DOI: 10.48137/2074–2975_2024_6_69
УДК 327. 343.9+004

Международный диалог по проблеме высокотехнологичной преступности

Иван СУРМА
Дарья КАРАСЕВА

Значимость информации в мировом политико-экономическом сообществе за последние десятилетия многократно увеличилась. Драйвером данной тенденции стала стихийная инфильтрация информационно-коммуникационных технологий в массовое пользование. Человечество столкнулось с необходимостью обработки больших объёмов данных (*big data)*, а информация стала одной из движущих сил как научно-технологического прогресса, так и военно-политического и социально-экономического развития.

Однако бесконтрольные возможности, легкодоступность информации, практичность и неограниченное количество данных разного уровня создают наиболее благоприятные условия для неправомерных действий в цифровой среде. Киберпреступность сейчас распространяется быстрее, чем традиционная преступность, поскольку она легче в плане реализации и в какой-то степени безопаснее, так как лично в интернет-сети никто не встречается, а тотальная анонимность содействует криминалу.

СУРМА Иван Викторович – кандидат экономических наук, доцент, доцент кафедры международной и национальной безопасности Дипломатической академии МИД России, вице-президент АНО «Национальный институт исследований глобальной безопасности», член Национальной ассоциации международной информационной безопасности. *SPIN-код:* 4592-8693, *E-mail:* isurma@yandex.ru

КАРАСЕВА Дарья Максимовна – стажёр Национальной ассоциации международной информационной безопасности. *SPIN-код:* 5239-0237, *E-mail:* dashakara@yandex.ru

Ключевые слова: киберпреступность, конвенция ООН, искусственный интеллект, международное сотрудничество.

Высокотехнологичная преступность в России

Сравнение уровня преступности в традиционном смысле этого термина и киберпреступности в России в 2023 г. иллюстрирует серьёзность проблемы неправомерного использования информационно-коммуникационных технологий (ИКТ).

По данным российского МВД, в январе–ноябре 2023 г. зарегистрировано 1804,8 тыс. преступлений, или на 1% меньше, чем за аналогичный период прошлого года [1], из них 614 782 тыс. преступлений совершено с использованием ИКТ или в сфере компьютерной информации (по сравнению с прошлым годом количество киберпреступлений в России увеличилось на 30,8%), что составляет 34% от общего числа преступлений.

7 февраля 2024 г. начальник департамента проблем безопасности в информационной сфере аппарата Совета безопасности России А. Петров сказал, что «Интернет превратился из безопасной среды и экономической среды развития суверенных стран в арену противодействия и политического противостояния. Только за 2023 г. в отношении информационной инфраструктуры Российской Федерации было около 200 тысяч наиболее опасных компьютерных атак» [2].

Таким образом, количество высокотехнологичных преступлений не превышает уровня традиционных преступлений, но при этом за последние годы выявлена тенденция по снижению общего количества преступлений и резкого повышения киберпреступлений. Киберпреступность, в свою очередь, является критической угрозой для информационной безопасности государств[3], и особенно злободневной данная тема воспринимается на международном уровне, когда безнаказанно воруют крупные суммы денег, *NFT*-собственность, взламывают стратегически важные информационные системы с целью кражи информации особой важности[4].

Статистика высокотехнологичной преступности в мире

В контексте актуальной общемировой статистики киберпреступности можно выделить два фактора:

– *во-первых,* количество кибератак экспоненциально возросло с началом пандемии *COVID-19* из-за перехода на удалённую работу и онлайн-обучение большого количества людей, что привело к многократному увеличению онлайн-транзакций и использованию веб-приложений. Киберпреступниками были использованы методы фишинга и мошенничества по большей части в отношении лекарств и вакцин, а также персональных данных и кражи денег;

[1] Доклад Министерства внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр» о состоянии преступности в России за январь-ноябрь 2023 г. // URL: https://media.mvd.ru/files/application/5040806

[2] На Россию за год совершено 200 тысяч мощных кибератак, заявили в Совбезе // URL: https://ria.ru/20240207/kiberataka-1925871562.html

[3] *Kirilenko V.P., Alekseev G.V.* Cybercrime and Digital Transformation. Theoretical and Applied Law. 2021. № 1. P. 39–53.

[4] Ibid. P. 39.

– *во-вторых*, важной вехой в резком увеличении числа киберпреступников и их возможностей в киберпространстве (использование технологий искусственного интеллекта и др.) стал украинский конфликт.

В табл. 1 представлена динамика роста кибератак с 2020 по 2023 г.

Независимый блог по киберпреступности и информационной безопасности *Hackmageddon*, руководимый П Пассери*, публикует раз в две недели статистику по кибератакам.

По итогам 2023 г. было совершено 4128 кибератак, что на 35% больше по сравнению с 3074 кибератаками в 2022 г.**

Таблица 1

Ежемесячное сравнение кибератак с 2020 по 2023 г.

Месяцы	По годам, количество			
	2020	2021	2022	2023
Январь	160	185	200	281
Февраль	191	255	205	325
Март	187	279	260	335
Апрель	145	243	222	347
Май	187	177	240	338
Июнь	194	212	243	355
Июль	192	187	284	385
Август	205	173	310	342
Сентябрь	214	207	287	381
Октябрь	231	198	275	376
Ноябрь	199	206	275	393
Декабрь	227	217	273	260

Учитывая именно подобное увеличение незаконных действий в киберпространстве в мире необходимо единство международного сообщества в разработке нормативно-правовых актов и их реализации для противодействия международной киберпреступности.

* Работает старшим инженером по продажам и директором по киберразведке в компании Netskope, имеющей филиалы в Великобритании, Сингапуре, Испании, Индии, Японии, Австралии и Тайване.

** Таблица составлена авторами на основании данных Cyber Attacks Statistics. 2023 Cyber Attacks Statistics // Hackmageddon // URL: https://www.hackmageddon.com/2024/03/26/2024-cyber-attacks-statistics/

Типы высокотехнологичной преступности

Фундаментальные знания о высокотехнологичной преступности и киберпреступности тесно взаимосвязаны между собой, но имеют различия практического характера.

Для дифференциации двух понятий необходимо обратиться в первую очередь к более многогранному термину «информационная безопасность» (ИБ), который означает сохранение конфиденциальности, целостности и доступности информации[5]. Многие ошибочно относят информационную безопасность исключительно к сфере высоких технологий, Интернету и киберпространству, однако именно информационный аспект чётко прослеживается в дефиниции ИБ, что синонимично вопросу о безопасности данных. Не секрет, что большая часть данных и информации хранится в киберпространстве, но не стоит забывать и про информацию в офлайн-режиме.

Параллельно с информационной безопасностью выделяют понятие «кибербезопасность» (иногда её называют компьютерной безопасностью), которое, как правило, представляется в двух определениях:

1) кибербезопасность – это безопасность защищаемого объекта, системы которого функционируют в условиях деструктивных информационных воздействий;

2) кибербезопасность – это действие, необходимое для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли или повреждения критических систем или информационных объектов[6, 7].

Таким образом, информационная безопасность и кибербезопасность являются разными терминами.

Информационная безопасность охватывает все аспекты, связанные с защитой конфиденциальной информации, включая управление доступом, шифрование данных, защиту от утечек информации и т. д.

Кибербезопасность, напротив, ориентирована на защиту компьютерных систем, сетей и данных от кибератак. Она включает в себя защиту от вирусов, хакерских атак, фишинга и других видов киберугроз.

Информационная безопасность шире кибербезопасности.

Кибербезопасность соотносится с двумя понятиями, относящимися к незаконным действиям в Интернете: киберпреступность и высокотехнологичная преступность. Между ними также есть различия.

Высокотехнологичная преступность (*high-tech crime*), или преступность в сфере высоких технологий, определяется как деяние, предполагающее активное использование современных технических средств

[5] Национальный стандарт ГОСТ Р ИСО/МЭК 27000-2021 // URL: https://docs.cntd.ru/document/1200179675

[6] Kaspersky Industrial CyberSecurity. Что будет завтра с кибербезопасностью в промышленности? // URL: https://neftegaz.ru/analisis/companies/630587-kaspersky-industrial-cybersecurity-chto-budet-zavtra-s-kiberbezopasnostyu-v-promyshlennosti/

[7] Национальный стандарт ГОСТ Р 56205-2014 (IEC/TS 62443-1-1:2009) // URL: https://docs.cntd.ru/document/1200114169

и методов в преступной деятельности[8]. Однако существует тонкая грань между преступлениями, направленными на сами технологии, и преступлениями, совершёнными с помощью технологий, т. е. выделяются два вида высокотехнологичных преступлений, а именно:

– киберзависимые преступления (*cyber dependent crimes*). Это вид преступлений, направленных на информационные технологии, например, взлом баз данных, вывод из строя веб-сайтов;

– киберпреступления (*cyber enabled crimes* или *cybercrimes*). Это традиционные преступления, в которых ИТ играют важную роль, например, интернет-мошенничество и киберпреследование[9].

Таким образом, высокотехнологичная преступность охватывает больший диапазон преступной деятельности, связанной с использованием передовых технологий. В эту категорию входят такие преступления, как контрафакт, кража интеллектуальной собственности и использование сложного оборудования для совершения таких преступлений, как кража со взломом или ограбление.

Киберпреступность относится к преступной деятельности, совершаемой с использованием компьютеров или Интернета (хакерство, кража личных данных, онлайн-мошенничество и другие незаконные действия, совершаемые с помощью новых технологий). На рис. представлено измерение кибербезопасности и информационной безопасности в контексте высокотехнологичной преступности, указаны виды преступности и распространённые методы противоправных деяний.

Преступления, которые совершаются людьми в обычной жизни (кражи, мошенничества и пр.), приобретают киберпереориентацию в XXI в. и носят гибридный характер, сочетая традиционные методы преступлений с потенциалом и возможностями современных технологий.

Так, например, 17-летний китайский студент, учившийся по обмену в США, пропал без вести и был спасён, хотя и почти замёрз до смерти в палатке за пределами Солт-Лейк-Сити.

Правоохранительные органы объяснили, что подросток сбежал из дома 28 декабря после того, как киберпреступники убедили его, что его семье в Китае угрожают, и убедили «похитить себя» (*cyber kidnapping*).

Его семья сообщила полиции, что заплатила выкуп в размере 80 тыс. долл. после того, как Чжуан прислал им фотографию, свидетельствующую о том, что его удерживают против его воли.

Обычно при киберпохищениях преступники звонят или отправляют сообщения жертве, чтобы обмануть её и заставить думать, что её близкий человек похищен, хотя на самом деле он находится в безопасности[10].

---

[8] *Смольянинов Е.С., Долинко В.И.* Высокотехнологичная преступность как угроза экономической безопасности // Уголовная политика России на современном этапе: состояние, тенденции, перспективы Сб. ст. Междунар. науч.-практич. конференции. М.: Изд-во Академия управления Министерства внутренних дел Российской Федерации, 2018. С. 140.

[9] *Schiks J.A.M., Weijer E. van de, Leukfeldt R.L.* High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals // Computers in Human Behavior. 2022. № 126. – 8 p.

[10] Kai Zhuang: Chinese teen found alive in US after «cyber kidnapping» // URL: https://www.bbc.com/news/world-us-canada-67861852

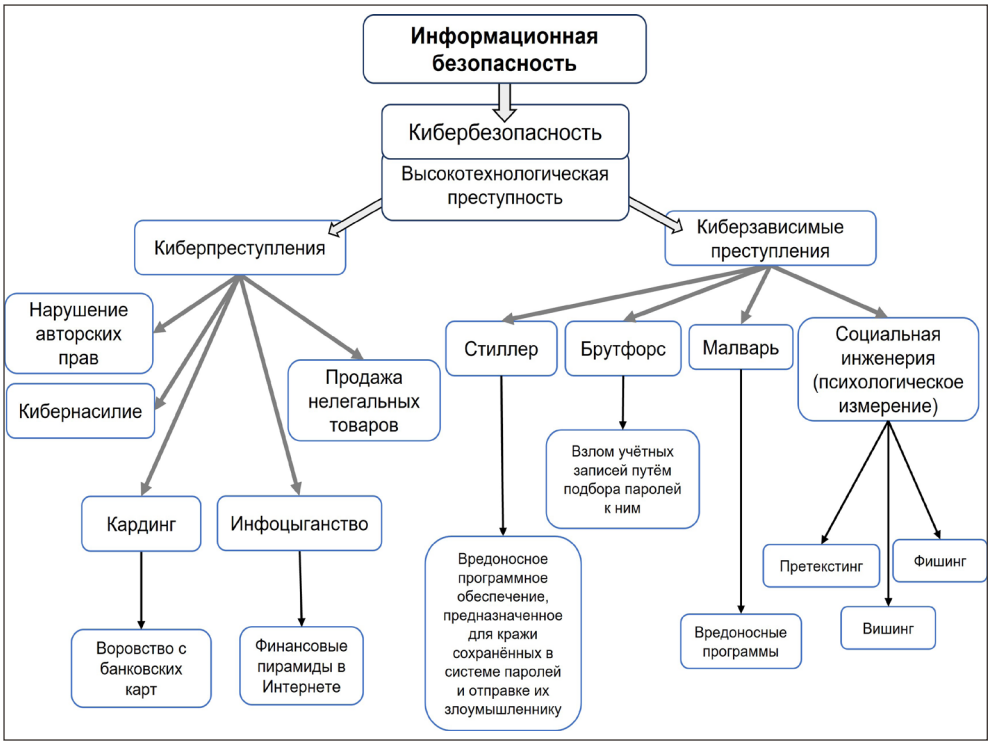

Рис. Информационная безопасность и кибербезопасность в контексте высокотехнологичной преступности

Международный обзор киберпреступности в современном мире

Согласно блогу *Hackmageddon*, в международных киберпреступлениях в 2023 г. самыми популярными инструментами для киберпреступлений стали: малварь (*malware*, вредоносное программное обеспечение, имеющее своей целью в той или иной форме нанести ущерб пользователю или компьютеру и его содержимому); повышенная уязвимость информационных систем; атака с захватом аккаунта (табл. 2).

Такие злоумышленники обладают определённым уровнем опыта и достаточными ресурсами для проведения своих кампаний в течение длительного времени. Они могут адаптировать, корректировать или совершенствовать свои атаки, чтобы противостоять защитным средствам как отдельной жертвы, так и корпорации или даже целого государства.

В этой связи возникают вопросы относительно правосудия против незаконных действий с помощью технологий и остальных проблем, появляющихся при расследовании совершённых преступлений.

Таблица 2

Техники кибератак за 2023 год*

Инструменты киберпреступлений	% от общего числа
Malware – вредоносные программы	35,9
Vulnerability – уязвимость	16,3
Account Takeover – захват аккаунта	9,2
Targeted Attack – целенаправленное нападение	7,0
DDoS – атаки	3,8
Scam – мошенничество	1,7
Coordinated Inauthentic Behavior – скоординированное неаутентичное поведение	1,6
Misconfiguration – ошибка конфигурации	0,9 %
Malicious script injection – внедрение вредоносных программ	0,6 %
Other – другие	3,1 %
Unknowen – неизвестные	19,9 %

Можно выделить несколько наиболее важных проблем в области международного сотрудничества по вопросам противодействия киберпреступности:

– отсутствие чёткого алгоритма сотрудничества между странами по вопросам противодействия киберпреступности;

– отсутствие комплементарности в национальных законах по вопросам киберпреступлений и киберзависимых преступлений;

– недостаток соответствующих *IT*-специалистов в области кибербезопасности;

– несовершенство технологий и проблема интероперабельности данных.

Подобные сложности возникают из-за низкого уровня транспарентности процессов в интернет-сети; особенностей киберпространства и неосведомлённости сотрудников правоохранительных органов о возможных выходах в даркнет. Кроме того, существуют сложности государственно-частного партнёрства в этой сфере. Диалог государства и бизнеса по вопросам кибератак мог бы дать варианты повышения эффективности предотвращения будущих высокотехнологичных преступлений, а сложность диалога строиться на:

– нежелании бизнес-структур сотрудничать с государством;

– плохой репутации государственных органов, активно распространяющейся в социальных сетях.

Ещё одной проблемой обеспечения кибербезопасности в условиях развития высокотехнологичной преступности становится обычный

* Таблица составлена авторами на основании данных Cyber Attacks Statistics. 2023 Cyber Attacks Statistics // Hackmageddon // URL: https://www.hackmageddon.com/2024/03/26/2024-cyber-attacks-statistics/

блок домена сайта с противоправной деятельностью, поиск лиц, задействованных в преступлении, либо упускается, либо невозможен из-за хорошо скрываемой личности в интернет-сети. В дальнейшей перспективе хакеры будут создавать новые сайты, приложения и развивать иные способы реализации своей противоправной деятельности. При этом ещё одна проблема для государства заключается в том, чтобы, как минимум на законодательном уровне, отделить зёрна от плевел, т. е. чтобы правоохранительные органы смогли, не дискредитируя добросовестных пользователей, заблокировать любой аккаунт или сайт, созданные злоумышленниками.

Спектр возможного ущерба от киберпреступлений варьируется от всевозможных экономических и финансовых потерь до социально-психологических проблем в обществе. Однако существуют более серьёзные угрозы, связанные с кибератаками, которые могут привести к военным нападениям, взрывам на атомных станциях, выводу из строя энергосетей и разрушению всей технологической инфраструктуры государства.

Появились, в частности, такие новые угрозы, как сетевой терроризм, хактивизм (*hacktivism*)*; вмешательство во внутренние дела государства; влияния на выборы. Поэтому важен диалог между странами для разработки норм и правил по предотвращению киберпреступлений.

Международно-правовые подходы к борьбе с киберпреступностью

Долгие годы после разработки под эгидой Совета Европы Конвенции о преступности в сфере компьютерной информации *ETS* № 185 (Будапешт, 23 ноября 2001 г.)[11] и ратификации этого соглашения странами – членами Совета Европы этот документ являлся одним из первых и основных элементов борьбы с киберпреступностью на международной арене.

Чуть позже был принят дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, касающийся введения уголовной ответственности за правонарушения, которые связаны с проявлением расизма и ксенофобии, совершённые с помощью компьютерных систем *ETS* № 189 (Страсбург, 28 января 2003 г.)[12]. Этот протокол распространил действие Конвенции на правонарушения экстремистской направленности.

Будапештская конвенция охватывает такие вопросы, как: наруше-

[11] https://www.coe.int/en/web/cybercrime/home

[12] Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем (СЕД № 189) // URL: https://www.coe.int/ru/web/conventions/full-list?module=treaty-detail&treatynum=189

* Слияние двух слов «хакер» и «активизм» – использование незаконными способами компьютеров и компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации.

ние авторских прав, компьютерные мошенничества, детская порнография и нарушение безопасности сети. Кроме того, Конвенция содержит ряд полномочий и процедур, таких как обыск и арест хранящихся компьютерных данных.

Хотя большинство положений Будапештской конвенции стало широко признанными нормами обычного международного права, но Российская Федерация не участвует в Конвенции о преступности в сфере компьютерной информации. Россия не является ни подписантом, ни участником данного документа в связи с тем, что считает Будапештскую конвенцию инструментом вмешательства во внутренние дела других государств и нарушения их суверенитета.

В частности, в ст. 32 (b) указано «Трансграничный доступ к хранящимся компьютерным данным с согласия или при наличии открытого доступа участник Конвенции может без разрешения другого участника получать доступ через компьютерную систему на своей территории хранимые компьютерные данные, находящиеся у другого участника Конвенции, если участник Конвенции получает законное и добровольное согласие лица, имеющего правовые полномочия на раскрытие данных другому участнику через эту компьютерную систему» [13].

В 2017 г. Россия предложила альтернативу Будапештской конвенции и направила письмо в Организацию Объединённых Наций, содержащее проект Конвенции о сотрудничестве в сфере противодействия информационной преступности [14]. Лишь через два года Генеральная Ассамблея ООН приняла эту резолюцию, подписантами которой выступили: Россия, Белоруссия, Камбоджа, Китай, Иран, Мьянма, Никарагуа, Сирия и Венесуэла. Резолюция была негативно встречена США, ЕС и их сторонниками [15].

В том же году был создан Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (*Ad Hoc Committee*).

С 2021 г. Комитет провёл шесть сессий по обсуждению Конвенции, не считая организационные сессии и межсессионные консультации.

С 29 января по 9 февраля 2024 г. прошла заключительная сессия Комитета по разработке Конвенции. Ожидалось, что после сессии будет принята итоговая всеобъемлющая Конвенция по борьбе с киберпреступностью на уровне ООН, но комитету не хватило десяти дней для обсуждения документа.

8 февраля 2024 г. стало известно решение комитета возобновить свою работу позднее [16].

От лица России в разработке Конвенции участвовали представители МИД России, в частности

[13] Будапештская конвенция о киберпреступности // URL: https://rm.coe.int/1680081561

[14] Россия внесла в ООН свой проект конвенции по борьбе с киберпреступностью // URL: https://www.rbc.ru/rbcfreenews/610021049a7947c17a15e6df

[15] Хронология обсуждений Конвенции ООН о киберпреступности // URL: https://www.eff.org/ru/deeplinks/2023/04/un-cybercrime-treaty-timeline

[16] Управление ООН по наркотикам и преступлениям, Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, проект решения. A/AC.291/L.13 // URL: https://documents.un.org/doc/undoc/ltd/v24/008/23/pdf/v2400823.pdf?token=Bg815v6xCdjy4FJIUP&fe=true

Департамент международной информационной безопасности (ДМИБ), изначально главой делегации был директор ДМИБ А.Р. Люкманов, но США отказали в выдаче визы главе российской делегации, и вместо директора ДМИБ выступал главный советник ДМИБ А.А. Акульчев.

На заключительных этапах подготовки Конвенции возникло множество противоречий между государствами. М.И. Ульянов, постоянный представитель Российской Федерации при международных организациях в Вене, считает, что страны коллективного Запада под различными предлогами стремятся как можно больше сузить сферу охвата соглашения, они продвигают в текст сомнительные «правочеловеческие» положения, недобросовестное применение которых способно существенно снизить эффективность борьбы с преступностью в сфере ИКТ[17].

Сегодня ряд экспертов прогнозируют два варианта развития дальнейших событий:

– в рамках заключительной сессии разногласия будут сглажены, и подписанты Конвенции примут документ, который будет устраивать всех;

– Россия, Китай и другие государства дополнят Конвенцию региональными соглашениями, например, в рамках БРИКС, ШОС и т. д.[18]

Кроме того, существует целый ряд других институтов, которые занимаются вопросами киберпреступности, и могут выступать со своими предложениями и инициативами.

Среди них следует отметить:

– Европейский центр киберпреступности (*The European Cybercrime Centre – EC3 or ECi)* – орган Полицейского управления (Европол) Европейского союза со штаб-квартирой в Гааге, работает с сетевой безопасностью и борьбой с киберпреступностью, координирует трансграничную правоохранительную деятельность по борьбе с компьютерными преступлениями и выступает в качестве центра технической экспертизы по данному вопросу[19];

– Интерпол (*The International Criminal Police Organization*) – имеет специализированные программы и проекты по борьбе с киберпреступностью. Интерпол сотрудничает с правоохранительными органами 196 стран, обменивается информацией и разрабатывает совместные операции для пресечения киберпреступлений[20];

– Агентство Европейского союза по кибербезопасности (*The European Union Agency for Cybersecurity – ENISA*) – предоставляет консультации и экспертную поддержку государствам-членам, а также проводит исследования и разрабатывает рекомендации по борьбе с киберпреступностью[21];

– Контртеррористическое управление ООН – одним из направлений деятельности центра является кибербезопасность[22];

– Глобальный форум киберэкспертизы (*The Global Forum on Cyber Expertise – GFCE*) – многосторонняя платформа для сотрудничества и координации действий по повышению киберустойчивости и кибербезопасности в развивающихся странах и регионах. *GFCE* объединяет официальных представителей государств, международных организаций, частного сектора, академического сообщества и гражданского общества, которые работают над реализацией конкретных проектов

[17] Постпред РФ: Запад пытается «размыть» российский проект конвенции ООН по инфобезопасности // URL: https://tass.ru/politika/19702881

[18] Под статью подвели не всё // URL: https://www.kommersant.ru/doc/6452715

[19] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[20] https://www.interpol.int/

[21] https://www.enisa.europa.eu/

[22] https://www.un.org/counterterrorism/ru

и инициатив в пяти приоритетных областях: киберполитика, киберпреступность, кибернормы, кибермощь и кибersотрудничество.

GFCE был создан в 2015 г. на основе инициативы Нидерландов и поддержки Европейского союза и США[23].

В современном мире существует расхождение взглядов акторов мировой политики по вопросам использования информационно-коммуникационных технологий. Существующее недопонимание между государствами влияет на эффективность принятия решений. Так, вопрос о принятии Конвенции в сфере компьютерной информации о преступности оставался неразрешённым в течение четырёх лет после начала работы Специального комитета.

В соответствии с резолюцией 75/282 Генеральной Ассамблеи и решением 78/549 Генеральной Ассамблеи Специальный комитет по разработке всеобъемлющей Международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, учреждённый ещё в 2019 г. Генеральной Ассамблеей в её резолюции 74/247, провёл заключительную сессию Специального комитета (29 июля – 9 августа 2024 г., Нью-Йорк), на которой консенсусом был принят проект конвенции ООН против киберпреступности (A/AC.291/L.15).

Итоги сессии показали, что не все стороны остались довольны результатом переговоров. Во время работы заключительной сессии государства-члены не смогли достичь консенсуса относительно сферы охвата и терминологии Конвенции. Так, при разработке документа Россия придерживалась *всеохватывающего подхода*, например, предлагала существенно расширить перечень правонарушений с использованием информационно-коммуникационных технологий до 23 видов, а также выступала за использование в названии документа термина «информационная преступность» или «ИКТ-преступность», а не киберпреступность.

«Россия настаивает на криминализации широкого круга преступлений в информационном пространстве. Западники же под различными предлогами стремятся как можно больше заузить сферу охвата соглашения. К тому же они продвигают в текст сомнительные “правочеловеческие” положения, недобросовестное применение которых способно существенно снизить эффективность борьбы с преступностью в сфере ИКТ», – заявил Постоянный представитель России при международных организациях в Вене М.И. Ульянов[24].

США и страны Европы поддержали более *узкий подход*, сосредоточенный на компьютерно-сетевых преступлениях (киберпреступлениях).

Как итог, в проекте конвенции были согласованы только 10 видов подобного рода преступлений. В настоящее время ожидается имплементация конвенции в национальные законодательства государств-подписантов и практическая реализация установленных договорённостей между странами.

Многостороннее сотрудничество и возможность участия негосударственных акторов в работе над конвенцией свидетельствует о стремлении госу-

[23] https://thegfce.org/

[24] https://vk.com/wall-205039982_506

дарств мира к международному диалогу и координации действий в борьбе с киберугрозами и киберпреступностью. Рост киберпреступности как следствие легкодоступности информации создаёт серьёзные вызовы для информационной безопасности всех стран мира. Статистика высокотехнологичной преступности как в России, так и в мире показывает необходимость применения более эффективных мер по борьбе с этими угрозами. Поэтому разработка и реализация нормативно-правовых актов, а также международное сотрудничество становятся все более важными для обеспечения безопасности в цифровой среде.

Библиография • References

Будапештская конвенция о киберпреступности // URL: https://rm.coe.int/1680081561

[Budapeshtskaya konvenciya o kiberprestupnosti // URL: https://rm.coe.int/1680081561]

Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем (СЕД № 189) // URL: https://www.coe.int/ru/web/conventions/full-list?module=treaty-detail&treatynum=189

[Dopolnitel'nyj protokol k Konvencii o prestupleniyah v sfere komp'yuternoj informacii, ob inkriminirovanii rasistskih aktov i sovershennogo ksenofoba pri pomoshchi informacionnyh sistem (SED № 189) // URL: https://www.coe.int/ru/web/conventions/full-list?module=treaty-detail&treatynum=189]

Национальный стандарт ГОСТ Р 56205-2014 (IEC/TS 62443-1-1:2009) // URL: https://docs.cntd.ru/document/1200114169

[Nacional'nyj standart GOST R 56205-2014 (IEC/TS 62443-1-1:2009) // URL: https://docs.cntd.ru/document/1200114169]

Национальный стандарт ГОСТ Р ИСО/МЭК 27000-2021 // URL: https://docs.cntd.ru/document/1200179675

[Nacional'nyj standart GOST R ISO/MEK 27000-2021 // URL: https://docs.cntd.ru/document/1200179675]

Россия внесла в ООН свой проект конвенции по борьбе с киберпреступностью // URL: https://www.rbc.ru/rbcfreenews/610021049a7947c17a15e6df

[Rossiya vnesla v OON svoj proekt konvencii po bor'be s kiberprestupnost'yu // URL: https://www.rbc.ru/rbcfreenews/610021049a7947c17a15e6df]

Смольянинов Е.С., Долинко В.И. Высокотехнологичная преступность как угроза экономической безопасности // Уголовная политика России на современном этапе: состояние, тенденции, перспективы Сб. ст. Междунар. науч.-практич. конференции. М.: Изд-во Академия управления Министерства внутренних дел Российской Федерации, 2018. С. 139–141.

[*Smol'yaninov E.S., Dolinko V.I.* Vysokotekhnologichnaya prestupnost' kak ugroza ekonomicheskoj bezopasnosti // Ugolovnaya politika Rossii na sovremennom etape: sostoyanie, tendencii, perspektivy Sb. st. Mezhdunar. nauch.-praktich. konferencii. M.: Izd-vo Akademiya upravleniya Ministerstva vnutrennih del Rossijskoj Federacii, 2018. S. 139–141]

2023 Cyber Attacks Statistics // Hackmageddon // URL: https://www.hackmageddon.com/2024/03/26/2024-cyber-attacks-statistics/

Kai Zhuang: Chinese teen found alive in US after «cyber kidnapping» // URL: https://www.bbc.com/news/world-us-canada-67861852

Kaspersky Industrial CyberSecurity. Что будет завтра с кибербезопасностью в промышленности? // URL: https://neftegaz.ru/analisis/companies/630587-kaspersky-industrial-cybersecurity-chto-budet-zavtra-s-kiberbezopasnostyu-v-promyshlennosti/

Kirilenko V.P., Alekseev G.V. Cybercrime and Digital Transformation. Theoretical and Applied Law. 2021. № 1. P. 39–53.

Schiks J.A.M., Weijer E. van de, Leukfeldt R.L. High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals // Computers in Human Behavior. 2022. № 126. – 8 p.

https://rm.coe.int/1680081561

https://www.coe.int/en/web/cybercrime/home

Статья поступила 6 июля 2024 г.