативного сотрудничества между странами - участницами ЕАЭС. На данный момент существует аналогичное соглашение в рамках СНГ. Для ЕАЭС, как более молодой международной организации наднационального характера, принятие такого регионального соглашения является актуальным.

Региональный уровень сотрудничества отличает более скоординированный и углубленный характер. Кроме того, в институциональном плане для развития регионального сотрудничества по

---

[155] Смирнов А. И. Международная информационная безопасность: теория и практика: учебник для вузов. В трех томах. Том 10 / под ред. А. В. Критских. 2-е изд. доп. М.: Аспект Пресс, 2021 384 с.

[156] Ильина М.Ю. Перспективы сотрудничества государств — членов ЕАЭС в области информационной безопасности. *ЕВРАЗИЙСКАЯ ИНТЕГРАЦИЯ: экономика, право, политика*. 2022;16(1):119-127.

предотвращению киберпреступности в рамках ЕАЭС целесообразно рассмотреть вопрос о создании регионального международного правоохранительного органа.

Африканский Союз

В рамках Африканского союза (далее – АС), учрежденного на основании Сиртской декларации[157] (принятой 9 сентября 1999 года) и Учредительного Акта АС (подписан 11 июля 2000 года в Ломе, Того)[158] была разработана Конвенция Африканского союза о кибербезопасности и защите персональных данных[159], (г. Малабо, 27 июня 2014 года) направленная на гармонизацию и укрепление законодательства стран Африки в сфере организации торговли через информационные сети, защите персональных данных, укрепление в части содействия и сотрудничества в целях обеспечения информационной безопасности и борьбы с киберпреступлениями. Кроме того, Конвенция АС содержит руководящие принципы в части обнаружения и пресечения киберпреступлений. Конвенция АС отражает озабоченность африканскими государствами проблематикой, связанной с киберпреступлениями, как глобальной угрозы[160].

Глава III Конвенции АС отображает информационную безопасность, а также борьбу против киберпреступлений. В соответствии с вышеназванной главой страны-участники обязуются на внутригосударственном уровне установить политику информационной безопасности, которая определит критическую информационную инфраструктуру, как важный стратегический элемент. Кроме того, установит риски в сфере кибербезопасности и методы борьбы с ними.

Стороны Конвенции АС обязуются принять юридические и регулятивные меры в части борьбы с киберпреступлениями, в частности, признав уголовно

---

[157] URL: https://archives.au.int/handle/123456789/10157?show=full/ (дата обращения: 18.07.2024). – Текст: электронный.
[158] URL: https://au.int/en/constitutive-act/ (дата обращения: 18.07.2024). – Текст: электронный.
[159] URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection/ (дата обращения: 18.07.2024). – Текст: электронный.
[160] Ball K. M. African Union Convention on Cyber Security and Personal Data Protection // International Legal Materials. — 2017. — Vol. 56. — Iss. 1. — P. 164-192.

наказуемыми деяния, посягающие на конфиденциальность, целостность, доступность информации[161].

Ч. 3 ст. 25 Конвенции АС постулирует о том, что необходимо соблюдать основные права и свободы человека при обеспечении информационной безопасности, которые гарантируются внутригосударственными актами и международными договорами. Анализирую вышеназванное положение, можно сделать вывод о том, что права и свободы человека имеют превалирующее значение в международном праве, и что несмотря на важность охраняемых отношений в области информационного пространства, страны должны соблюдать этот основный принцип[162].

Более того, ч. 4 ст. 25 указывает на важность обороны элементов критической инфраструктур. Обеспечение безопасности вышеприведённого объекта позволит государствам обеспечить в сохранности информационный суверенитет, а также предотвратить угрозу внутригосударственной безопасности. Данный подход можно достичь благодаря санкциям и укреплению мер охраны от нежелательных кибератак.

Ст. 26 Конвенции АС отображает необходимость регулярной кооперации между всеми участниками информационного пространства, как государственных структур, так и частного сектора. В целях обеспечения надлежащей кибербезопасности им необходимо консолидировать усилия в области разработки информационных систем, а также создание новых методов в части использования ИКТ. Страны-участники Конвенции АС полагают, что необходимо увеличение роста осведомленности среди пользователей ИКТ для обеспечения надлежащей информационной безопасности. Более того, присоединение к противодействию с компьютерными преступлениями институтов гражданского общества является также необходимым элементом.

---

[161] Peter A. S. Cyber resilience preparedness of Africa's top-12 emerging economies // International Journal of Critical Infrastructure Protection. — 2017. — Vol. 17. — P. 49-59.

[162] Abdulrauf L. A., Fombad C. M. The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa? // Journal of Media Law. — 2016. — Vol. 8. — Iss. 1. — P. 67-97.

Ст. 28 Конвенции АС включает в себя положения об унификации, взаимной правовой помощи по делам, связанными с киберпреступлениями, а также обмене информацией. В положении об обмене информацией содержится призыв к странам учреждать образования в целях содействия обмену данными об угрозах информационной безопасности. Кроме того, Конвенция АС предписывает странам-участникам «использовать существующие механизмы международного сотрудничества», которые могут включать в себя «международные, межправительственные, региональные или… государственно-частные партнерства», для принятия мер реагирования на киберпреступность.

Лига Арабских государств

В рамках Лиги арабских государств (далее – ЛАГ), созданной на основании Александрийского протокола (принят 7 октября 1944 года в Александрии, Египет) была разработана Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий[163]. Основной целью Конвенции ЛАГ является расширение и укрепление сотрудничества между арабскими странами в сфере борьбы с киберпреступлениями в целях обеспечения безопасности арабских государств в информационном пространстве. Конвенция ЛАГ была принята 21 декабря 2010 года в Каире, Египет.

Конвенция ЛАГ содержит такие киберпреступления, как несанкционированный доступ к персональным данным, кибертерроризм, нарушение авторских и смежных прав, а также хищение с использованием ИКТ. Кроме того, Конвенция ЛАГ включает положения о процессуальном праве, юрисдикции и взаимной правовой помощи[164]. Кроме того, статьи 32 и 34 Конвенции ЛАГ содержат положения об оказания взаимной помощи, процедурах сотрудничества и подачи запросов об оказании взаимной помощи.

---

[163] URL: https://www.unodc.org/e4j/ru/cybercrime/module-3/key-issues/international-and-regional-instruments.html/ (дата обращения: 18.07.2024). – Текст: электронный.

[164] П. Шерстюк. Сборник материалов по проблематике информационной безопасности государств-членов лиги арабских государств. Москва – 2023. С. 242.

Экономическое сообщество Западноафриканских государств

Экономическое сообщество Западноафриканских государств (ЭКОВАС) было основано 28 мая 1975 года в результате подписания Лагосского соглашения в городе Лагос, Нигерия[165]. В рамках ЭКОВАС разработана директива Экономического сообщества Западноафриканских государств (ЭКОВАС) C/DIR. 1/08/11 о борьбе с киберпреступностью в рамках ЭКОВАС от 19 августа 2011 года (далее – Директива ЭКОВАС)[166]. Целью данной директивы является установление между государствами-участниками тесной кооперации в части взаимной правовой помощи, а также криминализации киберпреступности во внутригосударственном законодательстве и выдаче киберпреступников в делах, коррелирующих с киберпреступностью и кибербезопасностью в целом. Директива ЭКОВАС подчеркивает, что киберпреступность является феноменом, требующая определённой классификации киберпреступлений, которые в свою очередь связаны с такими преступлениями, как кража, мошенничество, получение краденых товаров, шантаж, совершенные при помощи сети «Интернет».

В рамках ЭКОВАС также действует Конвенция об оказании взаимной помощи по уголовным вопросам 1992 года. Данный документ содержит такой механизм взаимодействия в части борьбы с киберпреступлениями, как запрос об оказании взаимной правовой помощи (статья 5). Другой договор, Конвенция ЭКОВАС о выдаче 1994 года, представляет собой соглашение о выдаче лиц запрашивающей стране в случаях, когда преступление, влекущее выдачу, соответствует установленному минимальному порогу наказания. Например, в соответствии со статьей 3 вышеназванного документа, порог наказания составляет минимум два года.

---

[165] https://www.loc.gov/collections/country-studies/about-this-collection/ (дата обращения: 18.07.2024). – Текст: электронный.

[166] The Economic Community of West African States (ECOWAS) Directive on Fighting Cyber Crime within ECOWAS. 2011 URL: https://issafrica.org/ctafrica/uploads/Directive%201:08:11%20on%20Fighting%20Cyber%20Crime%20within%20ECOWAS. pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

Совет Европы

В рамках Совета Европы принята Конвенция о преступности в сфере компьютерной информации Совета Европы (Будапешт, 23 ноября 2001 г.), положения которой направлены на защиту основных прав и свобод человека в информационном пространстве и основаны на положениях Европейской конвенции о защите прав человека и основных свобод, принятой Советом Европы в 1950 году, Международным пактом о гражданских и политических правах, принятым Организацией Объединенных Наций в 1966 году, а также других применимых международных договоров по правам человека и предусматривающих принцип соразмерности, что прямо предусмотрено в статье 15 Конвенции 2001 года.

Конвенция 2001 года носит комплексный характер и содержит положения, регламентирующие вопросы квалификации противоправных деяний, унифицирующие нормы процессуального характера, а также вопросы международной правовой помощи.

Основная цель Конвенции СЕ, изложенная в преамбуле, заключается в проведении общей уголовной политики, направленной на защиту общества от киберпреступности, в частности, путем принятия соответствующего законодательства и содействия международному сотрудничеству.

Конвенция СЕ принята Комитетом министров Совета Европы 8 ноября 2001 года и открыта для подписания в Будапеште 23 ноября того же года.
1 июля 2004 года Конвенция вступила в силу. Конвенция СЕ является первооткрывателем в части соглашений, регулирующих киберпреступления.

Конвенция СЕ призывает стран-участниц актуализировать положения внутригосударственного права в части незаконного доступа к компьютерным системам, взлома базы данных, нарушения авторских прав, мошенничества с использованием компьютеров, распространением детской порнографии и других противоправных действий в киберпространстве.

В рамках Конвенции СЕ реализуются следующие цели:

1) международное сотрудничество, которое включает содействие страны-участницы Конвенции СЕ правоохранительным органам другой стране-участнице данного соглашения;
2) совершенствование методов расследования киберпреступлений;
3) сдерживание атак, направленных против конфиденциальности, целостности и доступности компьютерных систем, сетей и данных.

Данный международный договор содержит положения, унифицирующие порядок обеспечения конкретных компьютерных данных и их получения компетентными органами. Предусматривается необходимость принятия государствами мер для оперативного обеспечения сохранности конкретных компьютерных данных (статья 16 Конвенции СЕ). В целях реализации данных мер предусматривается определение на территории государства компетентного лица и наделение его обязанностями по хранению и обеспечению целостности компьютерных данных для предоставления доступа к ним в случае необходимости их раскрытия (пункт 2 статьи 16 Конвенции СЕ). Раскрытие таких данных осуществляется в целях идентификации поставщиков услуг и пути, которым передавалось данное сообщение (статья 17 Конвенции СЕ).

Предусматривается получение доказательств в виде компьютерных данных от лица, у которого они находятся во владении или под контролем и сведений об абонентах от поставщика услуг.

Кроме лиц, определяемых для хранения и предоставления конкретных компьютерных данных, право на сбор и запись компьютерных данных (данных о потоках информации) в режиме реального времени предоставляется компетентным органам государства, а также поставщикам услуг при соблюдении конфиденциальности самого факта осуществления таких полномочий (раздел 5 Конвенции СЕ)

Конвенция также унифицирует положения об обыске и выемке компьютерных данных, предоставляя при этом компетентным органам государства право распространить производимый обыск или иной

аналогичный доступ как на саму систему, так и на взаимосвязанную с ней, если на ней хранятся искомые данные (статья 19 Конвенции СЕ).

Вместе с тем Конвенция СЕ упоминает институт экстрадиции, которая возможна на основании договора об экстрадиции, а также Европейской Конвенцией о выдаче 1957 года (далее – Конвенция о выдаче)[167].

В самой Конвенции СЕ экстрадиция (выдача) упоминается в статье 24, где посвящены целых 7 пунктов данному институту.

В пункте 1 уточняется, что экстрадиция применяется только к тем преступлениям, которые признаны таковыми в соответствии со статьями 2–11 Конвенции СЕ, и которые по национальному закону обеих заинтересованных сторон караются лишением свободы на максимальный срок не менее одного года или более суровым наказанием.

Пункт 2 постулирует о том, что преступления, предусмотренные статьями 2–11 Конвенции СЕ, рассматриваются как входящие в число преступлений, предполагающих экстрадицию, в любом двустороннем или многостороннем соглашении об экстрадиции, существующем между сторонами.

Согласно пункту 3, если какая-либо сторона, выдвигающая в качестве условия экстрадиции наличие договора, получает запрос об экстрадиции от другой стороны, с которой у нее нет соглашения об экстрадиции, она может использовать Конвенцию СЕ в качестве правового основания для экстрадиции запрашиваемого лица.

В соответствии с пунктом 4, стороны, не выдвигающие в качестве условия экстрадиции наличие соглашения, в отношениях между собой признают уголовные преступления, упомянутые в статьях 2–11 Конвенции СЕ, в качестве преступлений, предполагающих экстрадицию.

Пункт 5 предусматривает, что запрашиваемая сторона не обязана осуществлять экстрадицию, если она не удовлетворена тем, что были

---

[167] Европейская Конвенция о выдаче ETS № 024 (Париж, 13 декабря 1957 г.). URL: https://rm.coe.int/ (дата обращения: 18.07.2024). – Текст: электронный.

выполнены не все положения и условия, предусмотренные применимым международным договором или национальным законом.

Таким образом, это еще один пример принципа, согласно которому сотрудничество должно осуществляться в соответствии с положениями применимых международных документов, действующих между сторонами, взаимных договоренностей или внутреннего законодательства.

В пункте 6 отображен принцип *aut dedere aut judicare (либо выдай, либо суди),* и его действие заключается в следующем, когда сторона соглашения, если она не подвергла уголовному преследованию находящегося на ее территории преступника, обязана выдать его другой стороне, если последняя обратиться к ней с соответствующей просьбой для целей такого преследования.

Пункт 7 требует, чтобы каждая сторона при подписании или сдаче на хранение своего документа о ратификации, принятии, об одобрении или о присоединении, сообщает Генеральному Секретарю Совета Европы наименование и адрес каждого органа, ответственного за направление или получение запроса о выдаче или предварительном аресте при отсутствии договора.

Конвенция СЕ предоставляет возможность оказания международной правовой помощи на стадии расследования, а также судебного разбирательства (статья 25 Конвенции СЕ), что существенно расширяет возможности компетентных органов по оперативному сбору и фиксации электронных доказательств.

Международная правовая помощь в рамках Конвенции СЕ осуществляется также в виде предварительных мер, которые могут быть приняты в целях сохранности данных, расположенных в компьютерных системах запрашиваемого государства и в отношении которых предполагается обыск, выемка, иные действия, обеспечивающие сохранность или доступ к данным (ст. 29 Конвенции).

Оказание международной правовой помощи предусматривается для обеспечения сохранения и раскрытия данных и может быть осуществлено в виде обыска, выемки или аналогичных действий в указанных целях; доступа к хранящимся на территории запрашиваемого государства компьютерным данным; сбор данных о потоках информации в режиме реального времени; сбор или запись в режиме реального времени содержания данных конкретных сообщений, передаваемых с помощью компьютерной системы (раздел 2 Конвенции СЕ).

Одной из новых форм международной правовой помощи, предусмотренной в Конвенции СЕ, является создание в каждом государстве круглосуточного контактного центра, призванного обеспечить оказание неотложной помощи в целях сбора доказательств или судебных разбирательств в отношении киберпреступлений.

Таким образом, оказание международной правовой помощи предусматривается как в традиционных процессуальных, так и в новых организационных формах.

Порядок направления запросов о правовой помощи и получение сведений учитывает специфическую природу электронных данных, их уязвимость к потере или изменению. В Конвенции СЕ предусматривается возможность направления соответствующих запросов и получение сведений с помощью оперативных средств связи, в качестве которых рассматривается факсимильная связь и электронная почта (пункт 3 статьи 25 Конвенции). Оказание международной правовой помощи осуществляется через назначаемый каждым государством центральный орган (п. 2а статьи 27).

Особое значение для оказания международной правой помощи в данной сфере является соблюдение конфиденциальности (пункт 8 статьи 27 Конвенции). При этом сохранение конфиденциальности может рассматриваться в качестве обязательного условия для оказания правовой помощи (статьи 28, 29 Конвенции), при несоблюдении которого запрос не приобретает силу обязательного для запрашиваемой стороны.

На основании пункта 2 статьи 36, Конвенцию СЕ ратифицировали 68 стран, в том числе несколько крупных неевропейских стран, таких как Аргентина, Канада, Япония, Южная Африка. Соединенные Штаты Америки ратифицировали Конвенцию в 2006 году.

Российская Федерация не является участником Конвенции. Согласно Распоряжению Президента Российской Федерации от 15.11.2005 № 557-рп[168] Российская Федерация оставляла за собой право определиться с участием в Конвенции при условии возможного пересмотра положений пункта «b» статьи 32, поскольку не исключается возможность такого толкования и применения этого положения, которые могут нанести ущерб суверенитету и национальной безопасности государств-участников, правам и законным интересам их граждан и юридических лиц. В соответствии с указанным пунктом «b» статьи 32 Конвенции сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему.

Поскольку пересмотр положений пункта «b» статьи 32 Конвенции в порядке, предусмотренном пунктом 3 статьи 46 Конвенции, либо в ином порядке, избранном Сторонами, не осуществлен, Распоряжением Президента Российской Федерации от 22 марта 2008 года Распоряжение Президента Российской Федерации от 15 ноября 2005 года № 557-рп «О подписании Конвенции о киберпреступности» признано утратившим силу[169].

Исходя из вышесказанного, в целях эффективной реализации положений Конвенции СЕ странам-участницам следует продолжить курс на укрепление межгосударственного сотрудничества в области гармонизации национального

---

[168] Распоряжение Президента Российской Федерации от 15.11.2005 г. № 557-рп о подписании Конвенции о киберпреступности. Доступ из СПС «ГАРАНТ».

[169] Распоряжение Президента Российской Федерации о признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 года № 557-рп. «О подписании Конвенции о киберпреступности» от 28 марта 2008 года № 144-рп. Доступ из СПС «ГАРАНТ».

законодательства, которое криминализирует деяния с использованием ИКТ, а также ускорит расследование киберпреступлений. Важно подчеркнуть, что сфера действия Конвенции охватывает не только преступления против компьютерных систем и данных, но и преступления, совершенные с помощью электронных средств, к ним относятся, например, мошенничество, распространение детской порнографии и нарушение авторских прав. Также Конвенция СЕ направлена на совершенствование методов расследования киберпреступлений, требуя, чтобы каждая страна-участница актуализировала новые методы по розыску преступников у своих национальных правоохранительных органов. Наконец, Конвенция СЕ поощряет и расширяет международное сотрудничество, поскольку требует, чтобы каждая сторона Конвенции СЕ оказывала содействие правоохранительным органам другой стороне. И, более того, дает право спецслужбам стран-участниц без предварительного уведомления вмешиваться в цифровое пространство друг друга.

Кроме того, в рамках Совета Европы действует Европейский комитет по проблемам преступности (далее – ЕКПП), созданный в 1958 году и, наделенный Комитетом министров полномочиями в части надзора и координации деятельности Совета Европы в сфере предупреждения преступности и борьбы с ней. Заседания ЕКПП проходят в штаб-квартире Совета Европы в Страсбурге. В случае возникновения спора между странами-участницами в части толкования или применения Конвенции СЕ, государства-члены стремятся урегулировать спор путем переговоров и иных согласительных процедур, в том числе передать спор на рассмотрение в ЕКПП. Помимо этого, ЕКПП определяет приоритеты межправительственного правового сотрудничества, вносит предложения Комитету министров о деятельности в области уголовного права и уголовно-процессуального права, криминологии. Разрабатывает конвенции, рекомендации и отчеты. В дополнение к своим регулярным заседаниям ЕКПП также организует конференции по конкретным темам, представляющим интерес в области

уголовного права, в том числе Конференции министров юстиции Совета Европы. На сегодняшний день под руководством ЕКПП было разработано более 40 конвенций по уголовному праву, а также большое количество рекомендаций. ЕКПП обеспечил ключевое юридическое и техническое руководство, а также надзор за многими известными конвенциями Совета Европы.

Таким образом, в целях эффективной реализации положений Конвенции СЕ странам-участникам следует продолжить курс на укрепление межгосударственного сотрудничества в области гармонизации национального законодательства, которое криминализирует деяния с использованием ИКТ, а также ускорит расследование киберпреступлений. Важно подчеркнуть, что сфера действия Конвенции СЕ охватывает не только преступления против компьютерных систем и данных, но и преступления, совершенные с помощью электронных средств, к ним относятся, например, мошенничество, распространение детской порнографии и нарушение авторских прав. Также Конвенция СЕ направлена на совершенствование методов расследования киберпреступлений, требуя, чтобы каждая страна-участница актуализировала новые методы по розыску преступников у своих национальных правоохранительных органов. Наконец, Конвенция поощряет и расширяет международное сотрудничество, поскольку требует, чтобы каждая сторона Конвенции СЕ оказывала содействие правоохранительным органам другой стороне.

Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем (далее – Протокол № 1) принят 28 января 2003 г. Итоговый текст Протокола № 1 был принят Комитетом министров Совета Европы в 2002 г. Протокол № 1 вступил в силу 1 марта 2006 г. По состоянию на 2023 г., Протокол № 1 ратифицировало 34 государства, и еще 11 стран подписали документ, но не ратифицировали его. Российская

Федерация, Соединенные Штаты Америки не являются участниками данного Протокола № 1. В частности, США не подписало Протокол № 1 из-за противоречий положениям Конституции Соединенных Штатов Америки. Министерство юстиции США заявило, что подписание Соединенными Штатами Протокола № 1 было бы неконституционным, поскольку первая поправка Конституции США гарантирует свободу выражения мнений. Информационный центр электронной конфиденциальности в своем письме возражал против ратификации Конвенции США, поскольку это «создало бы прецедент расследований, при которых не были бы обеспечены должным образом гарантии конфиденциальности и иные гражданские свободы»[170].

К странам, не подписавшим Протокол № 1, также можно отнести Великобританию. Однако, Канада в 2005 присоединилась к Протоколу № 1 и тем самым стала первой неевропейской страной, присоединившейся к Протоколу № 1.

Положения Протокола № 1 носят обязательный характер. В целях добросовестного исполнения обязательств в соответствии с Протоколом № 1, государствам-участникам необходимо принять соответствующие законы на внутригосударственном уровне, а также обеспечить его применение.

Со времени принятия Конвенции СЕ и Протокола № 1 ИКТ прошли процесс эволюционирования во многих социальных сферах. В то же время использование ИКТ в преступных целях значительно возросло.

В настоящее время киберпреступления рассматриваются мировым сообществом, как серьезная угроза, направленная на нарушение прав и свобод человека, а также угроза целостности информационного суверенитета государств. Угрозы, исходящие от киберпреступлений, многочисленны. Например, сбыт поддельных медицинских изделий; незаконный оборот наркотиков; вовлечение несовершеннолетних в незаконную деятельность; создающую угрозу их жизни и здоровью; преступное использование

---

[170] URL: www.justice.gov/criminal/cybercrime/COEFAQs.htm/ (дата обращения: 18.07.2024). – Текст: электронный.

криптовалют. Во время пандемии COVID-19 в странах наблюдался значительный рост совершения киберпреступлений. Например, незаконное распространение фальсифицированных лекарственных средств и медицинских изделий. Данный вид киберпреступления получил свое глобальное распространение в эпоху пандемии COVID-19, когда преступники начали активно регистрировать доменные имена, содержащие такие обозначения, как «coronavirus» или «COVID». В результате многие потребители были введены в заблуждение и приобрели медицинские маски, дезинфицирующие средства для рук, а также поддельные лекарства, которые якобы предотвращают или лечат от COVID-19[171].

Таким образом, пандемия COVID-19 спровоцировала массовый всплеск кибератак по всему миру. Усугубление глобального кризиса в области здравоохранения резким ростом киберпреступлений, создает значительную нагрузку на правоохранительные органы по всему миру.

Несмотря на прогрессивное развитие информационных технологий, а вместе с тем и появления новых видов киберпреступлений, положения, воплощенные в Конвенции СЕ, остаются базовыми в части регулирования киберпреступлений.

Реализуя положения Конвенции СЕ, страны-участницы с уважением относятся к обязательству правительств в части защиты лиц от преступлений, независимо от того, совершаются ли они онлайн или офлайн, посредством эффективного уголовного преследования и дальнейшего судебного разбирательства.

В действительности некоторые страны-участницы Конвенции СЕ считают, что они связаны международным обязательством предоставлять средства защиты от преступлений, совершенных с помощью компьютерной системы, ссылаясь на процедуры и полномочия для проведения уголовных

[171] COVID-19 Cybercrime Analysis Report-August 2020 (Interpol). URL: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (дата обращения: 18.07.2024). – Текст: электронный.

расследований или судебных разбирательств, которые стороны должны установить в соответствии с Конвенцией СЕ.

Так, в деле *К.U. против Финляндии*[172], обжалуется уклонение от принуждения сервис-провайдера раскрыть данные о личности разыскиваемого за размещение непристойного объявления о несовершеннолетнем на интернет-сайте знакомств. Европейский Суд по правам человека (далее – ЕСПЧ) в своем постановлении от 2 декабря 2008 года указал, что по делу допущено нарушений требований статьи 8 Конвенции о защите прав человека и основных свобод (далее – Европейская Конвенция). В порядке применения статьи 41 Европейской Конвенции, ЕСПЧ присудил выплатить заявителю 3 000 евро в счет компенсации причиненного морального вреда.

Страны-участницы Конвенции СЕ стремятся выполнять свои обязательства по противодействию киберпреступлениям, опираясь на различные механизмы и органы, созданные в соответствии с Конвенцией СЕ, и предпринимая необходимые методы для обеспечения более эффективных расследований киберпреступлений и судебных разбирательств. Важно отметить, что реализации Конвенции СЕ способствует *Комитет Конвенции о киберпреступности* (далее – Комитет), учрежденный в соответствии со статьей 46 Конвенции. Комитет состоит из представителей государств-участниц Конвенции, которые ратифицировали или подписали договор. Комитет осуществляет толкование Конвенции. Также Комитет консультирует по вопросам в части эффективного использования и реализации положений Конвенции; обмена информацией по правовым, политическим или технологическим аспектам, относящихся к киберпреступлениям; сбора доказательств в электронной форме; рассмотрении дополнений или поправок к Конвенции. Таким образом Комитет является по большей части совещательно-консультативным органом, который также может издавать рекомендации в части применения положений Конвенции.

---

[172] Постановление Европейского Суда по правам человека от 2 декабря 2008 г. Дело «K.U. против Финляндии» [K.U. v. Finland] (жалоба № 2872/02). Доступ из СПС «ГАРАНТ».

Стоит отметить еще одно подразделение, которое занимается вопросами киберпреступлений. Офис Программы Совета Европы по борьбе с киберпреступностью (далее – Офис по борьбе с киберпреступностью) находится в Бухаресте (Румыния) и отвечает за оказание помощи странам по всему миру в укреплении их правовой базы по реагированию на киберпреступления и обмену электронными доказательствами в соответствии с положениями Конвенции. Офис по борьбе с киберпреступностью занимается следующими вопросами:

1. Укрепление законодательства о киберпреступности и электронных доказательствах в соответствии со стандартами верховенства закона и прав человека (включая защиту данных);
2. Подготовка судей, прокуроров и сотрудников правоохранительных органов;
3. Создание специализированных подразделений по борьбе с киберпреступностью и судебной экспертизой и улучшение межведомственного сотрудничества;
4. Содействие сотрудничеству между государственным и частным секторами;
5. Защита детей от сексуального насилия в сети «Интернет»;
6. Повышение эффективности международного сотрудничества.

В 2012 году Комитет учредил ad hoc группу под названием «Трансграничная группа». В 2014 Комитет принял ряд актов рекомендационного характера в части взаимной помощи по киберпреступлениям, положения которых в последующем должными были найти свое отражение в новом протоколе к Конвенции СЕ. В 2015 году была создана рабочая группа по доступу уголовного правосудия к доказательствам, хранящимся в облаке, в том числе в рамках взаимной правовой помощи (далее – рабочая группа СЕ).

В 2016 году рабочая группа СЕ пришла к выводу, что - «количество устройств (включая мобильные устройства), сервисов и пользователи, а

вместе с ними и число жертв достигли таких масштабов, что лишь незначительная доля киберпреступлений или других преступлений, связанных с обнаружением электронных доказательств, будет раскрыта. Большое количество жертв киберпреступлений с малой долей вероятности ожидают, что правосудие восторжествует, а преступники понесут наказание». Основные проблемы, выявленные рабочей группой СЕ, связаны с «облачными вычислениями, территорией и юрисдикцией» и, следовательно, с трудностями в части обнаружения электронных доказательств. Таким образом, вышесказанное в очередной раз подтверждает, что киберпреступления имеют латентный характер.

При рассмотрении выводов рабочей группы СЕ государства-участники Конвенции СЕ пришли к заключению, что нет необходимости вносить поправки в Конвенцию. Однако, государства-участники определились в необходимости принятия дополнительных мер с целью расширения и усовершенствования сотрудничества, а также обнаружении органами уголовного правосудия электронных доказательств.

В связи с быстро растущим количеством киберпреступлений и появлением определённой сложности в обнаружении электронных доказательств, которые могут находиться в юрисдикции иностранного государства, компетенция правоохранительных органов ограничена территорией национальной границы. Как итог, судебные решения выносятся по малой доле совершенных киберпреступлений из-за отсутствия электронных доказательств, информацией о которых обладают правоохранительные органы иностранных государств[173].

В целях скорейшего разрешения этой проблемы был принят Второй Дополнительный протокол к Конвенции Совета Европы «О преступности в сфере компьютерной информации» 2001 г. под названием Второй Дополнительный протокол к Конвенции о киберпреступности о расширении

[173] Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar. Cybercrime and Digital Forensics: An Introduction. 2018. P. 42.

сотрудничества и обнаружении электронных доказательств (Страсбург 12/05/2022) (СДСЕ № 224)[174].

Протокол № 2 принят Комитетом министров Совета Европы 17 ноября 2021 года и открыт для подписания в Страсбурге с 12 мая 2022 г. Протокол № 2 открыт для подписания государствами-членами Конвенции Совета Европы «О преступности в сфере компьютерной информации» 2001 г. Протокол № 2 предусматривает правовую основу для раскрытия информации о регистрации доменных имен и для прямого сотрудничества с поставщиками услуг с целью получения информации об абонентах, кооперации в чрезвычайных ситуациях, гарантии защиты и конфиденциальности персональных данных. Для вступления Протокола № 2 в силу необходимо 5 ратификацией. На сегодняшний день Протокол № 2 подписало 31 государство, и ни одно не ратифицировало. Российская Федерация не подписала данный документ. США и Япония подписали Протокол № 2, однако эти государства не являются членами Совета Европы[175].

Большое внимание Протокол № 2 уделяет защите персональных данных. В рамках сотрудничества сторона-участник может временно приостановить передачу персональных данных в случае систематического или существенного нарушения, которое представляет риск для безопасности физического лица или может нанести репутационный или денежный ущерб физическому лицу, и в этом случае она должна немедленно уведомить другую сторону и начать консультации с ней. Если консультации не дали результата, другая сторона Протокола № 2 может приостановить передачу персональных данных. Любые персональные данные, переданные до приостановления, подлежат обработке в соответствии с Протоколом № 2[176].

---

[174] URL: https://www.coe.int/en/web/cybercrime/home/ (дата обращения: 18.07.2024). – Текст: электронный.
[175] URL: https://www.coe.int/en/web/cybercrime/home/ (дата обращения: 18.07.2024). – Текст: электронный.
[176] Convention on Cybercrime, Protocol on xenophobia and racism, Second protocol on enhanced co-operation and disclosure of electronic evidence, Explanatory Reports and Guidance Notes, Council of Europe, April 2022. URL: https://www.coe.int/documents/8475493/0/PREMS+001323+GBR+2023+EN+Convention+booklets+Jan2023.pdf/aea70363-b646-e041-8e0a-dc6ed5f645b0?t=1675948139269/ (дата обращения: 18.07.2024). – Текст: электронный.

На 17-й пленарной сессии Комитет (8 июня 2017 года) утвердил техническое задание для подготовки Протокола № 2 на основе предложений, подготовленных рабочей группой СЕ. Комитет решил приступить к разработке Протокола № 2 по своей собственной инициативе в соответствии с пунктом 1.c статьи 46 Конвенции СЕ. 14 июня 2017 года заместитель генерального секретаря Совета Европы проинформировал Комитет министров (1289-е заседание заместителей министров) об инициативе, предложенной Комитетом.

Отправной точкой для положения начала работы над Протоколом № 2 стали результаты оценки положений Конвенции СЕ в части взаимной помощи, проведенной Комитетом в 2014 году, а также анализы и рекомендаций «Трансграничной группы» и рабочей группы СЕ в 2014 и 2017 годах.

Вопросы, касающиеся территориальной юрисдикции и связанные с ЭД вызвали озабоченность, так как конкретная информация, необходимая для расследования киберпреступлений, может храниться в разных юрисдикциях. Для этого необходимо принять соответствующие меры в целях реализации раскрытия такой информации действенным методом посредством уголовного расследования и дальнейшего судебного процесса.

В целом, авторы полагали, что положения Протокола № 2 будут иметь большую ценность как с практической, так и с политической точки зрения. Это международное соглашение значительно улучшит и укрепит сотрудничество между странами-участницами Конвенции СЕ, а также облегчит обмен ЭД в целях уголовного расследования киберпреступлений и дальнейших судебных процессов.

Протокол № 2, как и Конвенция СЕ, направлены на максимизирование навыков у компетентных органов для того, чтобы оказать надлежавшее противодействие киберпреступлениям в соответствии с соблюдением основных прав и свобод человека. Более того, вышеназванный документ направлен на обеспечение безопасности сети «Интернет», который в свою очередь образован на свободном потоке данных.

Таким образом, Протокол № 2 направлен на перманентную реализацию кооперации в части противодействия преступлениям в сфере информационных технологий, а также сбором доказательств органами уголовного преследования в электронной форме для дальнейшего расследования или судебного разбирательства с использованием, например, обмена информацией.

Резюмируя вышеприведенное, можно сделать вывод о том, что нынешняя международная кооперация по противодействию компьютерных преступлений имеет следующие отличительные характеристики:

– дробление кооперации под эгидой международных организаций регионального характера, а также интеграционных объединений, которые создают свои инструменты взаимодействия;

– существование пробела в понятийно-категориальном аппарате в части дефиниций основных используемых категорий;

– эволюция юридической базы сильно отстает от развития ИКТ.

Исходя из анализа вышеперечисленных международных соглашений можно сделать вывод о том, что международное регулирование киберпреступлений является региональным. Одна из причин кроется в открытом доступе к компьютерным данным государств. В основном дружественные государства идут на такой шаг сотрудничества. Однако практика показывает, что не все страны готовы поделиться информацией друг с другом и ссылаются на общие принципы международного права о невмешательстве в дела, входящие во внутреннюю компетенцию государств.

Анализ международных соглашения в части противодействия киберпреступлениям выявил следующие методы международного сотрудничества:

осуществление уголовного преследования по запросам иностранных государств;

1) запрос об оказании взаимной помощи;
2) выдача преступника;

3) передача лиц для отбывания наказания в государствах гражданства.

Важно отметить, что взаимная помощь (например, сбор доказательств) может быть осуществлена в отсутствии договоров и соглашений. Например, предоставление взаимной правовой помощи одним государством (Бразилия, Япония) может быть реализовано путем соблюдения принципа взаимности, когда запрашивающее государство гарантирует его (т. е. если аналогичный запрос запрашиваемого государства будет удовлетворен запрашивающим государством в будущем.). Также наличие договора о выдаче не гарантирует, что лицо будет выдано запрашивающей стране. Это наблюдалось в случае с Лори Лав, британским хакером, в выдаче которого США было отказано, несмотря на существование подписанного в 2003 году договора об экстрадиции между Великобританией и США[177].

Создание межгосударственных учреждений, которые могут содействовать обмену информацией, также является одним из способов противодействия киберпреступлениям. Например, исходя из анализа специальных подразделений в рамках Совета Европы можно сделать вывод о том, что такие межгосударственные структуры, как ЕКПП, Комитет и Офис по борьбе с киберпреступностью являются эффективным и важным инструментом в части осуществления толкования и реализации положений Конвенции СЕ, сотрудничеству в области обмена цифровыми доказательствами между национальными правоохранительными органами государств, а также механизмом по урегулированию споров путем согласительных процедур. Достаточно известным на сегодняшний день осуществляющим широкий круг функций в области международного правоохранительного сотрудничества является Агентство Европейского союза по сотрудничеству в правоохранительной сфере. Европол является региональным полицейским агентством, который осуществляет координацию работы правоохранительных органов государств в рамках ЕС, вправе ставить перед ними вопросы о

[177] URL: http://s.telegraph.co.uk/graphics/projects/hacker-lauri-love-extradition/index.html/ (дата обращения: 18.07.2024). – Текст: электронный.

создании совместных следственных групп, участвовать в совместных расследованиях. В рамках АС действует Механизм Африканского союза по полицейскому сотрудничеству (АФРИПОЛ), наделенный полномочиями в части обмена информацией или разведывательными данными в целях предотвращения транснациональных организованных преступлений, террористических актов, киберпреступлений и борьбы с ними. В рамках СНГ существует многостороннее соглашение в части противодействия преступлениям в сфере информационных технологий. Кроме того, в рамках данной международной организации функционирует Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств – участников СНГ.

Таким образом, формирование и деятельность региональных международных организаций и специализированных учреждений по сотрудничеству между правоохранительными органами ныне представляет собой доминирующую тенденцию современного развития институтов международного полицейского сотрудничества. Установлено, что на сегодняшний день у ЕАЭС отсутствует многостороннее соглашение в части противодействия киберпреступлениям. Сотрудничество через двусторонние международные договоры между государствами-участниками не работает, так как киберпреступления нарушают правопорядок более двух государств. В целях преодоления данной проблемы видится необходимым принятия договора под эгидой ЕАЭС, который сможет обеспечить безопасность информационного пространства путем обмена информацией, взаимной помощью в части расследования киберпреступлений, а также запросах о выдаче преступников. Вышеперечисленные механизмы взаимодействия должны обеспечить эффективность в части сотрудничества между странами-участниками ЕАЭС, а помощь их в реализации должен оказать специальный международный правоохранительный орган. Региональный уровень сотрудничества отличает более скоординированный и углубленный характер.

В связи с этим, целесообразным является учреждение регионального международного правоохранительного органа в рамках ЕАЭС.

Что касается глобального взаимодействия, то в рамках ООН идет субстантивная работа над будущим соглашением универсального характера, где будут отображены меры в части борьбы против преступлений и иных противозаконных действий в киберпространстве, а также выдача, взаимная правовая помощь, кооперация между компетентными органами и меры по возвращению активов. В настоящее время резолюцией ГА ООН 79/243 от 24 декабря 2024 года принята Конвенция ООН против киберпреступности.

Исходя из вышеизложенного, ни международные акты обязательного характера, ни международные акты рекомендательного характера, по сути, не играют особую роль в части противодействия преступлениям в сфере ИКТ. Вышеприведенные международные акты охватывают недостаточный на сегодняшний день объем киберпреступлений. Так, например, за пределами международных соглашений оказался кибербуллинг. Кроме того, нельзя не отметить, что традиционные методы международной кооперации, включая запросы, взаимопомощь и т. д., использовавшиеся в прошлом столетии и ранее, являются неактуальными в эпоху, когда преступления могут совершаться из любой точки мира со скоростью света[178]. Необходим универсальный механизм сотрудничества через всеобъемлющею конвенцию ООН. По мнению А.А. Данельяна, на сегодняшний день универсальное международное регулирование информационного пространства отсутствует[179]. Кроме того, у ряда стран отсутствует интерес в части образования актуального метода кооперации. На сегодняшний день усилия стран направлены на разработку вопросов в части прав человека, целостности информации и др. К сожалению, современное международное право не предлагает актуальных методов как для универсального регулирования киберпространства, так и в части борьбы с

[178] Smith R.G., Grabosky P., Urbas G. 2004. *Cyber Criminals on Trial.* Cambridge: Cambridge University Press. 263 p.

[179] Данельян А.А. Киберпространство и международное право // Электронное сетевое издание «Международный правовой курьер». 2019. № 4-5. С. 5–11.

киберпреступлениями. Пока относительно качественное противодействие использованию ИКТ в преступных целях предусмотрено в ряде национальных законодательств[180]. Международные соглашения в части противодействия киберпреступлениям носят фрагментарный характер и нуждаются в совершенствовании как на универсальном, так и на региональном уровне. Тем не менее, источниковая база отличается преобладающей ролью норм мягкого права. Это обуславливается тем, что акты мягкого права, как правило, образуют фундамент в части выработки соглашений обязательного характера.

§2. Практика международного расследования, реализация противодействия и гармонизация национального законодательства государств

В международном праве киберпреступления относят к преступлениям международного характера. По мнению А. Г. Волеводза преступления международного характера – это деяния, предусмотренные международными соглашениями, не относящиеся к международным преступлениям, но посягающие на нормальные стабильные отношения между государствами, наносящие ущерб мирной кооперации в различных сферах отношений, а также организациям и гражданам[181].

А. В. Наумов под преступлениями международного характера понимает конвенционные преступления. Конвенционные преступления – это преступления, предусмотренные международными соглашениями, не относящиеся к преступлениям против человечества, мира и безопасности, но посягающие на стабильные, позитивные отношения между странами, наносящие ущерб мирной кооперации в разных сферах отношений

[180] Aho B., Duffield R. Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China // J. Econ. Soc. 2020. No. 49. P. 187–221.
[181] Волеводз А.Г. К вопросу о сущности и содержании международного сотрудничества в борьбе с преступностью / А.Г. Волеводз // Международное уголовное право и международная юстиция. – 2007. – No 1. – С. 11-20.

(экономической, социальной, культурной, имущественной и т.п.), а также организациям и гражданам, наказуемые либо согласно нормам, установленным в международных соглашениях, либо согласно нормам внутригосударственного уголовного права в соответствии с этими соглашениями[182].

По мнению А.Н. Вылегжанина преступления международного характера представляют собой общеуголовные преступления, отягощенные «иностранным элементом» и, как следствие, затрагивающие интересы двух или более государств[183].

И.И. Лукашук считает, что конвенционные преступления, т.е. предусмотренные конвенциями, обязывающими участвующие государства ввести соответствующие нормы в свое уголовное право в целях обеспечения юрисдикции, включают такие деяния, как терроризм, захват заложников, торговля рабами и обращение в рабство, торговля людьми и эксплуатация проституции третьими лицами, подделка денежных знаков, незаконная торговля наркотиками, незаконные ввоз, вывоз и передача права собственности на культурные ценности и др.[184].

М.Ч. Бассиуни отмечает, что преступления международного характера содержат «иностранный элемент», т. е. угрожают порядкам двух или более государств. Борьба с ними ведется исключительно в рамках внутреннего порядка — государственными правоохранительными органами, действующими на основании материальных и процессуальных норм внутреннего уголовного права (содержание которых может определяться с учетом международных обязательств)[185].

Таким образом, для признания киберпреступления преступлением международного характера осложнение «иностранным элементом» должно

---

[182] 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.: Издательство Юрайт, 2014. С. 277–278.

[183] Международное право: учебник/ отв. ред. А. Н. Вылегжанин. – М.: Высшее образование, Юрайт-Издат, 2009. С. 787.

[184] Лукашук И. И. Международное право. Особенная часть. М ., 1998 . С. 242.

[185] Bassiouni M. C. The Penal Characteristics of Conventional International Criminal Law. P. 28–29.

быть выражено в форме негативных последствий правопорядкам двух или более государств.

Исходя из вышеизложенного, в международном праве киберпреступление является преступлением международного характера, которое посягает как на внутригосударственный, так и на международный правопорядок. Это противоправное деяние, которое не ограничено территориальными границами одного государства, что говорит о его трансграничном характере. Например, распространение вредоносных компьютерных программ (вирусы) преступниками могут быть совершены по всему миру за кротчайший промежуток времени.

Так, в деле США против Карима Баратова, обвиняемый взломал аккаунты пользователей Yahoo и украл их личные данные, включая адреса электронной почты и номера телефонов. Хакер был арестован в Канаде 14 марта 2017 года. Затем киберпреступника экстрадировали в США. Федеральный суд Северного округа Калифорнии в Сан-Франциско приговорил уроженца Казахстана 23-летнего Карима Баратова к 5 годам лишения свободы и штрафу в четверть миллиона долларов за взлом почтовых аккаунтов более чем 11 тысяч потерпевших[186].

Таким образом, киберпреступление как преступление международного характера не связано с какими-либо территориальными ограничениями по субъектному составу и способам совершения, поскольку информационное пространство не имеет политических, экономических и социальных границ[187], его последствия выходят за пределы правопорядка отдельного государства в силу степени общественной опасности. В этом смысле киберпреступление как противоправное уголовно наказуемое деяние, ответственность за которое предусмотрено в законодательстве государства, может быть квалифицировано в качестве преступления международного характера.

---

[186] United States District Court for the Northern District of California. Case 3:17-cr-00103-VC. February 28, 2017.
[187] P.S. Breivik «Education for the information age», D.W. Farmer and T.F. Mech, eds, New Directions for Higher.

Нередко в информационном пространстве нарушаются права и свободы граждан. Приведем несколько решений из практики ЕСПЧ.

Так, в деле «Роман Захаров против Российской Федерации», заявитель подал жалобу в Европейский суд по правам человека (далее – ЕСПЧ) ссылаясь на статью 34 Европейской Конвенции о защите прав человека и основных свобод (далее – Европейская Конвенция)[188].

Г-н Захаров утверждал, что система тайного перехвата мобильной телефонной связи в Российской Федерации нарушает его право на неприкосновенность частной жизнь и переписки, и что у него не было никакого эффективного средства правовой защиты.

ЕСПЧ постановил, что имело место нарушения статьи 8 Европейской Конвенции и посчитал разумным присудить сумму в 40 000 евро заявителю.

В своем единогласном решении ЕСПЧ выявил пробелы в национальном праве Российской Федерации, которое регулирует мониторинг мобильной связи. В целом, детальность и строгость анализа ЕСПЧ свидетельствуют о том, что ЕСПЧ будет в дальнейшем серьезно изучать судебную практику в части прослушивания телефонных разговоров и законодательство европейских государств, когда на его рассмотрение будут поступать аналогичные дела.

Так, в деле «Копланд против Соединённого Королевства» (Copland v. United Kingdom)[189] заявительница жаловалась на контроль за ее личной перепиской по электронной почте и прослушивание телефонных звонков, ссылаясь на ст. 8 и 13 Конвенции о защите прав человека и основных свобод. Европейский Суд по правам человека постановил, что данные, относящиеся к использованию телефона и электронной почты, подпадают под сферу действия ст. 8 Конвенции о защите прав человека и основных свобод. Таким образом, Европейский Суд признал нарушение требований ст. 8 Конвенции о защите прав человека и основных свобод.

---

[188] Постановление Европейского Суда по правам человека от 4 декабря 2015 г. Дело «Роман Захаров (Roman Zakharov) против Российской Федерации» (Жалоба № 47143/06) (Большая Палата Европейского Суда).

[189] Постановление Европейского Суда по правам человека от 3 апреля 2007 г. Дело «Копланд против Соединенного Королевства» [Copland v. United Kingdom] (жалоба № 62617/00). Доступ из СПС «ГАРАНТ».

В деле «Визер и компания «Бикос бетейлигунген ГмбХ» против Австрии[190] (Wieser and Bicos Beteiligungen GMBH v. Austria) не были соблюдены процессуальные гарантии при обыске и изъятии электронных данных из компьютерной системы адвоката. Европейский Суд по правам человека постановил, что данные, хранящиеся на компьютерных серверах, также подпадают под ст. 8 Конвенции о защите прав человека и основных свобод. В порядке применения ст. 41 Конвенции о защите прав человека и основных свобод Европейский Суд присудил выплатить заявителю 2500 евро.

Факт наличия нарушения зависит от контекста, в котором данные были получены, метода их сбора, обработки и использования, а также результатов, которые могут быть при этом получены. Так, статья 16 (1) Договора о функционировании Европейского Союза предусматривает право на защиту персональных данных в качестве одного из основных прав человека[191].

Таким образом, обширная судебная практика Европейского Суда по правам человека, а также ряд региональных международных соглашений устанавливают гарантии и право на защиту от таких видов киберпреступлений, как несанкционированного доступа к персональным данным, а также незаконный перехват данных. Кроме того, в юридической литературе подчеркивается, что ЕСПЧ чаще других международных судов по правам человека вовлекается в рассмотрение дел, связанных с ИКТ и затрагивающих вопросы юрисдикции[192].

Отсутствие соответствующих правовых норм для обеспечения международной информационной безопасности является проблемой, характерной для некоторых стран. Одной из проблем, которая затрудняет борьбу с киберпреступлениями, является отсутствие консолидированного договора в конкретном регионе. Например, правовые системы в разных

---

[190] Постановление Европейского Суда по правам человека от 16 октября 2007 г. Дело «Визер и компания «Бикос Бетейлигунген ГМБХ» против Австрии» [Wieser and Bicos Beteiligungen GMBH v. Austria] (жалоба № 74336/01). Доступ из СПС «ГАРАНТ».

[191] Договор о функционировании Европейского Союза. Доступ из СПС «ГАРАНТ».

[192] Липкина Н. Н. Принципы установления экстратерриториальной юрисдикции государств в киберпространстве в контексте правовых позиций Европейского Суда по Правам Человека // Правовая политика и правовая жизнь. № 2. 2021. С. 153–160.

странах Европы различаются, что делает эффективное трансграничное расследование и уголовное преследование киберпреступлений чрезвычайно сложными[193].

Основные различия касаются того, какое деяние будет квалифицироваться как киберпреступление в качестве уголовного преступления и как могут проводиться расследования. После призывов бороться с этой проблемой в некоторых регионах усилия были направлены на унификацию законов о киберпреступлениях. В 2014 году в Восточной Африке была принята Конвенция Африканского союза о кибербезопасности и защите персональных данных[194]; однако проблема остается нерешенной. Ученые придерживаются мнения, что сущность киберпреступлений требует универсальных механизмов для решения проблем в части юрисдикции, а также вопросов экстрадиции[195].

Механизмы международного права работают медленно, и это может стать серьезной проблемой, когда речь идет о таком постоянно меняющемся явлении как киберпреступление[196]. Право международных договоров постулирует о том, чтобы государства ратифицировали договоры с целью их дальнейшего вступления в силу и реализации их, а также имплементировали в свое национальное законодательство. Этап реализации имеет решающее значение для создания общего подхода к проблеме в части регулирования киберпреступлений[197].

В целом, многие государства склонны считать уголовно-процессуальную правовую базу достаточной, однако в регионах проблема киберпреступности регулируется по-разному[198]. В то время как многие страны

---

[193] Gibson &Miralis. 2021. *TheFive Key Challenges of Law Enforcements in Fighting Cybercrime.* NGM.
[194] STC-CICTC. *A Global Approach to Cybersecurity and Cybercrime in Africa.* Recommendations of the First Ordinary Session of the STC-CICT-1.
[195] Ajayi, E.F.G (2016). Challenges to Enforcement of Cyber-crimes Laws and Policy. *Journal of Internet and Information Systems* Vol. 6(1), p. 1-12
[196] Csonka, Peter. 2004. The Council of Europe Convention on cyber-crime: A response to the challenge of the new age? In Cybercrime: Conferenza internazionale. La Convenzione del Consiglio d'Europa sulla Criminalità Informatico, ed. Giovanni Ilarda and Gianfranco Marullo, 3- 29. Milano: Giuffrè. P. 10-14.
[197] Miquelon-Weismann, Miriam F. 2005. The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process? John Marshall Journal of Computer & Information Law, 23, no. 2: 329-61. P. 353.
[198] Brian B. Kelly, Investing In a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can And Should Influence Cybersecurity Reform 92 BOSTON UNIVERSITY LAW REVIEW, 1671-1673.

Европы склонны считать свое законодательство достаточным, обратная картина наблюдается в Африке, Северной и Южной Америке, Азии и Океании, где менее развитые государства считают нормативную базу в части регулирования киберпреступлений достаточной лишь частично или вовсе недостаточной[199].

Трансграничный характер, а также совершение киберпреступлений в информационном пространстве являются основными трудностями, с которыми сталкиваются правоохранительные органы. Традиционные предположения о том, что за преступником следят в процессе подготовки, совершения правонарушения уже не соответствуют действительности[200].

Проблемы в части расследования киберпреступлений возникают из-за криминальных нововведений преступников, трудностей с доступом к электронным доказательствам и нехватки внутренних ресурсов, мощностей и материально-технических ограничений. Подозреваемые часто используют технологии анонимизации и обфускации (процесс изменения кода программы, в результате которого он приобретает вид, трудный для понимания – при этом программа сохраняет свои функции), а новая техника быстро становится доступной для широкой аудитории через криминальные онлайн-рынки[201].

Кроме того, существуют определенные сложности в части обнаружения запрашиваемых данных в облачном хранилище[202]. Во-первых, облачное хранилище – это модель облачных вычислений, которая дает возможность хранить данные и файлы в сети «Интернет», пользуясь услугами поставщика облачных услуг. Кроме того, данные в облачном хранилище могут быть зеркально отражены по соображениям безопасности и доступности, и поэтому

---

[199] Comprehensive Study on Cybercrime xvii (John Sandage, et al. eds., United Nations Office on Drugs and Crime 2013).

[200] Susan W. Brenner, The Privacy Privilege: Law Enforcement, Technology and the Constitution, 7 JOURNAL OF TECHNOLOGY LAW & POLICY, 124-131.

[201] Comprehensive Study on Cybercrime xxi-xxii. 2013.

[202] It has also been argued in this regard that there is great need for the harmonization of laws in the area of cybercrime in the global space and particularly to include developing and underdeveloped countries in the realities presently existing in the cyber space. See Stein, J. (2012). *Recommendations for Potential New Global Legal Mechanisms Against Global Cyber Attacks and Other Global Cybercrimes*. A Paper for the East West Institute (EWI) Cybercrime Legal Working Group 2012.

их можно найти в нескольких местах в пределах одной страны или в нескольких странах. Следовательно, даже поставщик облачных услуг может не знать точно, где находятся запрашиваемые данные[203].

С процессуальной точки зрения основной проблемой для национального правоприменения является примирение с историческим фактом, что правоохранительные органы организационно локализованы в границах юрисдикции (неотъемлемо связанной с государственным суверенитетом), тогда как международная информационная безопасность и киберпреступления лишены четкой юрисдикции[204].

Вещественные доказательства – это средства, с помощью которых устанавливаются факты, относящиеся к виновности или невиновности лица. Электронные доказательства (далее – ЭД) — это все те материалы, которые существуют в электронной или цифровой форме. Вещественные доказательства редко используются в ходе судебного преследования за киберпреступления. В большинстве стран задача анализа электронных доказательств лежит на правоохранительных органах. Дополнительной сложностью является в незнании использования технологий правоохранительными органами. На данный момент киберпреступники лучше используют технологические возможности, которыми они владеют. Наличие соответствующего органа, обладающего специальными знаниями и опытом в рамках этого, является важнейшим элементом эффективного регулирования киберпространства[205].

Работникам правоохранительной системы (прокуроры, следователи, судьи) необходимо иметь определенные знания в части ЭД и компьютерной системы в целом. Многие развивающиеся страны не имеют достаточных ресурсов для обеспечения сотрудников достаточными компьютерными навыками. То же самое касается и судей, рассматривающих

---

[203] INTERPOL European Working Party on Information Technology Crime (EWPITC) – Project on cloud computing, 2011.
[204] WALL, Cybercrime: The Transformation of Crime in the Information Age 160. 2007.
[205] WALL, Cybercrime: The Transformation of Crime in the Information Age 160. 2007.

узкоспециализированные дела о киберпреступлениях. Обучение судей в части ЭД, а также фундаментальным знаниям в области компьютерной информации является необходимым.

Ряд стран не проводят правовые разграничения в части доказательств и ЭД. Кроме того, ряд стран полагают, что данный подход позволит обеспечить надлежащее использование ЭД. Ряд государств, находящихся за пределами европейского региона, не признают ЭД, и как следствие, расследование действий с использованием ИКТ в противоправных целях представляется невозможным.

Разница в национальных правовых системах в части квалификации киберпреступлений, установления ответственности за их совершение приводит к трудностям в оказании противодействия этому противозаконному деянию. Более того, определение преступного поведения во внутригосударственных правовых системах могут не совпадать. Страна, в которой находится правонарушитель, может не считать такое действие правонарушением[206].

Гармонизация внутригосударственных правовых систем является позитивным шагом в целях борьбы против киберпреступлений. Сближение уголовного и уголовно - процессуального права государств в целях решения технических и юридических трудностей, связанных с нынешним международным сотрудничеством, является необходимым[207].

В международных договорах, посвящённых киберпреступлениям, прописано, что основная роль в части реализации уголовного расследования киберпреступлений относится к внутригосударственному праву[208]. С одной стороны, в нем должна быть прописана подробная инструкция обеспечения их

[206] Flanagan, anne. 2005. The law and computer crime: Reading the Script of Reform. International Journal of Law and Information Technology, 13, no. 1: 98-117.
[207] Vermeulen, Gert. 2002. Where do we currently stand with harmonisation in Europe? In Harmonisation and harmonising measures in criminal law, edited by André H. Klip and Harmen G. van der Wilt, 65-76. Amsterdam: Royal Netherlands Academy of Science.
[208] Волеводз А.Г. К вопросу о сущности и содержании международного сотрудничества в борьбе с преступностью / А.Г. Волеводз // Международное уголовное право и международная юстиция. – 2007. – No 1. – С. 253.

предписаний, а с другой отображаться преобладающие нормы международных актов. Нормами внутригосударственного права должны регулироваться вопросы, содержащиеся в международных договорах и направленные на противодействие киберпреступлениям будут отображены в общем виде, однако для решения казусов уголовного судопроизводства необходимо проработанное юридическое обеспечение на внутригосударственном уровне.

Проблема является дискуссионной, поскольку остаются нерешенные вопросы. Т.Л. Тропина считает, что существующие международные механизмы в части обеспечения информационной безопасности являются фрагментарными. Не способность в сближении национальных правовых систем стран характеризует также мозаичность и конкуренция между собой[209].

Кроме того, не установлены международно-правовые инструменты в части обеспечения суверенного права стран на регулирование киберпространства, а также на внутригосударственном уровне сети «Интернет». Для решения проблем в области информационного пространства требуются усилия как государственных структур, так и частных акторов[210]. В данный момент большое количество стран старается моментальным образом приспособить регулирование киберпространства к актуальным реалиям[211].

Международно-правовое регулирование в части противодействия киберпреступлениям, на сегодняшний день, носит фрагментарный характер. Более того, необходимость в улучшении регулирования безопасности сетей как на универсальном, так и на региональном уровне является необходимым. Причины, по которым странам не удается достичь консенсуса, в данном вопросе являются допустимая степень ограничения суверенитета в части регулирования информационного пространства, а также несогласованность

---

[209] Тропина Т.Л. 2012. Борьба с киберпреступностью: возможна ли разработка универсального механизма – *Международное правосудие.* No 3. С. 86–95.

[210] Huey L., Nhan J., Broll R. 2013. ‘Uppity Civilians’ and ‘Cyber-Vigilantes’: The role of the general public in policing cyber-crime. – *Criminology and Criminal Justice.* Vol. 13. No. 1. P. 81–97. DOI: 10.1177/1748895812448086 (дата обращения: 18.07.2024). – Текст: электронный.

[211] Пункт 17 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента РФ от 9 мая 2017 г. No 203. Доступ: http://www.kremlin.ru/acts/bank/41919/page/3 (дата обращения: 18.07.2024). – Текст: электронный.

стран в части надлежащего сотрудничества в целях противодействия компьютерным преступлениям.

Резюмируя вышесказанное, можно сделать вывод о том, что меры в части борьбы с киберпреступлениями, принимаемые на международном уровне, должны быть синхронно установлены и на внутригосударственном уровне. Совместные усилия как на международном, так и на внутригосударственном уровне должны связывать и дополнять друг друга в целях надлежащего обеспечения координации, а также эффективного сотрудничества в части борьбы против преступлений в сфере информационных технологий и сближения внутригосударственных законодательств.

§3. Искусственный интеллект и кибербезопасность. Вопросы суверенитета, юрисдикции, экстрадиции, ответственности государств

В настоящее время происходит формирование системы международной информационной безопасности[212].

В соответствии с Соглашением между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, международная информационная безопасность трактуется, как состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве[213].

Российская Федерация на национальном уровне выработала концепцию, которая регламентирует вопросы информационной безопасности. Владимир Владимирович Путин подписал Указ от 5 декабря 2016 г. № 646 «Об

[212] Талимончик В.П. Международно-правовое регулирование отношений в сфере информации. Автореф. Дис. на соискание уч. степени д.ю.н. Санкт-Петербург, 2013.- 39.

[213] Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности.

утверждении Доктрины информационной безопасности Российской Федерации»[214].

В Указе Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» дается определение международной информационной безопасности – такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности[215].

Международно-правовое регулирование сети «Интернет» видится целесообразным в связи с тем, что ряд государств могут воспринять очередную кибератаку, например на свою критическую инфраструктуру и оценить этот акт, как серьезную угрозу национальной безопасности. Следствием этого может стать информационная война, в который будут втянуты наиболее развитые с технической точки зрения государства.

В ряде западных стран говорят больше о кибербезопасности. Вопрос кибербезопасности является глобальным и актуальным в двадцать первом века, требующий современного подхода к ее решению. Под кибербезопасностью подразумевается прежде всего безопасность сетей.

По словам президента Люксембургского форума по предотвращению ядерной катастрофы – Вячеслава Кантора: «киберугрозы уже сейчас непосредственно касаются государственной инфраструктуры ядерных государств и теоретически, у преступников может появиться доступ к ядерному оружию»[216]. Не сложно догадаться, что этот глобальный вопрос затронет безопасность всего населения и мирового сообществ.

---

[214] Доктрина информационной безопасности Российской Федерации № 646 от 5 декабря 2016 года.
[215] Указ Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности».
[216] URL: http://www.luxembourgforum.org/events/zasedanie-nablyudatelnogo-soveta-lyuksemburgskogo-foruma-zheneva-4-5-dekabrya-2019-goda/.

Зарубежные исследователи в данной области разработали разные подходы в части понимания кибербезопасности. Одни понимают под кибербезопасностью специальные мероприятия, направленные на пресечение киберпреступлений[217]. Другие авторы дают более подробное определение кибербезопасности – это междисциплинарный аспект информационно-коммуникационных технологий, который касается правовых, нормативных, а также технологических и нетехнологичных механизмов, созданных с целью защиты компьютеров, компьютерных систем, компьютерных сетей и цифровых технологий, включая информацию, хранящуюся или передаваемую ими от всех форм угроз[218]. В первую очередь, кибербезопасность призвана обеспечить защиту киберпространства, а также защиту информационных и коммуникационных технологий от всех форм киберугроз[219]. В кибербезопасность также входит разработка криптографии (метод защиты информации путем использования закодированных алгоритмов, электронных цифровых подписей). [220] Кибербезопасностью также может быть определена, как «совокупность инструментов, руководящих принципов, гарантий и технологий, которые могут быть использованы для защиты цифрового пространства, коммерческих организаций, государственных структур, а также личной информации пользователя»[221].

С технологической точки зрения кибербезопасность будет относиться к техническим мерам, разработанным для внедрения защищенной операционной системы, или технологиям, разработанным для защиты компьютерных систем и информации, хранящейся в таких компьютерных системах. Также сюда можно включить разработку технологий и технических

---

[217] Herjavec, R. (2019, July 17). Cybersecurity CEO: The History of Cybercrime, from 1834 To Present. *Cybercrime Magazine*. URL: https://cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime- from-1834-to-present/.

[218] Orji, U.J. (2012). *Cybersecurity Law and Regulation*. 1 Wolf Legal Publishers.

[219] Dunn, M. (2005). *A Comparative Analysis of Cybersecurity Initiatives Worldwide*. (A paper presented at the World Summit on Information Society (WSIS) Thematic Meeting on Cybersecurity, ITU: Geneva). p. 4

[220] Cryptography is the study and practice of securing information and communications to circumvent unauthorized access and safeguard the integrity of information. *Lawyard Journal* (2020). p.25

[221] ITU High Level Experts Group (HLEG). (2008). P. 27. URL: http://www.itu.int/cybersecurity/gca/.

мер для обеспечения безопасности компьютерного программного обеспечения[222].

Для физического компьютерного пользователя кибербезопасность будет означать меры личного характера, принимаемые для защиты персонального компьютера, а также безопасность и конфиденциальность данных, хранящихся на нем или в электронном устройстве, например флеш-накопитель[223]. Меры, принимаемые в этой связи для защиты персонального компьютера, также будут включать использование паролей для предотвращения несанкционированного доступа к персональным компьютерам, использование надежного и обновленного антивирусного программного обеспечения для предотвращения проникновения вредоносных программ и бережное обращение с личными данными, например, неразглашение личной информации подозрительным веб-сайтам или когда подлинность такого запроса данных вызывает сомнения[224].

В международном праве существует ряд сложных вопросов в части согласованного противодействия киберпреступлениям, требующих разъяснения. Например, отсутствие консенсуса в части юрисдикции и суверенитета делает затруднительными оперативное пересечение границ для реагирования на киберпреступления. Государство может считать свой информационный суверенитет нарушенным, если другое государство осуществит вмешательство в него без согласованного на то уведомления.

Кибердипломатия является одним из способов содействия защите интересов в области кибербезопасности. За последнее десятилетие десятки министерств иностранных дел создали специальные внутренние подразделения, занимающиеся вопросами киберпространства, и назначали так называемых «кибердипломатов», чтобы реагировать на растущую

---

[222] Orji, U.J. (2012). *Cybersecurity Law and Regulation*. Wolf Legal Publishers. P. 157.

[223] This definition will also extend to all appropriate safeguards applied to a computer user to protect his or her computer and personal data from any form of cyber threats such as virus attacks, identity theft, unauthorized access and interception, theft, destruction or alteration. See; Orji, U.J. (2012). *Cybersecurity Law and Regulation*. 1 Wolf Legal Publishers.

[224] Orji, U.J. (2012). *Cybersecurity Law and Regulation*. 1 Wolf Legal Publishers.

политизацию киберпространства[225]. Дипломаты очень хорошо понимают работу в части взаимоотношений и сотрудничества своей страны с другими государствами, что очень важно для дальнейшего развития обеспечения кибербезопасности. В мире, в котором все больше стран приобретают наступательный кибернетический потенциал, кибердипломатия необходима для предотвращения эскалации и кибератак путем поддержания постоянного диалога и обеспечения того, чтобы каналы коммуникации оставались открытыми даже во времена кризиса[226]. Кибердипломатия также необходима для разработки правил ответственного поведения государств в киберпространстве и устранения наиболее острых разногласий между заинтересованными сторонами в этой области. Это может быть реализовано благодаря такой международной организацией универсального характера, как ООН, а также на региональном уровне, например ОБСЕ.

Поскольку коллизии в части правового регулирования цифрового пространства неизбежно будут возникать, очень важным является создание во всех странах мира специальных внутренних подразделений на уровне министерств иностранных дел, занимающихся вопросами киберпространства.

Обеспечение международной информационной безопасности, а также более эффективное противодействие киберпреступлениям возможно благодаря сотрудничеству таких международных институтов, как Международное многостороннее партнерство против киберугроз (далее – ММППК) и специализированного учреждения ООН по ИКТ – Международного союза электросвязи (далее – МСЭ)[227]. ММППК является первым в мире всесторонним альянсом против киберугроз, объединяющим правительства, академические организации и ведущих экспертов отрасли для повышения эффективности обеспечения международной информационной

---

[225] Barrinha, A. (2020). *TheEmergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyber Space.*Council on Foreign Relations. URL: https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post- liberal-cyberspace/.

[226] Downing, R. W. (2005). Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime. P. 43 *Columbia Journal of Transnational Law.*

[227] The International Multilateral Partnership against Cyber Threats (IMPACT) URL: http://www.impact-alliance.org/.

безопасности. ММППК обеспечивает государствам, которые являются его членами, доступ к специальным знаниям, средствам и ресурсам для эффективного устранения киберугроз, а также оказывает учреждениям ООН помощь в защите их инфраструктур ИКТ. ММППК официально стал ключевым партнером МСЭ в соответствии с Соглашением о сотрудничестве, подписанным на Всемирном саммите по информационному обществу в 2011 году.

МСЭ является главным всемирным форумом, в рамках которого стороны могут добиваться консенсуса по широкому кругу вопросов, влияющих на будущее направление развития отрасли ИКТ. МСЭ инициировал Глобальную программу кибербезопасности, которая представляет для МСЭ основу международного сотрудничества, цель которого состоит в том, чтобы предложить стратегии для поиска решений в области укрепления доверия и безопасности в условиях информационного общества[228]. В Глобальной программе кибербезопасности МСЭ определены пять стратегических принципов: правовые меры, технические меры, организационные меры, создание потенциала и международное сотрудничество. МСЭ также выдвигает определенные решения в целях реализации программы

Таким образом, укрепление сотрудничества вышеназванных институтов повысит способность государств-членов обмениваться информацией, ресурсами и передовой практикой в области кибербезопасности. Это в немалой степени поможет в обеспечении своевременного предупреждения и реагирования на киберпреступления.

По мнению В.Д. Зорькина, наступила пора активного использования искусственного интеллекта (далее – ИИ) для управления в экономике, обществе и государстве[229]. Появление феномена ИИ стало возможным лишь благодаря исследованиям интеллекта естественного: процессов мышления, механизмов приобретения знания, структуры и сущности сознания.

---

[228] URL: https://ifap.ru/pr/2008/080908aa.pdf/.

[229] Зорькин В.Д. Конституционно-правовое развитие России: монография / В.Д. Зорькин. – 2-е изд., испр. и доп. – М.: Норма, 2019. – 448.

Способно ли мыслить то, что сотворено руками человека? Одним из первых кто задался таким вопросом, был выдающийся английский математик, криптограф - Алан Тьюринг, который во время второй мировой войны разработал ряд методов взлома немецкого шифратора Enigma. Он выдвинул тезис: «Может ли машина мыслить?»[230]. В СССР первым серьезно поднял эту проблему выдающийся академик В. М. Глушков. Он поставил знак равенства между искусственным интеллектом и мышлением человека. Но при этом утверждал, что машинное мышление в состоянии даже превзойти человеческое.[231]

На Дартмутской конференции в 1956 г. Джоном Маккарти был предложен термин «ИИ». Автор термина отмечает следующее: «Проблема состоит в том, что пока мы не можем в целом определить, какие вычислительные процедуры мы хотим называть интеллектуальными. Мы понимаем некоторые механизмы интеллекта и не понимаем остальные. Поэтому под интеллектом в пределах этой науки понимается только вычислительная составляющая, способная достигать целей в мире»[232].

В фундаментальной работе «Искусственный интеллект: современный подход» Стюарт Рассел и Питер Норвиг отмечают четыре главных подхода к созданию интеллектуальных систем, где в рамках искусственного интеллекта разрабатываются системы, которые:

1) действуют подобно людям;
2) думают подобно людям;
3) действуют рационально;
4) думают рационально[233].

Исследователи, изучающие феномен ИИ, выделяют следующие проблемы:

---

[230] A.M. Turing (1950) Computing Machinery and Intelligence. Mind 49: 433–460.
[231] В. М. Глушков. «Мышление и кибернетика». «Известия», №156 (1410), 1963.
[232] A proposal for the Darmouth summer research project on artificial intelligence. J. McCarthy, Dartmouth College M. L. Minsky, Harvard University N. Rochester, I.B.M. Corporation C.E. Shannon, Bell Telephone Laboratories. August 31, 1955. P. 2.
[233] Стюарт Рассел, Питер Норвиг. Искусственный интеллект: современный подход. Издательский дом «Вильямс» 2016. С 79–80.

1) соотношение ментального и методов алгоритмизации;
2) проблема неформализуемости поведения;
3) проблема возможности сильного и слабого искусственного интеллекта;
4) проблема интерпретации компьютерной метафоры сознания;
5) проблемы интеракции машины и человека и этический аспект проблематики ИИ.

В последнее время, на внутригосударственном уровне, активно обсуждается вопрос ИИ на самом высоком уровне. В целях обеспечения ускоренного развития ИИ, проведения научных исследований в области ИИ, повышения доступности информации и вычислительных ресурсов для пользователей, совершенствования системы подготовки кадров в этой области, Президентом Российской Федерации подписан указ от 10.10.2019 № 490 «О развитии искусственного интеллекта В Российской Федерации» (далее — Указ)[234]. В Указе утверждена национальная стратегия по развитию ИИ, в которой определены цели и основные задачи развития ИИ в Российской Федерации, а также меры, направленные на его использование в целях обеспечения национальных интересов и реализации стратегических национальных приоритетов, в том числе в области научно-технологического развития.

Международным и национальным компаниям необходимо своевременно реагировать на возрастающее количество предупреждений систем кибербезопасности. Из-за нехватки квалифицированных кадров в предотвращении киберугроз, компании обращаются к средствам машинного обучения и искусственного интеллекта для автоматизации процессов безопасности. Анализ кибератак необходимо выполнять быстро, сократив до минимума время между распознаванием и реакцией. Система ИИ может быть настроена таким образом, чтобы в будущем быть способной предвидеть

[234] Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации». Доступ «СПС ГАРАНТ».

потенциальную киберугрозу и нанести упреждающий удар, а также выступать в качестве превентивной меры в отношении кибератак. Оперативное реагирование на киберпреступление минимизирует возможный ущерб[235].

Для обеспечения эффективной работы ИИ необходимо обучение на огромном количестве данных. Необходимо располагать искусственной нейронной сетью и моделью глубокого машинного обучения, которые ускорят анализ данных. Только тогда ИИ сможет использовать данные для обучения, адаптации и развития.

Могут потребоваться годы обучения для того, чтобы программа искусственного интеллекта была готова к работе в полевых условиях. Преступники создают новые способы взлома корпоративных систем и это порождает перманентное поступление новых данных о киберпреступниках, которые необходимо регулярно включать в обучение. Модели обучения искусственного интеллекта необходимо будет постоянно обновлять и адаптировать к новым угрозам наряду с разработкой новых стратегий борьбы с ними.

Существующие механизмы противодействия киберпреступлениям применяются не полностью или реализованы лишь частично.

Существует пробел в международном праве в части регулирования систем ИИ в целях обеспечения международной информационной безопасности. Несомненно, существует ряд международных актов, направленных на решение этого вопроса, но они имеют больше факультативный характер. Тем не менее, в эпоху цифровизации и интенсивной интеграции ИИ практически во все сферы жизнедеятельности, (экономическую, социальную, культурную, политическую) необходимо выработать международное соглашение универсального характера, которое будет регулировать развитие систем ИИ в целях защиты прав человека, международного сотрудничества, совместного научно-технологического развития, а также соблюдения мира, безопасности и

---

[235] М. Королов. Как искусственный интеллект может противостоять киберугрозам. «Директор информационной службы». 2017. № 10. С. 13.

стабильности. Юридически обязательный всеобъемлющий документ должен быть направлен на предотвращение и/или смягчение рисков, связанных с применением систем ИИ, которые могут препятствовать реализации прав человека, демократии и соблюдению верховенства закона, при одновременном продвижении социально полезных приложений ИИ.

Несомненно, ИИ принес человечеству огромные преимущества и выгоду за последнее десятилетие, и эта тенденция, вероятно, сохранится в ближайшие годы, поскольку ИИ постепенно становится частью цифровых услуг, которыми мы пользуемся. Многие государства придерживаются политики развития систем и приложений ИИ в целях скорейшего выявления, а также прогнозирования киберпреступлений, для того чтобы обеспечить национальную безопасности.

Появились современные технологии, например использование распознавания лиц в сфере уголовного судопроизводства, использование дронов, беспилотных транспортных средств, которые при неправильной настройке или управлении без надлежащих механизмов надзора могут быть использованы в деструктивных целях.

Кроме того, ИИ при помощи машинного обучения обладает возможностью обнаружить и реагировать на кибератаки, направленные на критически важные секторы инфраструктуры, включая водоснабжение, энергоснабжение и электроснабжение. ИИ также способен правильно управлять решениями в области международной информационной безопасности в целях уменьшения рисков угроз.[236] Тем не менее, остаются нерешенные проблемы, в частности, для малых и средних предприятий, которые в силу нехватки финансовых ресурсов лишены возможности укрепления своей информационной безопасности.

Из-за пандемии COVID-19 большая часть населения мира оказалась в изоляции. Эта ситуация повлекла к тому, что юридические и физические лица

[236] MIT Technology Review, «Transforming the Energy Industry with AI», January 21, 2021. URL: https://www.technologyreview.com/2021/01/21/1016460/transforming-the-energy-industry-with-ai/.

стали более зависимыми от использования систем, технологий и приложений, основанных на ИИ для осуществления своей деятельности, включая удаленную работу, дистанционное обучение, онлайн-платежи или просто наличие доступа к развлекательному контенту.

Благодаря использованию технологий ИИ киберпреступники не только нашли новое средство для использования своей противоправной деятельности, но и, в частности, нашли новые пути осуществления киберпреступлений в отношении юридических компаний, физических лиц, а также правительств. Сами члены организованной преступной группы не обладают достаточными знаниями в области информационных технологий для того, чтобы управлять ИИ в противозаконных целях. В силу этого они вербуют в свои ряды оснащенных знаниями в этой области хакеров в целях осуществления киберпреступлений в отношении ЭВМ, а также для совершения киберпреступлений в режиме 24/7 из любой точки мира[237].

Широкое использование технологий, основанных на системах распознавания лиц, является одним из механизмов противодействия киберпреступлениям в части выявления потенциальных преступников[238].

Существует и обратная сторона медали у ИИ. Распространения дезинформации с помощью технологий ИИ, известных как боты (виртуальный робот или ИИ, который функционирует на основе специальной программы, выполняющий автоматически и/или по заданному расписанию какие-либо действия через интерфейсы, предназначенные для людей). Кроме того, использование ботов может подорвать доверие и поставить под вопрос авторитет правительственных СМИ, а также дестабилизировать демократические и государственные институты.

Скорейшая цифровизация общества, а также хоатичное внедрение практически во все отрасли жизнедеятельности ИИ, может привести к

---

[237] INTSIGHTS, “The Dark Side of Latin America: Cryptocurrency, Cartels, Carding and the Rise of Cybercrime”, p.6. URL: https://wow.intsights.com/rs/071-ZWD-900/images/Dark%20Side%20of%20Latin%20America.pdf/.

[238] Special Report on Facial Recognition of the Center for AI and Digital Policy (CAIDP) that contains a summary of key references on this topic contained in the *2020 Report on Artificial Intelligence and Democratic Values*/ *The AI Social Contract Index 2020* prepared by CAIDP, December 2020. URL: https://caidp.dukakis.org/aisci-2020/.

сокращению умственной работы у молодого поколения в части образованя. По мнению А.Б. Мезяева, использование технологии быстрого поиска существенно сокращает условия для напряженной умственной работы. При этом формируются дополнительные «вредные привычуи», например, не просто использовать данную технологию для поиска истчоников, а для готовых ответов. Такая «вредная привычка» довольно быстро приводит к утрате способности отеделния нужной информации от ненужной, определения степени релеванстности полученной информации в отношении конкретной заданной темы и т.д[239].

Еще одна технология, широко используемая во многих отраслях, — это методика синтеза изображения, основанная на ИИ. Методика синтеза изображения используется для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики.

Противоправное использование методике синтеза изображения является серьезной проблемой, как на внутригосударственном, так и на международном уровне. Имитация голоса при помощи ИИ в противоправных целях также участились в последнее время. В 2019 году преступники использовали ПО для генерации голоса ИИ, чтобы выдать себя за голос генерального директора энергетической компании, находящейся в Великобритании. В итоге злоумышленникам удалось украсть 243 000 долларов США и распределить переводы денежных средств на банковские счета, находящиеся в Мексике и других государств.

Похожий кейс случился в ОАЭ вс 2020 году. Злоумышленники посредством применения систем ИИ имитировали голос директора транснациональной корпорации. В итоге преступники получили доступ к 35 миллионам долларов, которые были депонированы на несколько банковских счетов.

---

[239] Мезяев А.Б. К вопросу о некоторых рисках в процессе трансформации образования в контексте «цифровизации» общества и применения новых технологий // Материалы международной научно-практической конференции, посвященной 30-летию Университета управления «ТИСБИ» и 30-летию программы кафедр ЮНЕСКО/УНИТВИН. Казань, 2022. С. 179-182.

Вышеназванные киберпреступления появились при помощи ИИ. Расследование такого рода киберпреступлений, а также обнаружение доказательств является сложной задачей для правоохранительных органов. Прежде всего, правоохранительные органы разных государств не располагают всеми ресурсами, в частности, подготовленными экспертами, а также отсутствием обеспечения сохранения цифровых доказательств.

Большое количество кибератак осуществляются организованными преступными группами (далее – ОПГ), находящимися в разных государствах, вследствие чего возникает острая необходимость в международной кооперации, например, в сотрудничестве с глобальными поставщиками услуг в целях обеспечения сохранности данных об абонентах и трафике, а также в проведении совместных мероприятий, таких как оперативно-розыскная деятельность (далее – ОРД) компетентным органам разных государств.

ОПГ оперативно внедряют новые технологии в свои методы работы, что приводит не только к постоянным изменениям в криминальном мире, но и создает значительные проблемы для правоохранительных органов и кибербезопасности в целом.

Бизнес-модель «Преступление как услуга» позволяет не подкованным в технологическом плане преступникам приобретать технические инструменты и услуги в цифровом пространстве, которые помогают им расширить свои возможности для кибератак.

Тем самым, увеличивается вероятность того, что преступники будут использовать новые технологии в противоправных целях, а ИИ впоследствии станет движущей силой киберпреступности[240].

В докладе одного из структурных подразделений Европола, а именно, Европейского центра по борьбе с киберпреступностью (далее – ЕЦБК) говорится, что риски, коррелирующие с применением ИИ в противоправных целях, должны быть сокращены для того, чтобы обеспечить информационную

[240] Europol and Eurojust. (July 5, 2019). *Europol and Eurojust*. «Common Challenges in Combating Cybercrime». Accessed on Oct. 14, 2020. URL: https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime.

безопасность. В соответствии с сообщением ЕЦБК, посредством ИИ, киберпреступники увеличивают возможность получения доходов за небольшой промежуток времени, и образовывая современные модели криминального бизнеса, минимизируют возможность быть отслеженными и идентифицированными правоохранительными органами[241].

Кроме того, ЕЦБК рекомендует изучать использование ИИ преступниками с целью прогнозирования возможных противоправных действий, а также для предотвращения, реагирования или смягчения последствий противоправных деяний при помощи ИИ.

ЕЦБК совместно с Центром искусственного интеллекта и робототехники при Межрегиональном научно-исследовательском институте Организации Объединенных Наций по вопросам преступности и правосудия (далее – ЮНИКРИ) опубликовали доклад под названием: «Противоправное использование искусственного интеллекта».

В докладе дается определение системе ИИ. Система ИИ – это программные (и, возможно, также аппаратные) системы, разработанные человеком, которые, преследуя определенную цель, действуют в физическом или цифровом измерении, воспринимая окружающую реальность посредством сбора данных, интерпретируя собранные структурированные или неструктурированные данные, рассуждая на основе знаний или обрабатывая информацию, полученную из этих данных и принятие решения о наилучших действиях, которые следует предпринять для достижения поставленной цели[242]. По мнению П. Н. Бирюкова, систему ИИ можно определить как компьютерную программу с возможностью самообучения, установленную на соответствующем оборудовании[243]. Иными словами, система ИИ – это

---

[241] Europol. (Feb. 28, 2017). *Europol*. «European Union Serious and Organized Crime Threat Assessment (SOCTA)». Accessed on Jul. 20, 2020. URL: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised- crime-threat-assessment-2017.

[242] Trend Micro Research, EUROPOL EC3 and UN Interregional Crime and Justice Research Institute (UNICRI), *Malicious Uses and Abuses of Artificial Intelligence*, 19 November 2020. URL: https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence.

[243] Бирюков П.Н. Искусственный интеллект: вызовы современной юридической науке // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 2 (66). С. 256–260.

свойство искусственных систем выполнять творческие функции, которые традиционно считаются прерогативой человека.

21 апреля 2021 г. Европейская комиссия опубликовала предложение по регулированию систем ИИ и внесение поправок в некоторые акты ЕС[244]. Предложение Европейской комиссии по регулированию также содержит четкие запреты на использование ИИ, противоречащие ценностям ЕС и нарушением основных прав граждан, и учреждает Европейский совет по ИИ в качестве официального органа, который будет контролировать применение и обеспечение соблюдения регулирования систем ИИ в ЕС[245]. Более того, глава Еврокомиссии ЕС по внутреннему рынку Тьерри Бретон заявил, что ЕС в связи с резко возросшим в последнее время объемом кибератак намерен оснаститься «киберщитом». По случаю открывшегося в среду в Лилле международного форума по кибербезопасности Бретон объявил о строительстве, начиная с 2024 года, нескольких «центров по обеспечению безопасности» с целью усиления кибербезопасности государств-членов ЕС. Кроме того, по мнению Д.В. Красикова, для того, чтобы обеспечить кибербезопасность на территории стран ЕС, необходимо укрепить и развить концепцию цифрового суверенитета[246].

Инициатива разработки новой международной конвенции, которая будет регулировать соответствующие аспекты, касающиеся регулирования и развития систем ИИ была предложена Специальным межправительственным комитетом экспертов по ИИ Совета Европы (далее – Комитет по ИИ). Комитет по ИИ был учрежден Комитетом министров на его 1353-м заседании 11 сентября 2019 года. Конкретная задача Комитета по ИИ состоит в том, чтобы разработать правовые механизмы для регулирования технологий ИИ с учетом стандартов Совета Европы в области прав человека.

---

[244] Proposal for a Regulation of the European Parliament and the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Brussels 21.4.2021, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

[245] European Commission, «Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence», Brussels, April 21, 2021.

[246] Красиков Д.В. Развитие концепции цифрового суверенитета в правовой политике Европейского Союза. // Бизнес. Образование. Право. № 4 (57). 2021. С. 255–259.

Комитет по ИИ отмечает, что применение систем ИИ может способствовать процветанию социальному благополучию за счет прогрессивных технических инноваций, но в то же время определенные области применения систем ИИ вызывают озабоченность, поскольку они представляют риски в отношении соблюдения прав человека, процветания демократических устоев, а также обеспечения верховенство закона[247].

Работа Комитета по ИИ актуальна, поскольку она создает многостороннюю группу, в которой эксперты со всего мира могут инициировать идеи в части реализации международных соглашений в сфере ИИ, образования юридического механизма, который сможет регулировать ИИ, реализуя такие основополагающие принципы, как защита основных прав и свобод человека, обеспечение верховенство права и процветание демократических ценностей, содержащиеся в международных договорах Совета Европы.

Комитет по ИИ отмечает, что целью будущего международного универсального соглашения должно быть не установление подробных технических параметров для проектирования, разработки и применения систем ИИ, а установление определенных базовых принципов и норм, регулирующих разработку, проектирование и применение систем ИИ[248].

Необходимость дальнейшего стратегического партнерства для борьбы с киберпреступлениями является актуальным для мирового сообщества[249].

Работа ЮНИКРИ, Комитета по ИИ, ЕЦБК и Интерпола в части регулирования систем ИИ является очень важным для различных институтов государственной власти в целях дальнейшего укрепления внутригосударственной политики в части ИИ.

---

[247] URL: https://rm.coe.int/cahai-2021-09rev-elements/1680a6d90d/.

[248] Ad hoc committee on artificial intelligence (CAHAI). Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy, and the rule of law. Strasbourg, 3 December 2021.P. 15.

[249] European Parliament, Special Committee on Artificial Intelligence in a Digital Age (AIDA), «Joint hearing on the external policy dimension of AI», March 1st and 4th 2021.

Получение электронных доказательств является очень важным элементом международного сотрудничества. Глобальные поставщики услуг (например, Google, Microsoft, WhatsApp) могут оказать содействие в этом вопросе национальным правоохранительным органам. Наличие таких ЭД может поспособствовать в реализации уголовного преследования преступника и привлечения его к ответственности. В силу того, что такого рода расследования являются трудными, дорогими и требуют немало времени, очень важно на первом этапе принять во внимание возможность в запрашивании ЭД у глобального поставщика услуг. Данный механизм международного сотрудничества является неоперативным из-за перегруженности. ЭД имеют свойство быстро пересекать территориальные границы государств, когда получение необходимой информации через взаимную правовую помощь осуществляется небыстро и является очень сложной задачей для специалиста, у которого отсутствует надлежащий опыт в части реализации вышеназванной процедуры. В Практическом руководстве по порядку запроса ЭД 2019 года содержатся инструменты, благодаря которым компетентные органы могут запрашивать ЭД[250].

Таким образом, вышеприведенный метод международного сотрудничества видится эффективным, сочетающимся со стремительным характером киберпреступлений, для которых в сети «Интернет» нету границ.

Цифровизация постоянно развивается. ИИ приобретает все большее значение в борьбе с киберпреступлениями. Чтобы определить будущие риски, ИИ изучает данные в информационном пространстве. Это облегчает сотрудникам службы безопасности обнаружить киберпреступления до того, как они будут совершены[251].

Одним из механизмов в области обеспечения международной информационной безопасности является установление международно-

---

[250] Практическое руководство по порядку запроса электронных доказательств. 2019 г. URL: https://www.unodc.org/documents/organized-crime/GPTOC/GPTOC2/_ebook.pdf/.

[251] Malwarebytes Lab, «When Artificial Intelligence goes awry: separating science fiction from fact», without publication date, URL: https://resources.malwarebytes.com/files/2019/06/Labs-Report-AI-gone-awry.pdf/.

правовой ответственности государств за действие и бездействие на своей территории, которые наносят трансграничный ущерб другим странам[252]. Иначе говоря, государство должно быть привлечено к ответственности в тех случаях, когда непринятие сдерживающих мер на его территории привело к совершению киберпреступлений, которые затронули другие государства или отдельных физических лиц или организации, расположенные в других государствах.

Кроме того, необходимо эффективное трансграничное сотрудничество по правовым и техническим аспектам международной информационной безопасности. Требуется согласование нормотворческой базы о международной информационной безопасности, расширения трансграничной правовой и технической помощи, а также эффективное участие информационной индустрии и оказания помощи развивающимся странам в совершенствовании их технического оснащения в области регулирования международной информационной безопасности[253].

Международная информационная безопасность – это такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности.

Киберпреступление может создать угрозу международной информационной безопасности, например, оказать неправомерное воздействие на критически информационную инфраструктуру (вывод из строя телекоммуникации, транспорт, ЭВМ, программное обеспечение, сеть «Интернет», промышленные системы, используемые для управления

---

[252] Council of Europe. A Conceptual Approach for Setting a Standard of Care for Cross-Border Internet', discussion Paper of the Council of Europe Ad Hoc Advisory Group on Cross-border Internet for Workshop. P. 6

[253] Digital Divide is used to refer to the gap between countries at different socio-economic levels with regards to their opportunities to access information and communication technologies for a wide variety of purposes. According to the Organization for Economic Cooperation and Development (OECD), digital divide refers to the gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard to their opportunities to access information and communication technologies (ICTS) and the use of the internet for a wide variety of activities – OECD. (2001). *Understanding the Digital Divide* (OECD, 2001) p.5.

производством и распределением энергии, процессами химического производства и переработки).

Для того чтобы эффективно противостоять киберпреступлениям при помощи ИИ, необходимо использовать хакерскую стратегию. Сотрудники Microsoft создали исходный код внутреннего инструмента PyRIT, который способен посодействовать разработчикам в обнаружении рисков в моделях нейросети. PyRIT автоматически генерирует тысячи состязательных запросов нейросети, с целью проверить способен ли ИИ эффективно противодействовать попыткам взлома. Алгоритм работы инструмента сгенерирован таким образом, что позволяет разработчикам добавлять разных видов ввода систем ИИ, например, голоса или изображения.

Таким образом, ИИ может быть орудием способным предотвратить совершение киберпреступлений, а также оказать важную помощь правоохранительным органам в части расследовании и собирании доказательств, инструментом обеспечения международной информационной безопасности в целом. С другой стороны ИИ может нанести угрозу международной информационной безопасности, если системы ИИ окажутся в распоряжении умелых киберпреступников, способных взламывать базы данных, осуществлять кибератаки на инфраструктуру, критически важные объекты и при этом оставаться латентными. Более того, непосредственная реализация киберпреступления может быть совершена с помощью роботизированных компьютеров, находящихся под автономным управлением ИИ без непосредственного участия физического лица[254]. В связи с этим необходимо перманентное сотрудничество между национальными правоохранительными органами государств, а также международными правоохранительными органами, такими как Интерпол и Европол и иными международными институтами с целью недопущения и минимизирования

[254] Горелик И.Б., Зимненко Б.Л., Яковенко А.В., Ярышев С.Н. Актуальные международно-правовые проблемы в области обеспечения кибербезопасности // Электронное сетевое издание «Международный правовой курьер». 2023. № 5. С. 1–6.

совершения киберпреступлений при помощи систем ИИ. Международное взаимодействие глобальных поставщиков услуг и правоохранительных органов в части получения электронных доказательств является одним из элементов сотрудничества. Более того, разработка правового документа международного характера в части регулирования систем ИИ в целях защиты прав человека, международного сотрудничества, совместного научно-технологического развития, а также обеспечения мира, безопасности и стабильности, видится целесообразным. Однако, на сегодняшний день, обычные нормы международного права и механизмы международно-правовых институтов в части реализации ИИ не работают. Противостоять преступлениям в сфере информационных технологий при помощи нейросети возможно путем разработки исходного кода внутреннего инструмента специального ПО, посредством которого разработчики систем ИИ смогут находить риски и тем самым выявлять проблемы информационной безопасности.

Как в международных договорах, так и на национальном законодательном уровне содержатся положения о суверенитете государств.[255] Значение суверенитета для государства заключается в том, что каждое государство имеет право решать вопросы на своей территории независимо и при невмешательстве других государств. В результате этого коллизия законов между различными государствами становится неизбежной, поскольку законы принимаются в разных юрисдикциях. В связи с этим обстоятельством возникают вопросы в части борьбы с киберпреступлениями, особенно в рамках юрисдикции.

Таллинское руководство 2.0 начинается с раскрытия суверенитета и в своем первом правиле подчеркивает, что «Принцип суверенитета применим к киберпространству». В двух последующих правилах проводится различие между внутренним и внешним суверенитетом, а в правиле 4 говорится, что

[255] United Nations. (2021). *United Nations Charter*. URL: https://www.un.org/en/about-us/un-charter/ (дата обращения: 18.07.2024). – Текст: электронный.

государство не должно проводить действия в киберпространстве, которые нарушают суверенитет другого государства.

Предположение, лежащее в основе заключения эксперта в правиле 4, заключается в том, что суверенное равенство государств является одним из основополагающих принципов международного права, закреплённое в Уставе ООН, нарушение которого является международно-противоправным деянием. В комментарии к правилу 4 говорится:

«В киберпространстве осуществление действий органом государственной власти или должностным лицом на территории другого государства в отношении этого государства является нарушением суверенитета. Например, если агент спецслужбы одного государства использует флэш-накопитель USB для внедрения вредоносного ПО в инфраструктуру, расположенную в другом государстве, то это будет квалифицироваться, как нарушение суверенитета»[256].

Киберпреступления не имеют определенных границ. Преступник, например, находясь дома при помощи гаджета или персонального компьютера, подключенного к сети «Интернет», может совершить противоправное деяние, которое может привести к серьезным негативным последствиям за тысячи километров от него. Повсеместное распространение информации в современных системах связи говорит нам о неважности территориального расположение преступников и потерпевших. Использование ИКТ в противоправных целях в одном государстве могут нанести урон ЭВМ другого государства[257].

По этой причине международное сотрудничество в части обеспечении безопасного информационного пространства является открытым. Специалисты считают, что организованные преступные группы используют

[256] Professor of Law, Brigham Young University Law School. Professor Jensen served as a member of the International Group of Experts on both Tallinn 1.0 and Tallinn 2.0. © 2017, Eric Talbot Jensen.
[257] Prof. Dr. Ulrich, S. (1999). Memorandum On A European Penal Code. *European Journal of Law Reform*, *1*, 445-471. URL: http://www.jura.uni-muenchen.del/.

пробел в части неясности установления юрисдикции в своих корыстных целях, чтобы избежать уголовного преследования.

Юрисдикция является компетенцией суда в части ведения судебного процесса[258]. Вопрос о юрисдикции настолько важен, что он формирует базу любого судебного решения[259].

Данный дискурс требует проведения соотношения в части различия между экстерриториальной и территориальной юрисдикцией. Первый случай учитывает компетенцию суда, когда его решение запрашивается для приведения в исполнение за пределами его юрисдикции.

В доктрине международного права выделяют территориальную юрисдикция и юрисдикция in personam. Территориальная юрисдикция решает фундаментальный вопрос о том, обладает ли суд компетенцией за пределами своей территории, в то время как юрисдикция in personam касается того, вправе ли суд вынести решение по делу подсудимого, не подпадающего под его юрисдикцию[260]. Киберпространство не имеет четких территориальных границ; трудно определить, из какой страны преступник получает доступ к сети «Интернет» или с территории какого государства отправляется конкретная информация[261]. Учитывая трансграничную особенность киберпреступлений, их можно отнести в отдельную категорию преступлений международного характера. Отличительной особенностью традиционных преступлений от киберпреступлений является то, что они совершаются в определенном месте.

Приведем в качестве примера кейс с вирусом «Я ЛЮБЛЮ ТЕБЯ», который атаковал более половины интернет-пользователей на Филиппинах в 2000 году несмотря на то, что отправитель находился за много миль от них[262].

---

[258] *Alade V Alemuloke* (1988) 1 NWLR (Pt. 69) 207.
[259] *Madukolu&Ors V Nkemdilim* (1962) 1 All NLR 587.
[260] Ajayi, E.F.G (2016). Challenges to Enforcement of Cyber-crimes Laws and Policy. *Journal of Internet and Information Systems* Vol. 6(1), pp. 1-12.
[261] A cybercriminal can be in location A, and then make the server hosting his information or transaction be location B and this information is sent to location C.
[262] Lokwani, P. 2020. *Do You Know About Strange I LOVE YOU Virus?* Procaffenation. URL: https://procaffenation.com/know-about-strange-i-love-you/.

При помощи распространения информации через компьютерные сети преступники могут совершать киберпреступления удаленно. Использование ИКТ в противоправных целях в одном государстве, могут нанести непоправимый урон в отношении ЭВМ другого государства[263].

В 2014 году Барак Обама подтвердил, что кибератака, в результате которой была взломана Sony Entertainment Pictures в Соединенных Штатах Америке, и как следствие обнародованы личные данные и фотографии сотрудников, была осуществлена из Северной Кореи[264]. Северная Корея отрицала обвинение в свой адрес.

Приведенный выше пример киберпреступления свидетельствуют о неясности в вопросе, касающейся юрисдикции. Предполагая, что проблема идентификации преступника решена и оказывается, что он/она находится в другой стране, отличной от страны проживания жертвы преступления, становится довольно проблематичным определить, кто должен обладать юрисдикцией для рассмотрения дела о преступлении[265].

В Таллиннском Руководстве 2.0 рассматривается территориальная юрисдикция и подтверждается, что к действиям в киберпространстве применяется как субъективная, так и объективная территориальная юрисдикция[266].

В Таллиннском Руководстве 2.0 также говорится, что государства могут устанавливать экстерриториальную юрисдикцию посредством принципа защиты, национального принципа в отношении действий в киберпространстве за пределами их территории.

Согласно мнению экспертов Таллиннского руководства 2.0, международное право, включая конкретные договоры в области морского,

---

[263] Sieber, U. 1997. Memorandum on a European Model Penal Code, p. 2.

[264] Gala, J. 2017. *How Cybercrime Affects International Relations*. Stanford Management, Science and Engineering. URL: https://mse238blog.stanford.edu/2017/07/jugal23/how-cyber-crime-affects-international- relations/ (дата обращения: 18.07.2024). – Текст: электронный.

[265] Ajayi, E.F.G. 2016. Challenges to Enforcement of Cyber-crimes Laws and Policy. *Journal of Internet and Information Systems* Vol. 6(1), pp. 1-12.

[266] The Tallinn Manual 2.0: Highlights and Insights. Eric Talbot Jensen. Brigham Young University School of Law.2017. P. 746.

космического воздушного права, могли бы способствовать осуществлению принудительной юрисдикции за рубежом. Эксперты пришли к выводу, что там, где происходит предоставление юрисдикции, они будут включать деятельность, связанную с кибербезопасностью. Фактически, некоторые договоры могут конкретно ссылаться на определенные экстерриториальные правоприменительные привилегии, такие как Конвенция о киберпреступности (2001)[267].

Учитывая природу электронных данных, Киберцентр НАТО признал, что могут быть случаи, когда неясно, в каком состоянии находятся эти данные или цифровые доказательства. Киберцентр НАТО определил, что международное право в настоящее время четко не регулирует этот вопрос, поэтому Киберцентр НАТО не смог прийти к какому-либо консенсусу по этому вопросу. Предполагается, что в таком случае государство, решившее воспользоваться своей правоприменительной юрисдикцией, сделало бы это с определенным риском.

Специалисты также указали, что существует трудность в части квалификации определения электронных данных, доступных во всемирной паутине и размещенных на платформах в другой стране, под ведомством территориальной или экстерриториальной юрисдикции. В итоге Киберцентр НАТО пришел к выводу, что данный кейс относится скорее к территориальной юрисдикции, поскольку данные имеются в соответствующем государстве.

Конвенция СЕ предлагает определенные руководящие принципы в части юрисдикции. Государство обладает юрисдикцией, если было совершено киберпреступление:

1. На своей территории;

2. На борту судна, плавающего под флагом страны;

3. На борту воздушного судна, зарегистрированного в соответствии с законодательством страны;

---

[267] The Tallinn Manual 2.0: Highlights and Insights. Eric Talbot Jensen. Brigham Young University School of Law.2017. P. 748.

4. Гражданами одной из стран, если преступление наказуемо по уголовному законодательству той страны, где оно было совершено, или если преступление совершено за пределами территориальной юрисдикции какого-либо государства.

Учитывая трансграничный характер киберпреступления, юрисдикция государства будет распространяться, когда потерпевший находится в пределах ее границ, а также когда сам преступник будет находиться на территории данного государства. Более того, IP-адрес, с помощью которого осуществляются хакерские атаки будет также подпадать под юрисдикцию того государства, на территории которого он находится.

В случае возникновения спорной ситуации между государствами в части установления юрисдикции, участникам Конвенции СЕ необходимо провести консультации для того, чтобы определить в чьей юрисдикции будет осуществлено уголовное преследование и дальнейшее судебное разбирательство. Страна, в которой было совершено большинство преступлений, или страна, которая в наибольшей степени пострадала от преступлений, может иметь решающее значение. Местонахождение свидетелей также может быть важным фактором. Проблема Конвенции СЕ заключается в том, что она применима только к государствам, ратифицировавшим ее[268].

Анализируя вышесказанное, можно сделать вывод о том, что проблема в отсутствии четких правил юрисдикции порождает трудность у государств в части регулирования киберпространства. Киберпространство не имеет четких территориальных границ. Таким образом, становится затруднительно определить конкретную страну, где преступник получает доступ к сети «Интернет» или с территории какого государства отправляется конкретная компьютерная информация.

[268] Daskal, J., Kennedy-Mayo, D. (2020). Budapest Convention: What is it and How is it being Updated?.Cross Border Data Forum. URL: https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it- being-updated/ (дата обращения: 18.07.2024). – Текст: электронный.

Кроме того, если преступник совершил киберпреступление, находясь в одной стране, а потерпевший находился в другой, то на преступника будет распространяться юрисдикция того государства, где находился потерпевший. Анализ международных договоров дает нам понять, что страна, на территории которого находится потерпевший, может устанавливать наказание. В таком случае институт экстрадиции будет играть важную роль в части одного из механизмов сотрудничества между государствами в части противодействия киберпреступлениям.

Экстрадиция – это процесс выдачи обвиняемого в преступлении одним государством другому. Оксфордский словарь определяет экстрадицию, как передачу одним государством другому лица, обвиняемого в совершении преступления в последнем. Таким образом, если лицо предположительно совершило компьютерное преступление в одной стране и скрывается в другой, то все, что нужно сделать государству, где проживает преступник, – это оперативно оказать содействие в выдаче преступника в запрашивающую страну, чтобы он предстал перед судом[269].

Вопрос экстрадиции в международном праве довольно дискуссионный. С одной стороны, основания, прописанные в двусторонних соглашениях между государствами в части отказа в выдаче, являются одним из гарантов защиты прав лиц, подлежащих выдачи, но с другой стороны, принцип суверенного равенства государств позволяет в итоге решить, хотят государства выдавать предполагаемого преступника или нет. Статья 3 ЕКПЧ запрещает выдачу лиц, если существуют реальные основания полагать, что возможно обращение с предполагаемым преступником, противоречащим статье 3 ЕКПЧ.

Суд в деле «Soering V The United Kingdom» отметил следующее – «страх предполагаемого преступника перед унижающим достоинство наказанием и пытками является достаточной причиной для отклонения запроса об

[269] Ajayi, E.F.G (2016). Challenges to Enforcement of Cyber-crimes Laws and Policy. *Journal of Internet and Information Systems* Vol. 6(1), pp. 1-12

экстрадиции»[270]. Таким образом, суд подтвердил, что страны, которые намерены осуществить судебный процесс в отношении преступника из другой страны, обязаны соблюсти принципы гуманности и справедливого судебного разбирательства. В теории, если будет вынесен такой заочный приговор, как смертельная казнь в отношении преступника, подлежащего выдаче, то большинство цивилизованных стран вправе отказать в экстрадиции. Легитимным основанием в отказе также может послужить преследование по политическим мотивам[271]. Проблема заключается в трудности отнесения конкретного политического преступления к киберпреступлению. Например, если хакер блокирует веб-сайт, используемый для пропаганды политической лжи о деятельности конкретного правительства, и затем скрывается в другой стране, будет ли его предполагаемое преступление политическим или уголовным[272]?

Основополагающим принципом международного права является невмешательство во внутренние дела другого государства.[273] Этот постулат включен в различные международные соглашения, такие как Конвенция Монтевидео 1933 года[274], Устав Организации американских государств 1948 года,[275] Декларация Генеральной Ассамблеи ООН о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций 1970 года[276]. Прежде чем пострадавшая страна сможет предпринять какие-либо действия, необходимы доказательства, подтверждающие нарушение международного права. Вмешательство в

---

[270] See *Soering V the United Kingdom* (1989) European Court of Human Rights; *Othman (Abu Qatada) V United Kingdom* 8139/09 (2012) ECHR 56

[271] Bassiouni., M. C (1999). The Sources and Content of International Criminal Law: A Theoretical Framework *International Criminal Law* 3-126; *Cheng V Governor of Pentonville Prison* (1973) A.C. 931, 945 H.L.;*Ex Parte Schtraks* (1964) AC 556, at 583 HL; and *Schtraks V Government of Israel* (1964) AC 556, 582- 584.

[272] Ajayi, E.F.G (2016). Challenges to Enforcement of Cyber-crimes Laws and Policy. *Journal of Internet and Information Systems* Vol. 6(1), pp. 1-12.

[273] UNODC. 2019. *Cybercrime: Legal Frameworks and Human Rights*. UNODC. URL: www.unodc.org/e4/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html/.

[274] URL: https://wa.nt.am/ru/archives/1719/.

[275] URL: https://docs.cntd.ru/document/1902051/.

[276] URL: https://www.un.org/ru/documents/decl_conv/declarations/intlaw_principles.shtml/.

информационное пространство может подорвать доверие общественности к способности правительства обеспечить безопасность и экономическую стабильность[277].

Вмешательство в информационное пространство может включать в себя: проведение DdoS-атак (хакерская атака на вычислительную систему с целью довести ее до отказа) на системы критической инфраструктуры; использование вредоносных программ для заражения секторов критической инфраструктуры с намерением повредить системы, украсть, удалить и модифицировать данные и/или нарушить работу служб; распространение дезинформации, поддельных новостей и пропаганды с целью подрыва авторитета государства. Определение юридических границ между законным и незаконным вмешательством в информационное пространство (основанными на принципах суверенного равенства, невмешательства и территориальной целостности) является чрезвычайно сложным. Отчасти это объясняется неспособностью государств в достаточной степени четко сформулировать, каким образом обычные международно-правовые нормы должны применяться в информационном пространстве.

Международное право позволяет одному государству привлечь к международно-правовой ответственности другое государство за совершение киберпреступления против него, однако необходимы доказательства, чтобы установить нарушение норм международного права[278].

Основным источником права международной ответственности является комплекс международно-правовых обычаев, который, как это широко признано в практике государств и институтов международного правосудия, в значительной степени отражен в принятых Комиссией международного права в 2001 г. Проектах статей об ответственности государств за международно-противоправные деяния.

---

[277] Maurer, T. (2018). Cyber Proxies and Their Implications for Liberal Democracies. *The Washington Quarterly* Vol 41, Issue 2 URL: https://www.tandfonline.com/doi/abs/10.1080/0163660X.2018.1485332?journalCode=rwaq2/.

[278] Diakonia. (2020). *What Should a State do if it Violates International Law*. URL: https://www.diakonia.se/en/IHL/The-Law/Internationl-Law1/Enforcement-of-IL/What-should-a-state-do-if-it-violates-IL/.

Согласно ст. 2 Проектов статей, «международно-противоправное деяние государства имеет место, когда какое-либо поведение, состоящее в действии или бездействии: a) присваивается государству по международному праву; и b) представляет собой нарушение международно-правового обязательства этого государства».

Если будет признано международно-противоправное деяние (киберпреступление), существуют обстоятельства, которые могут исключить противоправность конкретной деятельности в информационном пространстве. Эти обстоятельства изложены в статьях Комиссии международного права об ответственности государств за международно-противоправные деяния 2001 года[279]. Приведем некоторые статьи.

Статья 20. Согласие: Действительное согласие государства на совершение определенного деяния другим государством исключает противоправность этого деяния по отношению к первому государству в той мере, в какой деяние остается в пределах этого согласия.

Статья 21. Самооборона: Противоправность деяния государства исключается, если это деяние представляет собой законную меру самообороны, принятую в соответствии с Уставом ООН.

Статья 25. Состояние необходимости:

1) Государство не может ссылаться на необходимость в качестве основания для исключения противоправности деяния, не соответствующего международному обязательству этого государства, за исключением случаев, когда это деяние: (a) является единственным способом для государства защитить существенный интерес от серьезной и неминуемой опасности; и (b) не наносит серьезного ущерба существенным интересам государства или государств, в отношении которых существует обязательство, или международного сообщества в целом.

2) В любом случае государство не может ссылаться на необходимость в качестве основания для исключения противоправности, если: (a)

[279] URL: https://www.un.org/ru/documents/decl_conv/conventions/pdf/responsibility.pdf/.

рассматриваемое международное обязательство исключает возможность ссылки на необходимость; или (b) государство способствовало возникновению ситуации необходимости.

Довольно трудно представить себе вышеуказанные обстоятельства в случае киберпреступления одного государства против другого государства. Согласно правилу 6 Таллиннского руководства 2.0: «государство должно проявлять должную осмотрительность, не позволяя использовать свою территорию, находящуюся под его правительственным контролем, для деятельности в информационном пространстве, которая нарушает суверенитет других государств и приводит к серьезным неблагоприятным последствиям для них».

Важно отметить, что государства обязаны предотвращать использование их территорий в целях совершения кибератак на другие страны[280]. В соответствии с принципом должной осмотрительности государства обязаны принять меры для прекращения деятельности в информационном пространстве, проводимых из их государства, используя разумно доступные средства, когда их уведомляют о них[281].

Правило 14 Таллиннского руководства 2.0 гласит: «Государство несет международно-правовую ответственность за связанное с киберпространством деяние, которое приписывается государству, и которое представляет собой нарушение международно-правового обязательства».

Примечательно также, что в соответствии с правилами 15-17 Таллиннского руководства 2.0 и статьями 4, 6, 8 и 11 Доклада Комиссии международного права об ответственности государств за международно-противоправные деяния 2001 года, деятельность в информационном пространстве государственных органов, органов других государств и негосударственных акторов могут быть отнесены к деятельности государства.

---

[280] Lotrionte, C. State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights. *Emory International Law Review.* URL: https://law.emory.edu/eilr/content/volume-26/issue-2/symposium%20/state-sovereignty-self-defense-in-cyberspace.html/ (дата обращения: 18.07.2024). – Текст: электронный.

[281] Rule 7 of Tallinn Manual 2.0: note that the Tallinn Manuals (2013; 2017) are non-binding documents.

Большая семерка в своей декларации об ответственности государств в информационном пространстве отметила, что «обычное международное право об ответственности государств устанавливает стандарты для присвоения деяний государствам, которые могут быть применимы к деятельности в информационном пространстве[282].

Однако, несмотря на применимость норм общего права международной ответственности к отношениям в киберпространстве, существуют определённые сложности в части присвоения государствам поведения, связанного с причинением трансграничного вреда с использованием ИКТ. Например, государство, которому в той или иной форме причинен вред в результате совершения киберпреступления, не всегда в состоянии самостоятельно предпринять все необходимые действия для сбора доказательств, в том числе в силу территориальной ограниченности исполнительной юрисдикции. Одним из наиболее действенных мер преодоления этих проблем, по мнению многих ученых, является признание существования обязательства должной распорядительности, возлагаемого на страны общим международным правом и распространяющегося на межгосударственные отношения в информационном пространстве[283]. Данное обязательство требует, чтобы страны не разрешали использовать свою территорию и инфраструктуру в целях реализации деятельности, причиняющей негативные последствия другим странам. Реализация данного обязательства применительно к осуществлению деятельности в информационном пространстве тем не менее может быть сопряжена с определенными рисками для межгосударственных отношений и требует ответственного подхода стран к применению контрмер в порядке самозащиты.

---

[282] CCDCOE. *G7 Recognizes Emerging Challenges of Responsible State Behavior.* URL: https://ccdcoe.org/incyder-articles/g7-recognises-emerging-challenges-of-responsible-state-behaviour/ (дата обращения: 18.07.2024). – Текст: электронный.

[283] Carlin J.P. Detect, disrupt, deter: A whole-of-government approach to national security cyber threats // Harvard national security journal. – Cambridge, 2016. – Vol. 7. – P. 414.

Таким образом, вопросы суверенитета, юрисдикции, экстрадиции, а также ответственности взаимосвязаны между собой. В международном уголовном праве необходимо учитывать каждый из этих факторов, когда речь идет о расследовании киберпреступлений. На сегодняшний день регулирует вышеназванные вопросы в совокупности Таллиннское руководство. Положения Таллиннского руководства являются рекомендательными и не имеют обязательной силы. Таким образом, целесообразно прописать правила о юрисдикции и экстрадиции, а также международно-правовой ответственности в международном соглашении универсального характера, нормы которого будут относиться к твёрдому праву в целях эффективного противодействия киберпреступлениям.

Заключение

Подводя итог вышеизложенному на страницах предпринятого научного исследования, сделаем следующие выводы.

Настоящее научное исследование позволило автору на основе анализа международных соглашений, национального законодательства разных стран, а также национальных и зарубежных доктрин в части регулирования киберпреступлений выработать определённые рекомендации.

В частности, необходимо расширить перечень киберпреступлений, содержащийся в действующих международных соглашениях, добавив, например, кибербуллинг, имитацию голоса при помощи ИИ в целях совершения преступных действий в сети «Интернет», сбыт поддельных медицинских изделий, преступное использование криптовалют.

В диссертационном исследовании было уделено большое внимание понятийно-категориальному аппарату. Автором было выработано определение понятия киберпреступление. Киберпреступление – это виновно совершенный, несанкционированный доступ к информационно-коммуникационным технологиям при помощи компьютерных устройств и иных технических средств, с целью нанесения как материального, так и нематериального ущерба и влекущее негативные последствия трансграничного характера неограниченному круг лиц.

Кроме того, выработка консолидированного определения киберпреступление, как на доктринальном, так и на правовом уровне видится необходимым, для того чтобы иметь четкое представление относительно данного криминогенного явления.

Международному сообществу следует усовершенствовать, а также укрепить сотрудничество в части противодействия киберпреступлениям в целях обеспечения международной информационной безопасности. В силу того, что киберпреступление является с точки зрения международного права преступлением международного характера, противодействовать этому

криминальному явлению на уровне одного государства представляется невозможным. Остаются пробелы, как на национальном, так и на международном уровне, касающиеся юрисдикции и экстрадиции. Гармонизация и унификация внутреннего права в части регулирования киберпреступлений видится логичным в целях уголовного преследования преступников и дальнейшего судебного разбирательства.

В качестве противодействия киберпреступлениям автором предлагается использовать ИИ. ИИ может быть применен, как упреждающий удар, а также в качестве превентивной меры. Оказать незаменимую помощь правоохранительным органам в части оперативно-розыскной деятельности и обеспечения международной информационной безопасности. Благодаря алгоритмам машинного обучения (машинное обучение – это подмножество ИИ, где алгоритмы обучаются выводить определенные шаблоны на основе набора данных, чтобы определить действия, необходимые для достижения заданной цели) и обработке больших массивов данных, автоматизации процесса выявления и ликвидации опасностей, ИИ способен обеспечить необходимую киберзащиту. Обычные нормы международного права и механизмы международно-правовых институтов в части реализации ИИ не работают. Противостоять киберпреступлениям при помощи ИИ возможно путем разработки исходного кода внутреннего инструмента специального ПО, посредством которого разработчики систем ИИ смогут находить риски и тем самым выявлять проблемы кибербезопасности.

Принятие под эгидой ООН универсальной Конвенции в части регулирования киберпреступлений видится актуальным и необходимым. Во-первых, необходимо закрепить определение киберпреступление и привести актуальную классификацию киберпреступлений. Во-вторых, необходимы положения, которые облегчат и усовершенствуют сотрудничество правоохранительных органов государств в части расследования и собирания доказательств. В-третьих, урегулировать пробелы в части, касающейся юрисдикции, а также экстрадиции с соблюдением принципа суверенного

равенства государств и прав человека. В-четвертых, если рассматривать киберпреступление, как международное преступление, то необходимо создать международный оперативный и судебный орган, которые будут наделены соответствующими полномочиями и юрисдикцией в отношении использования ИКТ в противоправных целях.

Государства развиваются в части технологического совершенствования, и принятие предложений, содержащихся в этой диссертации, будут иметь большое значение для обеспечения того, чтобы такое развитие сети «Интернет» и технологий не предвещало глобальных угроз мировому сообществу.

Исходя из диссертационного исследования, вектор развития международного уголовного права в части киберпреступлений требует к себе особого внимания ученых разных специальностей. Приведенные в диссертации тезисы не носят полный характер. Поднимая проблему киберпреступлений, автор хотел привлечь внимание к данному вопросу и побудить дискутирование этой тематики в обозримом будущем. Положения настоящей диссертации могут найти практическое применение в законотворческой деятельности, а также быть использованы в учебном процессе.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Международно-правовые акты и официальные документы

1. Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами соответствии с Уставом Организации Объединенных Наций, принята Резолюцией Генеральной Ассамблеи ООН 1970 г. – URL: https://www.un.org/ru/documents/decl_conv/declarations/intlaw_principles.shtml (дата обращения: 18.07.2024). – Текст: электронный.

2. Декларация о цифровой экономике: инновации, рост и социальное благополучие 2016 г. (OECD/LEGAL/0426 Declaration on the Digital Economy: Innovation, Growth and Social Prosperity. Доступ из СПС «Гарант».

3. Директива 96/9/ЕС от 11 марта 1996 года «О правовой охране баз данных». Доступ из СПС «Гарант».

4. Директива № 2013/40/ЕС Европейского парламента и Совета Европейского Союза «Об атаках на информационные системы и о замене Рамочного решения 2005/222/ПВД Совета ЕС» (Принята в г. Брюсселе 12.08.2013). Доступ из СПС «Гарант».

5. Директива Европейского Союза 2001/29/ЕС от 22 мая 2001 года «О гармонизации срока действия охраны авторского права и некоторых смежных прав в информационном обществе». Доступ из СПС «Гарант».

6. Директива Европейского Союза 91/250/ЕЕС от 14 мая 1991 года «О правовой охране программ для ЭВМ». Доступ из СПС «Гарант».

7. Директива Совета Европейского Союза 2008/114/ЕС от 8 декабря 2008 г. о европейских критических инфраструктурах и мерах по их защите. Доступ из СПС «Гарант».

8. Договор о функционировании Европейского Союза. Доступ из СПС «Гарант».

9. Доктрина информационной безопасности Российской Федерации № 646 от 5 декабря 2016 года. Доступ из СПС «Гарант».

10. Европейская Конвенция о выдаче ETS № 024 (Париж, 13 декабря 1957 г.). – URL: https://rm.coe.int/ (дата обращения: 18.07.2024). – Текст: электронный.

11. Йоханнесбургская Декларация Десятого Саммита БРИКС от 26.07.2018. БРИКС в Африке: «Сотрудничество для достижения инклюзивного роста и всеобщего процветания в эпоху Четвертой промышленной революции». – URL: http://www.kremlin.ru/ supplement /5323/ (дата обращения: 18.07.2024). – Текст: электронный.

12. Конвенция Совета Европы «О предупреждении терроризма» (CETS № 196) (Варшава, 16 мая 2005 г.). Доступ из СПС «Гарант».

13. Доклада Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности 14.07.2021. – URL: https://crb.rgup.ru/rimg/files/Model-OON/2022/Doc/Доклад%20СБ%20ООН.pdf (дата обращения: 18.07.2024). – Текст: электронный.

14. Понимание киберпреступности: явление, задачи и законодательный ответ: отчет Международного союза электросвязи (МСЭ). – 2014. – URL: http://www.itu.int/ (дата обращения: 18.07.2024). – Текст: электронный.

15. Практическое руководство по порядку запроса электронных доказательств. – 2019. – URL: https://www.unodc.org/documents/organized-crime/GPTOC/GPTOC2/_ebook.pdf (дата обращения: 18.07.2024). – Текст: электронный.

16. Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (29.06.2021). – URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (дата обращения: 18.07.2024). – Текст: электронный.

17. Рамочное решение Совета ЕС 2002/584//ПВД от 13 июня 2002 года «О европейском ордере на арест и о процедуре передачи лиц между государствами-членами». Доступ из СПС «Гарант».

18. Резолюция ГА ООН от 18 декабря 2019 года. A/RES/74/177. – URL: https://documents.un.org/doc/undoc/gen/n19/431/57/pdf (дата обращения: 18.07.2024). – Текст: электронный.

19. Резолюция Совета Безопасности ООН 2253 от 17 декабря 2015 г. «Угрозы международному миру и безопасности, создаваемые террористическими актами». Доступ из СПС «Гарант».

20. Рекомендация Совета по принципам формирования интернет-политики 2011 г. (OECD/LEGAL/0387 Recommendation of the Council on Principles for Internet Policy Making). – URL: https://cdn.www.gob.pe/uploads/document/file/4017013/OECD-LEGAL-0387-en.pdf.pdf (дата обращения: 18.07.2024). – Текст: электронный.

21. Североатлантический пакт (Вашингтон, 4 апреля 1949 г.). Доступ из СПС «Гарант».

22. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2019 года). Доступ из СПС «Гарант».

23. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 года). Доступ из СПС «Гарант».

24. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г.). Доступ из СПС «Гарант».

25. Устав Организации Объединенных Наций (Сан-Франциско, 26 июня 1945 г.). Доступ из СПС «Гарант».

26. Ad hoc committee on artificial intelligence (CAHAI). Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy, and the rule of law. – Strasbourg. – 3 December. – 2021. – P. 15.

27. African Union Convention on Cyber Security and Personal Data Protection. 2014. – URL: https://au.int/ (дата обращения: 18.07.2024). – Текст: электронный.

28. Arab Convention on Combating Information Technology Offences. 2010. – URL: https://www.asianlaws.org/ (дата обращения: 18.07.2024). – Текст: электронный.

29. CCDCOE. G7 Recognizes Emerging Challenges of Responsible State Behavior. – URL: https://ccdcoe.org/incyder-articles/g7-recognises-emerging-challenges-of-responsible-state-behaviour/ (дата обращения: 18.07.2024). – Текст: электронный.

30. Commission on Crime Prevention and Criminal Justice, Enabling International Cooperation against Cybercrime through Technical Assistance and Capacity-Building, UN ESCOR, 22nd, Agenda Item d 7, UN Doc E/CN.15/2013/L.16 (2 April 2013) paras 3–4. – URL: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP11/E-CN15-2013-CRP11_E.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

31. Commission on Crime Prevention and Criminal Justice, Strengthening International Cooperation to Combat Cybercrime, UN ESCOR, 22nd sess, Agenda Item 7, UN Doc d E/CN.15/2013/L.14 (2 April 2013) para 3. – URL: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-NGO1/E-CN15-2013-NGO1_E.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

32. Comprehensive Study on Cybercrime xvii / (John Sandage, et al. eds.; United Nations Office on Drugs and Crime // Comprehensive Study on Cybercrime xxi-xxii. – 2013. – URL: https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html (дата обращения: 18.07.2024). – Текст: электронный.

33. Computer-Related Crime: Analysis of Legal Policy. – Paris: OECD, 1986. – URL: https://unov.tind.io/record/559?ln=ru (дата обращения: 18.07.2024). – Текст: электронный.

34. Convention on Cybercrime, Protocol on xenophobia and racism, Second protocol on enhanced co-operation and disclosure of electronic evidence, Explanatory Reports and Guidance Notes, Council of Europe, April 2022. – URL: https://www.coe.int/documents/8475493/0/PREMS+001323+GBR+2023+EN+Convention+booklets+Jan2023.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

35. Council of Europe. A Conceptual Approach for Setting a Standard of Care for Cross-Border Internet', discussion Paper of the Council of Europe Ad Hoc Advisory Group on Cross-border Internet for Workshop. – URL: https://www.coe.int/t/dc/files/events/internet/20100914_setting_standard_en.asp (дата обращения: 18.07.2024). – Текст: электронный.

36. COVID-19 Cybercrime Analysis Report-August 2020 (Interpol). // – URL: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID (дата обращения: 18.07.2024). – Текст: электронный.

37. ECOSOC Resolution 2007/20, International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime. – URL: https://www.un.org/ecosoc/en/docs/2007/Resolution%202007-20.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

38. EMCDDA and Europol 2019, EU Drug Markets Report 2019. // – URL: https://www.emcdda.europa.eu/system/files/publications/12078/20192630_TD0319332ENN_PDF.pdf (дата обращения: 18.07.2024). – Текст: электронный.

39. Eurojust and Europol 2019, Common challenges in combating cybercrime. // – URL: https://www.eurojust.europa.eu/sites/default/files/assets/2019-06-joint-eurojust-europol-report-common-challenges-in-combating-cybercrime-en.pdf (дата обращения: 18.07.2024). – Текст: электронный.

40. European Commission, «Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence», Brussels, April 21, 2021. // – URL: https://digital-strategy.ec.europa.eu/en/news/europe-fit-

digital-age-commission-proposes-new-rules-and-actions-excellence-and-trust-artificial (дата обращения: 18.07.2024). – Текст: электронный.

41. European Parliament, Special Committee on Artificial Intelligence in a Digital Age (AIDA), «Joint hearing on the external policy dimension of AI», March 1st and 4th 2021 / European Parliament, Special Committee on Artificial Intelligence in a Digital Age (AIDA). – URL: // https://www.europarl.europa.eu/cmsdata/232345/AIDA_Verbatim_1_March_2021_EN.pdf (дата обращения: 18.07.2024). – Текст: электронный.

42. European Union. 2021 – serious and organized crime threat assessment. A CORRUPTING INFLUENCE: THE INFILTRATION AND UNDERMINING OF EUROPE'S ECONOMY AND SOCIETY BY ORGANISED CRIME. P. 39. // – URL: https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021 (дата обращения: 18.07.2024). – Текст: электронный.

43. Europol 2020, Exploiting isolation – Offenders and victims of online child sexual abuse during the COVID- 19 pandemic. // – URL: https://www.europol.europa.eu/cms/sites/default/files/documents/europol_covid_reportcse_jun2020v.3_0.pdf (дата обращения: 18.07.2024). – Текст: электронный.

44. European Parliamentary Research Service. P. 7. // – URL: https://www.europarl.europa.eu/at-your-service/en/stay-informed/research-and-analysis (дата обращения: 18.07.2024). – Текст: электронный.

45. Europol and Eurojust. (July 5, 2019). Europol and Eurojust. «Common Challenges in Combating Cybercrime». Accessed on Oct. 14, 2020. // – URL: https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime (дата обращения: 18.07.2024). – Текст: электронный.

46. Europol (Feb. 28, 2017). Europol. «European Union Serious and Organized Crime Threat Assessment (SOCTA)». // – URL: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised- crime-threat-assessment-2017 (дата обращения: 18.07.2024). – Текст: электронный.

47. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: note by the Secretary-General. 2021. // – URL: https://digitallibrary.un.org/record/3934214/ (дата обращения: 18.07.2024). – Текст: электронный.

48. Information provided by Steven Malby, Senior Expert, Division of Treaty Affairs, Organized Crime and Illicit Trafficking Branch, UNODC, 23 May, 2014. // https://www.unodc.org/roseap/uploads/archive/documents/2012/05/cyber-crime/Bangkok_intro_presentation.pdf (дата обращения: 18.07.2024). – Текст: электронный.

49. International Telecommunication Union, World Summit on the Information Society, 'Tunis Agenda for the Information Society', WSIS-05/TUNIS/DOC/6 (Rev. 1) E, (18 November 2005) 40. // – URL: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html/ (дата обращения: 18.07.2024). – Текст: электронный.

50. INTERPOL European Working Party on Information Technology Crime (EWPITC) – Project on cloud computing, 2011. // – URL: https://www.coe.int/en/web/cybercrime/interpol-technical-webinars-e-first- (дата обращения: 18.07.2024). – Текст: электронный.

51. INTERPOL's contribution to the elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. // – URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/ (дата обращения: 18.07.2024). – Текст: электронный.

52. Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, 2009, E/CN.15/2009/CRP.13. // – URL: https://www.unodc.org/documents/treaties/organized_crime/ECN152009_CRP10.pdf (дата обращения: 18.07.2024). – Текст: электронный.

53. Proposal for a Regulation of the European Parliament and the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Brussels 21.4.2021. // – URL: available

at: https://eur-lex.europa.eu/legal- (дата обращения: 18.07.2024). – Текст: электронный.

54. Rep. of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, UN Doc A/CONF.213/18 at 56 – 7 [202] – [204] (18 May 2010). – URL: https://www.un.org/ru/conf/crimecongress2010/ (дата обращения: 18.07.2024). – Текст: электронный.

55. SADC Treaty. – URL: http://www.sadc.int/documents-publications/sadc-treaty/ (дата обращения: 18.07.2024). – Текст: электронный.

56. Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime. – 2012. // – URL: https:// www.itu.int/en/ITU/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

57. Special Report on Facial Recognition of the Center for AI and Digital Policy (CAIDP) that contains a summary of key references on this topic contained in the 2020 Report on Artificial Intelligence and Democratic Values // The AI Social Contract Index 2020 prepared by CAIDP. – 2020. // – December. – URL: https://caidp.dukakis.org/aisci-2020/ (дата обращения: 18.07.2024). – Текст: электронный.

58. STC-CICTC. A Global Approach to Cybersecurity and Cybercrime in Africa. Recommendations of the First Ordinary Session of the STC-CICT-1. // – URL: https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf (дата обращения: 18.07.2024). – Текст: электронный.

59. The Economic Community of West African States (ECOWAS) Directive on Fighting Cyber Crime within ECOWAS. 2011. – URL: https://issafrica.org/ctafrica/uploads/Directive%201:08:11%20on%20Fighting%20Cyber%20Crime%20within%20ECOWAS. pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

60. The Rome Statute of the International Criminal Cour. // URL: https://legal.un.org/icc/statute/99_corr/cstatute.htm (дата обращения: 18.07.2024). – Текст: электронный.

61. The right of the child to freedom from all forms of violence, CRC/C/GC/13, 18 April 2011, § 31(c)(iii) // UN Committee on the Rights of the Child, General Comment. – 2011. – № 13.

62. The Tallinn Manual 2.0: Highlights and Insights. Eric Talbot Jensen. Brigham Young University School of Law. – 2017. – P. 748.

63. Trend Micro Research, EUROPOL EC3 and UN Interregional Crime and Justice Research Institute (UNICRI), Malicious Uses and Abuses of Artificial Intelligence, 19 November 2020. // – URL: https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence (дата обращения: 18.07.2024). – Текст: электронный.

64. Ulrich, S. Memorandum on a European Penal Code. European / S. Ulrich. – 1999. // – URL: https://anti-fraud.ec.europa.eu/system/files/2021-07/eucrim_13_03_en.pdf (дата обращения: 18.07.2024). – Текст: электронный.

65. UN General Assembly, A/RES/45/121. 1990. 14 December. – URL: https://www.un.org/ru/ga/45/docs/45res.shtml (дата обращения: 18.07.2024). – Текст: электронный.

66. United Nations Charter. – 2021. // – URL: https://www.un.org/en/about-us/un-charter/ (дата обращения: 18.07.2024). – Текст: электронный.

67. United Nations. UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5). // – URL: http://www.uncjin.org/Documents/EighthCongress.html/ (дата обращения: 18.07.2024). – Текст: электронный.

68. UNODC. Cybercrime: Legal Frameworks and Human Rights /. UNODC. – 2019. // – URL: www.unodc.org/e4/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html/ (дата обращения: 18.07.2024). – Текст: электронный.

II. Список материалов судебной практики

69. Постановление Европейского Суда по правам человека от 16 октября 2007 г. Дело «Визер и компания «Бикос Бетейлигунген ГМБХ» против Австрии» [Wieser and Bicos Beteiligungen GMBH v. Austria] (жалоба № 74336/01) // СПС «ГАРАНТ».

70. Постановление Европейского Суда по правам человека от 2 декабря 2008 г. Дело «K. U. против Финляндии» [K. U. v. Finland] (жалоба № 2872/02) // СПС «ГАРАНТ».

71. Постановление Европейского Суда по правам человека от 3 апреля 2007 г. Дело «Копланд против Соединенного Королевства» [Copland v. United Kingdom] (жалоба № 62617/00) // СПС «ГАРАНТ».

72. Постановление Европейского Суда по правам человека от 4 декабря 2015 г. Дело «Роман Захаров (Roman Zakharov) против Российской Федерации» (Жалоба № 47143/06) (Большая Палата Европейского Суда). // – URL: https://base.garant.ru/71414610/?ysclid=m3l9kb6ubt49232557 (дата обращения: 18.07.2024). – Текст: электронный.

73. Soering V the United Kingdom (1989) European Court of Human Rights; Othman (Abu Qatada) V United Kingdom 8139/09 (2012) ECHR 56.

74. UNITED STATES DISTRICT COURT CLARK COUNTY, NEVADA. Case No. 2:17-cr-00306-JCM-VCF. 2nd day of April 2021.

75. United States District Court for the Northern District of California. Case 3:17-cr-00103-VC. February 28, 2017.

76. UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON AT SEATTLE NONO. CR11-0070RAJ SENTENCING MEMORANDUM. April 14, 2017.

III. Нормативные правовые акты Российской Федерации

77. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». // – URL: http://www.kremlin.ru/acts/bank/41919/page/3 (дата обращения: 18.07.2024). – Текст: электронный.

78. Распоряжение Президента Российской Федерации о признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 года № 557-рп «О подписании Конвенции о киберпреступности» от 28 марта 2008 года № 144-рп. // – URL: http://www.kremlin.ru/acts/bank/27059 (дата обращения: 18.07.2024). – Текст: электронный.

79. Распоряжение Президента Российской Федерации от 15.11.2005 г. № 557-рп о подписании Конвенции о киберпреступности. // – URL: https://base.garant.ru/2563598/?ysclid=m3k3kcpsl8999038261 (дата обращения: 18.07.2024). – Текст: электронный.

80. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности (Москва, 25 декабря 2013 г.). // – URL: https://base.garant.ru/70593484/?ysclid=m3k3qvddt7374055005 (дата обращения: 18.07.2024). – Текст: электронный.

81. Соглашение между Правительством Российской Федерации и Правительством Киргизской Республики о сотрудничестве в области обеспечения международной информационной безопасности (Москва, 25 февраля 2021 г.) // – URL: https://base.garant.ru/400779330/?ysclid=m3k3toku4y444985330 (дата обращения: 18.07.2024). – Текст: электронный.

82. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. От 09.11.2024) // – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/?ysclid=m3k3vb20v3740172829 (дата обращения: 18.07.2024). – Текст: электронный.

83. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // – URL: https://base.garant.ru/71556224/?ysclid=m3k4croaf4511177368 (дата обращения: 18.07.2024). – Текст: электронный.

84. Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // – URL: https://base.garant.ru/72838946/?ysclid=m3k3zjt78d695417937 (дата обращения: 18.07.2024). – Текст: электронный.

85. Указ Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности». // – URL: https://www.garant.ru/products/ipo/prime/doc/400473497/?ysclid=m3k40jt3wx350658531 (дата обращения: 18.07.2024). – Текст: электронный.

86. Федеральный закон «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» от 01.07.2021 № 237-ФЗ (последняя редакция) // СПС «Гарант».

IV. Нормативные акты иностранных государств

87. Federal Decree-Law № (5) of 2012 ON COMBATING CYBERCRIMES. United Arabic States. Issued on 25 Ramadan 1433 AH. Corresponding to 13 August 2012. // – URL: https://uaelegislation.gov.ae/en/legislations/1526 дата обращения: 18.07.2024). – Текст: электронный.

88. National Security Strategy. The White House, February 2015. // – URL: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf (дата обращения: 18.07.2024). – Текст: электронный.

89. National Cyber Strategy. The White House, September 2018. // – URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 18.07.2024). – Текст: электронный.

90. National Cybersecurity Strategy. The White House, March 2023. // – URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата обращения: 18.07.2024). – Текст: электронный.

V. Книги и статьи на русском языке

91. Аббуд, Р. Р. Актуальные вопросы международного права в части преступлений в сфере компьютерной информации / Р. Р. Аббуд // Евразийский юридический журнал. – 2021. – № 2 (153). – С. 43–44.

92. Аббуд, Р. Р. Актуальные проблемы международного права в части киберпреступлений / Р. Р. Аббуд // Актуальные проблемы международных отношений и международного права: сборник статей под редакцией Т. В. Кашириной, С. А. Агуреева, С. В. Воробьева. – М.: Дипломатическая академия МИД России, 2021.

93. Аббуд, Р. Р. Киберхалифат: нормативное определение и криминологическая характеристика в национальном и международном информационном праве / Р. Р. Аббуд // Вопросы российского и международного права. – 2018. – Том 8. – № 8А. – С. 195.

94. Аббуд Р.Р. Международно-правовое регулирование борьбы с киберпреступлениями // Российское правосудие. № 4. 2023. С. 24–30.

95. Аббуд Р.Р. Международно-правовая классификация новых киберпреступлений // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и Право. № 8. 2024 С. 121–124.

96. Бабаш, А. В. Актуальные вопросы защиты информации: монография / А. В. Бабаш, Е. К. Баранова. – М.: РИОР: ИНФРА-М, 2017. – 87 с.

97. Бирюков П. Н. Искусственный интеллект: вызовы современной юридической науке // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 2 (66). С. 256–260.

98. Буз, С. И. Киберпреступления: понятие, сущность и общая характеристика / С. И. Буз. – Юрист-Правоведъ. – 2019. – № 4. – С. 78–82.

99. Васильева, И. Н. Расследование инцидентов информационной безопасности: учебное пособие / И. Н. Васильева. – СПб.: Изд-во СПбГЭУ, 2019. – 5 с.

100. Волеводз, А. Г. К вопросу о сущности и содержании международного сотрудничества в борьбе с преступностью / А. Г. Волеводз //

Международное уголовное право и международная юстиция. – 2007. – № 1. – С. 11–20.

101. Глушков, В. М. Мышление и кибернетика / В. М. Глушков // Известия. – 1963. – № 156 (1410).

102. Голубев, В. А. Кибертерроризм – угроза национальной безопасности / В. А. Голубев. – URL: http://www.crime-research.ru/ articles/Golubev_Cyber_Terrorism/ (дата обращения: 18.07.2024). – Текст: электронный.

103. Горелик И. Б., Зимненко Б. Л., Яковенко А. В., Ярышев С.Н. Актуальные международно-правовые проблемы в области обеспечения кибербезопасности // Электронное сетевое издание «Международный правовой курьер». 2023. № 5. С. 1–6.

104. Данельян, А. А. Киберпространство и международное право / А. А. Данельян // Электронное сетевое издание «Международный правовой курьер». – 2019. – № 4–5. – С. 5–11.

105. Ефремова, М. А. К вопросу об уголовной ответственности за создание, распространение и использование вредоносных компьютерных программ М. А. Ефремова // Информационное право. – 2015. – № 3. – С. 12.

106. Жданов, Ю. Н. Кибермафия. Мировые тенденции и международное противодействие: монография / Ю. Н. Жданов, С. К. Кузнецов, В. С. Овчинский; вступ. ст. О. В. Храмова. – Москва: Норма, 2022. – 175 с.

107. Зорькин В.Д. Конституционно-правовое развитие России: монография / В.Д. Зорькин. – 2-е изд., испр. И доп. – М.: Норма, 2019. – 448.

108. Иванов, С. М. Международно-правовое регулирование борьбы с кибертерроризмом / С. М. Иванов // Право и безопасность. – 2013. – № 3–4. – С. 82–87.

109. Ильина, М. Ю. Перспективы сотрудничества государств — – членов ЕАЭС в области информационной безопасности / М. Ю. Ильина //

ЕВРАЗИЙСКАЯ ИНТЕГРАЦИЯ: экономика, право, политика. – 2022. – 16(1). – С. 119–127.

110. Ковалева, С. Е. О некоторых актуальных социально-психологических проблемах виртуальной коммуникации в информационную эпоху / С. Е. Ковалева // XXI век: итоги прошлого и проблемы настоящего плюс. – 2017. – № 5–6. – С. 122–127.

111. Козик, А. Л. Развитие информационных технологий и правовое регулирование общественных отношений / А. Л. Козик // Studii Juridice Universitare. – 2008. – № 3–4. – С. 122–123.

112. Королов, М. Как искусственный интеллект может противостоять киберугрозам / М. Королов // Директор информационной службы. – 2017. – № 10. – С. 13.

113. Красиков Д. В. Развитие концепции цифрового суверенитета в правовой политике Европейского Союза. // Бизнес. Образование. Право. № 4 (57). 2021. С. 255–259.

114. Крутских, А. В. Проблемы применения международного права к злонамеренному использованию ИКТ / А. В. Крутских, А. А. Стрельцов // Международная жизнь. – 2014. – № 11.

115. Липкина Н. Н. Принципы установления экстратерриториальной юрисдикции государств в киберпространстве в контексте правовых позиций Европейского Суда по Правам Человека // Правовая политика и правовая жизнь. № 2. 2021. С. 153–160.

116. Лукашук, И. И. Международное право. Особенная часть / И. И. Лукашук. – М., 1998. – 242 с.

117. Международное право: учебник / отв. ред. В. И. Кузнецов, Б. Р. Тузмухамедов. – 3-е изд., перераб. – М.: Норма: Инфра-М, 2010. – 720 с.

118. Международное право: учебник / отв. ред. А. Н. Вылегжанин. – М.: Высшее образование, Юрайт-Издат, 2009. – 787 с.

119. 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.: Издательство Юрайт, 2014. – С. 277–278.

120. Мезяев А.Б. К вопросу о некоторых рисках в процессе трансформации образования в контексте «цифровизации» общества и применения новых технологий // Материалы международной научно-практической конференции, посвященной 30-летию Университета управления «ТИСБИ» и 30-летию программы кафедр ЮНЕСКО/УНИТВИН. Казань, 2022. С. 179-182.

121. Нешатаева Т. Н. Международные организации и право: Новые тенденции в международно-правовом регулировании / Т. Н. Нешатаева. - Москва: Дело, 1998. - 270,[1] с.; 21 см.; ISBN 5-7749-0058-4: Б. ц.

122. Петрова, И. А. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств / И. А. Петрова, И. А. Лобачев // Журнал прикладных исследований. – 2020. – № 1. – С. 52–62.

123. Пищик, В. Я. Киберпреступность как ключевой операционный риск платежно-расчетной инфраструктуры глобальной финансовой системы и подходы к его регулированию в ЕАЭС / В. Я. Пищик, П. В. Алексеев // Финансовый журнал. – 2021. – № 3. – С. 54–66.

124. Попов, А. Н. Преступления в сфере компьютерной информации.: учебное пособие / А. Н. Попов. – СПб.: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. – С. 4–11.

125. Право Европейского Союза: учебник и практикум для бакалавриата и магистратуры / под ред. А. Х. Абашидзе, А. О. Иншаковой. – М.: Издательство Юрайт, 2016. – 482 с. – Серия: Бакалавр и магистр. Академический курс.

126. Русскевич, Е. А. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий / Е. А. Русскевич //

Международное уголовное право и международная юстиция. – 2018. – № 3. – С. 10–13.

127. Селиванов, Н. А. Проблемы борьбы с компьютерной преступностью / Н. А. Селиванов // Законность. – 1993. – № 8.

128. Смирнов, А. И. Международная информационная безопасность: теория и практика: учебник для вузов. В трех томах. Том 10 / А. И. Смирнов; под ред. А. В. Критских. – 2-е изд., доп. – М.: Аспект Пресс, 2021. – 384 с.

129. Скуратова А. Ю. Новый Европол: основные изменения в статусе Европейского полицейского ведомства // Международное право - International Law. - М.: Юрис Пруденс, 2010, № 3 (43). - С. 55–59.

130. Толстых, В. Л. Курс международного права / В. Л. Толстых. – 2019. – 453 с.

131. Тропина, Т. Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма / Т. Л. Тропина // Международное правосудие. – 2012. –№ 3. – С. 86–95.

132. Тункин Г.И. Теория международного права. Под общей ред. Проф. Л. Н. Шестакова. – М.: ИКД «Зерцало-М», 2019–416 с.

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

134. Шерстюк, П. // Сборник материалов по проблематике информационной безопасности государств – членов лиги арабских государств. – Москва, 2023. – 242 с.

VI. Диссертации, авторефераты диссертаций

135. Ефремов А.А. Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации: дис. … д-ра юрид. наук. / Ефремов А.А. – Москва, 2021. – 418 с.

136. Касенова М. Б. Правовое регулирование трансграничного функционирования и использования интернета: дис. … д-ра юрид. наук / Касенова М. Б. – Москва, 2016. – 511 с.

137. Суслопаров, А. В. Компьютерные преступления как разновидность преступлений информационного характера: дис. ... канд. юрид. наук / Суслопаров А. В. – Владивосток, 2010. – С. 32–56.

138. Талимончик, В. П. Международно-правовое регулирование отношений в сфере информации: автореф. дис. … д-ра юрид. наук / Талимончик В. П. – СПб., 2013. – 39 с.

139. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры: автореф. дис. ... канд. юрид. наук / Тропина Т. Л. –. Владивосток, 2005. – 19 с.

140. Nnesochi Nweze-Iloekwe. The legal and regulatory aspect of international cybercrime and cybersecurity: limits and challenges". /The golden gate university school of law, department of international legal studies, in fulfilment of the requirement for the confernment of the degree of scientiae juridicae doctor (SJD). – San Francisco, California, February 2022.

VII. Книги и статьи иностранных авторов

141. Рассел, Стюарт. Искусственный интеллект: современный подход / Стюарт Рассел, Питер Норвиг. – Издательский дом «Вильямс», 2016. – С 79–80.

142. A proposal for the Dartmouth summer research project on artificial intelligence / J. McCarthy, Dartmouth College M. L. Minsky, Harvard University N. Rochester, I. B. M. Corporation C. E. Shannon, Bell Telephone Laboratories. – August 31. – 1955. – P. 2.

143. Aaron, A. A legal Analysis of Cybercrime and Cyber Torts: Lessons for Nigeria [L. B. Thesis, University of Lagos] / A. Aaron. – 2019. – P. 6.

144. Abdulrauf, L. A. The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa? / L. A. Abdulrauf, C. M. Fombad // Journal of Media Law. – 2016. – Vol. 8. – Iss. 1. – P. 67–97.

145. Aho, B. Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China / B. Aho, R. Duffield // J. Econ. Soc. – 2020. – № 49. – P. 187–221.

146. Ajayi, E. F. G. Challenges to Enforcement of Cyber-crimes Laws and Policy / E. F. G. Ajayi // Journal of Internet and Information Systems. – 2016. – Vol. 6(1). – P. 1–12.

147. Ajetunmobi, R. L. (2015). Cybercrimes (Prohibition, Prevention, etc. Act 2015: A Review (2014–2015) / R. L. Ajetunmobi // NIALS Journal of Intellectual Property, 17. – 2015. – P. 171.

148. Alade, V. Alemuloke / V. Alade. – 1988. – 1 NWLR (Pt. 69) 207.

149. Australian Institute of Family Studies 2015, Conceptualising the prevention of child sexual abuse, accessibleat. // Antonia Quadara, Vicky Nagy, Natalie Siegel – URL: https://acuresearchbank.acu.edu.au/download/5bb2f7760724b150faee97eef3bf9afcfd4cb50e87d7fbab4096c71055c5c82c/1704205/OA_Quadara_2015_Conceptualising_the_prevention_of_child_sexual.pdf (дата обращения: 18.07.2024). – Текст: электронный.

150. Ball, K. M. African Union Convention on Cyber Security and Personal Data Protection / K. M. Ball // International Legal Materials. – 2017. – Vol. 56. – Iss. 1. – P. 164–192.

151. Barrinha, A. The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyber Space. Council on Foreign Relations / A. Barrinha. – (2020). – URL: https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace/ (дата обращения: 18.07.2024). – Текст: электронный.

152. Bassiouni, M. C. The Penal Characteristics of Conventional International Criminal Law / M. C. Bassiouni. P. 28–29.

153. Bassiouni, M. C. The Sources and Content of International Criminal Law: A Theoretical Framework / M. C. Bassiouni // International Criminal Law. – 1999. – 3–126.

154. Belsey, B. Cyberbullying: An emerging threat to the «always on» generation / B. Belsey. – URL: http://www. cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf (дата обращения: 18.07.2024). – Текст: электронный.

155. Black's Law Dictionary, 9th ed. – Изд., год. – P. 427.

156. Brenner, Susan W. Distributed Security: Preventing Cybercrime / Susan W. Brenner and L. Clarke Leo // John Marshall Journal of Computer & Information Law, 23. – 2005. – № 4. – P. 659–709.

157. Brenner, Susan W. The Privacy Privilege: Law Enforcement, Technology and the Constitution / Susan W. Brenner // 7 JOURNAL OF TECHNOLOGY LAW & POLICY, 124.

158. Brian, B. Kelly. Investing In a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform 92 / B. Kelly Brian // BOSTON UNIVERSITY LAW REVIEW, 1671–1673.

159. Calderoni, Francesco. A Definition that Could not Work: The EU Framework Decision on the Fight against Organised Crime / Francesco Calderoni // European Journal of Crime, Criminal Law and Criminal Justice. – 2008. – 16. – P. 265–282.

160. Carlin, J. P. Detect, disrupt, deter: A whole-of-government approach to national security cyber threats / J. P. Carlin // Harvard national security journal. – Cambridge, 2016. – Vol. 7. – P. 414.

161. Charvat, J. P. I. A. G. Cyber Terrorism: A New Dimension in Battlespace, CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM 7 (2009) / J. P. I. A. G. Charvat. – URL: http:// www.ccdcoe.org/publications/virtualbattlefield/05_CHARVAT_Cyber%20Terrorism.pdf (дата обращения: 18.07.2024). – Текст: электронный.

162. Cheng V Governor of Pentonville Prison (1973) A.C. 931, 945 H. L.; Ex Parte Schtraks (1964) AC 556, at 583 HL; and Schtraks V Government of Israel (1964) AC 556, 582–584.

163. Cryptography is the study and practice of securing information and communications to circumvent unauthorized access and safeguard the integrity of information //. Lawyard Journal. – (2020). – P. 25.

164. Csonka, Peter. The Council of Europe Convention on cyber-crime: A response to the challenge of the new age? / Peter Csonka // Cybercrime: Conferenza internazionale. La Convenzione del Consiglio d'Europa sulla Criminalità Informatico. – Ed. Giovanni Ilarda and Gianfranco Marullo, 3-29. – Milano: Giuffrè, 2004. – P. 10–14.

165. Daskal, J. Budapest Convention: What is it and how is it being Updated? / J. Daskal, D. Kennedy-Mayo // Cross Border Data Forum. – (2020). – URL: https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it- being-updated/ (дата обращения: 18.07.2024). – Текст: электронный.

166. Deflem. International Police Co/operation – History / Deflem // The Encyclopedia of Criminology. – New York, 2005. – P. 795–798.

167. Denning, D. E. Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Networks and netwars: The future of terror, crime, and militancy / D. E. Denning // – 2001. – P. 239, 288.

168. Diakonia. What Should a State do if it Violates International Law / Diakonia. – 2020. – URL: https://www.diakonia.se/en/IHL/The-Law/Internationl-Law1/Enforcement-of-IL/What-should-a-state-do-if-it- violates-IL/ (дата обращения: 18.07.2024). – Текст: электронный.

169. Downing, R. W. Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime / R. W. Downing // Columbia Journal of Transnational Law. – 2005. – № 3. – P. 43.

170. Duggan, M. Online harassment / M. Duggan // URL: http://www.pewinternet.org/2014/10/22/part-1-experiencing-online- harassment/ (дата обращения: 18.07.2024). – Текст: электронный.

171. Dunn, M. A Comparative Analysis of Cybersecurity Initiatives Worldwide. – 2005. – P. 4.

172. Flanagan, Aanne. The law and computer crime: Reading the Script of Reform / Anne Flanagan // International Journal of Law and Information Technology, 13. – 2005. – №. 1: 98–117.

173. Gabriel Weimann, Gabriel. Cyberterrorsim: The Sum of All Fears? 28 STUD / Gabriel Weimann // CONFLICT & TERRORISM. – 2005. – 129, 130), cited in Clive Walker, Cyber-Terrorism: Legal Principle and Law in the United Kingdom, 110 PENN ST. L. REV., 625, 634 – (2006).

174. Gala, J. How Cybercrime Affects International Relations / J. Gala // Stanford Management, Science and Engineering. – 2017. – URL: https://mse238blog.stanford.edu/2017/07/jugal23/how-cyber-crime-affects-international- relations/ (дата обращения: 18.07.2024). – Текст: электронный.

175. Gibson &Miralis. The Five Key Challenges of Law Enforcements in Fighting Cybercrime / Gibson &Miralis // NGM. – 2021.

176. Haataja, Samuli. Cyber Attacks and International Law on the Use of Force / Samuli Haataja // Emerging Technologies, Ethics and International Affairs. – 2020. – P. 2.

177. Hague Programme / Anne Weyembergh // Common Market Law Review. – 2005. – P. 42.

178. Herjavec, R. Cybersecurity CEO: The History of Cybercrime, from 1834 to Present / R. Herjavec //. Cybercrime Magazine. – 2019. – July 17. – URL: https://cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/ (дата обращения: 18.07.2024). – Текст: электронный.

179. Hogben, G. Botnets: Detection, Measurement, Disinfection and Defence. European Network and Information Security Agency (ENISA) / G. Hogben (ed.). 2011. – P. 97-115.

180. Holt, Thomas J. Cybercrime and Digital Forensics: An Introduction / Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar. – 2018. – P. 42.

181. Huey, L. ‘Uppity Civilians’ and ‘Cyber-Vigilantes’: The role of the public in policing cyber-crime / L. Huey, J. Nhan, R. Broll // Criminology and

Criminal Justice. – 2013. – Vol. 13. – № 1. – P. 81–97. DOI: 10.1177/1748895812448086.

182. INTSIGHTS, «The Dark Side of Latin America: Cryptocurrency, Cartels, Carding and the Rise of Cybercrime». – P. 6. – // URL: https://wow.intsights.com/rs/071-ZWD- (дата обращения: 18.07.2024). – Текст: электронный.

183. ITU High Level Experts Group (HLEG). – 2008. – P. 27. – // URL: http://www.itu.int/cybersecurity/gca/ (дата обращения: 18.07.2024). – Текст: электронный.

184. Jahangiri, Ali. Cyberspace, Cyberterrorism and Information Warfare: A Perfect Recipe for Confusion / Ali Jahangiri // WORLDWIDE SECURITY CONFERENCE 6: BACKGROUND MATERIALS AND SELECTED SPEAKER'S NOTES. – 2009. – 29.

185. James, A. Lewis. The Internet and Terrorism, 99 AM / A. Lewis James // SOC'Y INT'L L. 112, 114 (2005) One of the characteristics of terrorist websites is their ability to manage rapid changes of Internet addresses. When authorities force a site to move, informal networks based on chatrooms or e-mail inform the group's supporters of the new network address. – 112, 114.

186. Jensen, Eric Talbot. The Tallinn Manual 2.0: Highlights and Insights / Eric Talbot Jensen; Brigham Young University School of Law. – 2017. – P. 746.

187. Journal of Law Reform, 1, 445–471. – URL: http://www.jura.uni-muenchen.del/ (дата обращения: 18.07.2024). – Текст: электронный.

188. Kenichi, T. The Role of INTERPOL in the Fight against Cybercrime INTERPOL NCRP for Computer Related Crime, being a paper presented at 3rd Facilitation Meeting for WSIS Action Line C5 Geneva / T. Kenichi. – 2008. – P. 645.

189. Ladan, M. T. Overview of the 2015 Legal and Policy Strategy on Cybercrime and Cybersecurity in Nigeria / M. T. Ladan // Prof. M. T. Ladan's Law and Policy Review Research Working Papers, Faculty of Law, Ahmadu Bello University. – 2015. – P. 2.

190. Lokwani, P. Do You Know About Strange I LOVE YOU Virus? / P. Lokwani // Procaffenation. – 2020. – URL: https://procaffenation.com/know-about-strange-i-love-you/ (дата обращения: 18.07.2024). – Текст: электронный.

191. Lotrionte, C. State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights / C. Lotrionte // Emory International Law Review. – URL: https://law.emory.edu/eilr/content/volume-26/issue- 2/symposium%20/state-sovereignty-self-defense-in-cyberspace.html/ (дата обращения: 18.07.2024). – Текст: электронный.

192. Malwarebytes Lab «When Artificial Intelligence goes awry: separating science fiction from fact», without publication date. – URL: https://resources.malwarebytes.com/files/2019/06/Labs-Report-AI-gone-awry.pdf/ (дата обращения: 18.07.2024). – Текст: электронный.

193. Maras, Marie-Helen. *Computer Forensics: Cybercriminals, Laws and Evidence,* second edition. Jones and Bartlett / Marie-Helen Maras. – 2014. – P. 357.

194. Martin, James. Lost on the Silk Road: online drug distribution and the «cryptomarket» / James Martin. // Criminology and Criminal Justice. – 2014. – Vol. 14 (3). – 351–367.

195. Maura Conway, Maura. Terrorism and IT: Cyberterrorism and Terrorist Organisations Online 6 / Maura Conway (paper prepared for presentation at the International Studies Association Annual International Convention in Portland, Oregon). – 2012. – P. 458.

196. Maurer, T. Cyber Proxies and Their Implications for Liberal Democracies / T. Maurer // The Washington Quarterly. – 2018. – Vol. 41. – Issue 2. // – URL: https://www.tandfonline.com/doi/abs/ (дата обращения: 18.07.2024). – Текст: электронный.

197. Mercado Kierkegaard, Sylvia. Here comes the «cybernators!» / Sylvia Mercado Kierkegaard // Computer Law & Security Report, 22. – 2006. – № 5. – P. 381–391.

198. Mitliaga, Varvara. Cyber-terrorism: A Call for Governmental Action? / Varvara Mitliaga // BRITISH AND IRISH LAW, EDUCATION & TECHNOLOGY

ASSOCIATION 5 (2001). – URL: http://www. bileta.ac.uk/01papers/mitliaga.html (дата обращения: 18.07.2024). – Текст: электронный.

199. Miquelon-Weismann, Miriam F. The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process? / F. Miriam Miquelon-Weismann // John Marshall Journal of Computer & Information Law, 23. – 2005. – № 2: 329–61. – P. 353.

200. MIT Technology Review, «Transforming the Energy Industry with AI». – 2021. – URL: https://www.technologyreview.com/2021/01/21/1016460/ (дата обращения: 18.07.2024). – Текст: электронный.

201. Noor, Elina. The Problem with Cyber Terrorism / Elina Noor // 2 SOUTHEAST ASIA REGIONAL CTR. FOR COUNTER-TERRORISM. – 2011. – 51, 52.

202. Norbutas, Lukas. Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network / Lukas Norbutas // International Journal of Drug Policy. – (2018). – Vol. 56. – P. 92–100.

203. Orji, U. J. Cybersecurity Law and Regulation / U. J. Orji. – 1 Wolf Legal Publishers. – 2012.

204. Owens, William A. Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities / William A. Owens and others eds. // National Academies Press. – 2009. – 10–11.

205. Parker, D. B. Computer crime Criminal Justice Resource Manual / D. B. Parker // Cambridge, Mass.; Department of Justice. – 1989. – 223 p.

206. Peter, A. S. Cyber resilience preparedness of Africa's top 12 emerging economies / A. S. Peter // International Journal of Critical Infrastructure Protection. – 2017. – Vol. 17. – P. 49–59.

207. Przepiorka, Wojtek, Przepiorka. Lukas Norbutas, and Rense Corten. Order without law: Reputation promotes cooperation in a cryptomarket for illegal drugs / Wojtek Przepiorka, Lukas Norbutas and Corten. Rense // European Sociological Review. – 2017. – Vol. 33(6). – P. 752–764.

208. Raghay, S. S. Cyber Security in India's Counter Terrorism Strategy, INTEGRATED DEFENSE STAFF 2 (Sept. 15, 2012) / S. S. Raghay. – URL: ids.nic.in/art_by_offids/Cyber security in india by Col SS Raghav.pdf (дата обращения: 18.07.2024). – Текст: электронный.

209. Republic of Kenya in the High Court of Kenya at Nairobi Milimani Law Courts Constitutional and Human Rights Division Petition. – 2015. – № 149.

210. Schjolberg, Stein. The history of cybercrime (third edition) / Stein Schjolberg. – 2020. – P. 25.

211. Schjolberg, Stein. The History of Global Harmonization on Cybercrime Legislation / Stein Schjolberg // The Road to Geneva. – 2008. – URL: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (дата обращения: 18.07.2024). – Текст: электронный.

212. Schmitt, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / Michael N. Schmitt (ed.). – 2nd ed. – Cambridge University Press. – 2017. – P. 330.

213. SHIRYAEV, YAROSLAV. Cyberterrorism in the Context of Contemporary International Law / YAROSLAV SHIRYAEV. – 2012. – P. 167.

214. Sieber, U. Memorandum on a European Model Penal Code / U. Sieber. – 1997. – P. 2.

215. Smith, R. G. Cyber Criminals on Trial / R. G. Smith, P. Grabosky, G. Urbas. – Cambridge: Cambridge University Press, 2004. – 263 p.

216. Sofaer, Abraham D. A Proposal for an International Convention on Cyber Crime and Terrorism 26 (Aug. 2000) (paper presented at the Stanford Conference at Stanford University), available at / Abraham D. Sofaer et al. – URL: http://iis-db.stanford.edu/pubs/11912/sofaer goodman.pdf (дата обращения: 18.07.2024). – Текст: электронный.

217. Stahl, W. M. [Электронный ресурс] / W. M. Stahl. – URL: http://interlaws.ru/kiberbezopasnost-i-mezhdunarodnoe-pravo/ (дата обращения: 18.07.2024). – Текст: электронный.

218. Stanford Encyclopedia of Philosophy. Theories of Criminal Law. – 2018. – URL: https://plato.stanford.edu/entries/criminal-law/ (дата обращения: 18.07.2024). – Текст: электронный.

219. Stein, J. (2012). Recommendations for Potential New Global Legal Mechanisms Against Global Cyber Attacks and Other Global Cybercrimes // A Paper for the East West Institute (EWI) Cybercrime Legal Working Group. – 2012.

220. Studying illicit drug trafficking on Darknet markets: Structure and organization from a Canadian Perspective / Broseus, Julian Broseus, Damien Rhumorbarbe Damien, Caroline Mireault Caroline, Vincent Ouellette, Frank Crispino, and David Decary-Hetu... at al. // Forensic Science International. – 2016. – Vol. 264, 7–14.

221. Techopedia. Cybercrime. – URL: https://www.techopedia.com/definition/2387/cybercrime/ (дата обращения: 18.07.2024). – Текст: электронный.

222. The History of Cybercrime by Stein Schjolberg. – 2020. – P. 51.

223. Turing, A. M. (1950) Computing Machinery and Intelligence. Mind / A. M. Turing. – Mind 1950. – 49: 433–460.

224. US Department of Justice. (2017). Gun traffickers arrested for allegedly using the Dark Net to export guns across the world. US Attorney's Office, Northern District of Georgia.

225. Vermeulen, Gert. Where do we currently stand with harmonisation in Europe? / Gert Vermeulen // Harmonisation and harmonising measures in criminal law / edited by André H. Klip and Harmen G. van der Wilt, 65-76. – Amsterdam: Royal Netherlands Academy of Science, 2002.

226. WALL. Cybercrime: The Transformation of Crime in the Information Age 160 / WALL. – 2007.

227. Wilson, Clay. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress / Clay Wilson. – 2008. – P. 4.

VIII. Интернет-ресурсы

228. Библиотека Организации Объединенных Наций. // – URL: https://www.un.org/library (дата обращения: 18.07.2024). – Текст: электронный.

229. Международный союз электросвязи. // – URL: http://www.itu.int/ru/about/ (дата обращения: 18.07.2024). – Текст: электронный.

230. Официальный сайт МИД России. // – URL: http://mid.ru (дата обращения: 18.07.2024). – Текст: электронный.

231. Справочная правовая система «КонсультантПлюс». Версия Проф. // – URL: https://www.consultant.ru (дата обращения: 18.07.2024). – Текст: электронный.

232. Справочно-правовая система «Гарант». // – URL: https://www.garant.ru/?ysclid=m3lawsyuk2892327754 (дата обращения: 18.07.2024). – Текст: электронный.

233. European Telecommunication Standards Institute. // – URL: https://www.etsi.org/ (дата обращения: 18.07.2024). – Текст: электронный.

234. United Nations Office of Information and Communications Technology. // – URL: https://unite.un.org/information-security (дата обращения: 18.07.2024). – Текст: электронный.

235. United Nations Office on Drugs and Crime. // – URL: https://www.unodc.org (дата обращения: 18.07.2024). – Текст: электронный.