ДОКЛАД ЭКСПЕРТА

ШЕСТОЙ КОМИТЕТ ГЕНЕРАЛЬНОЙ АССАМБЛЕИ

МОСКОВСКАЯ МЕЖДУНАРОДНАЯ МОДЕЛЬ ООН ИМ. В.И. ЧУРКИНА

ЗАЩИТА ПРАВ ЧЕЛОВЕКА В КОНТЕКСТЕ МАССОВОЙ ЦИФРОВОЙ СЛЕЖКИ, СБОРА И УТЕЧЕК ПЕРСОНАЛЬНЫХ ДАННЫХ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

«Нарушения прав человека — это нечто большее, чем личная трагедия. Они — как тревожный набат, который может возвещать о гораздо более серьёзном кризисе» — Пан Ги Мун, генеральный секретарь ООН.

В современную эпоху цифровые технологии стали необходимым компонентом человеческой жизни: существенная часть нашей активности перемещена в онлайн-пространство, что обусловливает массовое хранение персональных данных и их использование в цифровой среде. В условиях инновации сбор и обработка цифровых данных приобрели системный и всеобъемлющий характер. Вместе с тем, подобное цифровое развитие сопровождается утечкой этих самых данных и нарушением фундаментальных прав человека. В связи с этим, защита прав человека в цифровом пространстве становится жизненной необходимостью для сохранения свободы и достоинства личности в современных реалиях.

Актуальность рассматриваемой повестки обусловлена ее непосредственным влиянием как на интересы отдельного индивида, так и на мировое сообщество. Решение вопроса обеспечения защиты прав человека в условиях повсеместной цифровой слежки и утечки персональных данных требует всеобъемлющего международного сотрудничества.

Рассмотрение данного вопроса на международном уровне, в том числе на площадке ООН, позволит выработать эффективные и действенные меры по укреплению цифровой безопасности. Особое внимание необходимо уделить рискам, связанным с нарушением прав человека в условиях цифровизации — утечка и неправомерное использование персональных данных, ограничение доступа к информации, киберпреступность и кибершпионаж. Следование универсальным международным стандартам позволяет минимизировать эти риски и, в конечном итоге, обеспечить надежную защиту прав человека в цифровой среде.

ГЛАВА 1. КЛЮЧЕВЫЕ МЕЖДУНАРОДНЫЕ СОГЛАШЕНИЯ В ОБЛАСТИ ЦИФРОВЫХ ПРАВ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

За последние десятилетия было принято множество различных международных документов, направленных не только на урегулирование законодательства различных стран, но и на создание единого подхода к защите цифровых прав и данных. Несмотря на то, что существующие международные стандарты помогают регулировать сбор, обработку, хранение и передачу личных данных, они все еще не в полной мере защищают пользовательские права в цифровой сфере.

К ключевым международным соглашениям следует отнести Всеобщую декларацию прав человека, Международный пакт о гражданских и политических правах, Международный пакт об экономических, социальных и культурных правах. К региональным, в свою очередь, можно отнести Европейскую конвенцию о защите прав человека и основных свобод, Общий регламент по защите данных, Конвенцию 108 Совета Европы и дополнительный протокол к Конвенции, Будапештскую конвенцию о киберпреступности.

Первый рассматриваемый документ – Всеобщая декларация прав человека[1] – один из наиболее значимых международных документов. Декларация, принятая резолюцией 217A (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года, состоит из 30 статей и является основой международных стандартов в области прав человека. В декларации закреплены следующие положения, среди них следующие:

- «Все люди рождаются свободными и равными в своем достоинстве и правах», – статья 1;
- «Каждый человек имеет право на жизнь, на свободу и на личную неприкосновенность», – статья 3;
- «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь», – статья 12.

Однако Всеобщая декларация прав человека сейчас не в полной мере отражает специфику прав человека в цифровой среде, так как была принята в контексте общественных отношений середины XX века, и, следовательно, не учитывает изменения, обусловленные цифровизацией.

---

[1] Всеобщая декларация прав человека.
URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

Второй документ для рассмотрения – Международный пакт о гражданских и политических правах[2], принятый 16 декабря 1966 года и вступивший в силу 23 марта 1976 года, включает 53 статьи. Пакт основан на Всеобщей декларации прав человека и обязывает уважать гражданские и политические права людей. Данный документ связан с областью цифровых прав и защиты персональных данных через закрепление права на неприкосновенность частной жизни. Таким образом, статья 17 гласит: «Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию».

Международный пакт об экономических, социальных и культурных правах[3] – следующий важный документ для анализа. Это международный договор, принятый Генеральной Ассамблеей Организации Объединенных Наций 16 декабря 1966 года. Вступил в силу 3 января 1976 года. Пакт состоит из 31 статьи и обязывает все государства предоставлять экономические, социальные и культурные права всем лицам.

Предоставим несколько дополнительных фактов. Три представленных международных документа вместе составляют Международный билль о правах человека.[4] До 1976 года Всеобщая декларация прав человека была единственной завершенной частью билля. Документы оказали значительное влияние на деятельность людей и правительств. Декларация завоевала популярность и авторитет, став основой для многих международных документов и национальных законодательств. В свою очередь, Пакты усилили значение Декларации, придали ей новую силу. Важен факт, что Пакты и Всеобщая декларация учитываются в резолюциях и решениях органов ООН, а надзор за выполнением Всеобщей декларации прав человека, Международного пакта о гражданских и политических правах и Международного пакта об экономических, социальных и культурных правах осуществляют следующие комитеты или органы ООН:

1. Комитет по правам человека ООН.
2. Комитет по экономическим, социальным и культурным правам ООН.

---

[2] Международный пакт о гражданских и политических правах. URL: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

[3] Международный пакт об экономических, социальных и культурных правах. URL: https://www.un.org/ru/documents/decl_conv/conventions/pactecon.shtml

[4] Международный билль о правах человека. URL: https://www.un.org/ru/documents/decl_conv/hr_bill.shtml

Международный билль о правах человека является крупной вехой в истории прав человека, знаменующей собой жизненно важный этап развития человечества.

Следующими по очередности представляются региональные документы. Европейская конвенция о защите прав человека и основных свобод (ЕКПЧ)[5] – основополагающий документ Совета Европы (далее – СЕ) и международное соглашение между странами-участниками СЕ. Документ был подписан 2 ноября 1950 года и вступил в силу 3 сентября 1953 года, состоит из 59 статей. Конвенция принята в развитие Всеобщей декларации прав человека и повторяет ее главный тезис о том, что признание равных и неотъемлемых прав и свобод человека – основа «справедливости и всеобщего мира». Однако если Декларация не является обязательным документом, будучи лишь «задачей, к выполнению которой должны стремиться все народы и государства», Конвенция гарантирует соблюдение прав человека на территории стран-членов СЕ и определяет конкретный механизм их защиты. Членство в СЕ прямо предполагает присоединение к Конвенции. В Конвенции закреплены ведущие положения, которые следует интерпретировать, наряду с практиками Совета Европы, применительно к цифровым правам и защите персональных данных. Например:

- «Право на уважение частной и семейной жизни» – статья 8;
- «Свобода выражения мнения» – статья 10;
- «Право на эффективное средство правовой защиты» – статья 13.

Следующий пример, Общий регламент по защите данных Европейского союза (GDPR)[6] – нормативный акт Европейского союза, который определяет правила сбора, обработки, хранения и распространения персональных данных на территории Европейского Союза (далее - ЕС). Регламент вступил в силу 25 мая 2018 года и все государства-члены ЕС обязаны соблюдать его положения. Основная задача GDPR – защита персональных данных и предотвращение нарушений прав человека. Регламент предоставляет гражданам ЕС расширенные права, позволяя им запрашивать информацию о способах обработки своих данных, а также требовать их удаления или передачи другому оператору. Основными принципами регламента стали законность, честность, прозрачность, целостность и конфиденциальность данных.

---

[5] Европейская конвенция о защите прав человека и основных свобод (ЕКПЧ). URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&collection=1&nd=203000250&page=1&rdk=0&link_id=56#I0

[6] Общий регламент по защите данных Европейского союза (GDPR). URL: https://ogdpr.eu/ru

Далее рассмотрим Конвенцию Совета Европы 108[7] о защите физических лиц при автоматизированной обработке персональных данных. Документ был открыт для подписания 28 января 1981 года. Это первый международно-правовой документ в области защиты данных. В нём определён ряд главных принципов, которые легли в основу многих законов о неприкосновенности личной жизни. Конвенция защищает физических лиц от вторжения в их личную жизнь со стороны государственных органов и администрации частных организаций. Также существует Дополнительный протокол к Конвенции 108[8], который усиливает саму Конвенцию СЕ 108. Протокол был открыт для подписания 8 ноября 2001 года и обеспечивает эффективную защиту прав человека и основных свобод, в частности права на уважение частной жизни, в отношении обмена персональными данными через национальные границы.

Также интерес представляет Будапештская Конвенция о киберпреступности, известная как Конвенция о преступности в сфере компьютерной информации[9]. Это международный договор, направленный на борьбу с преступностью в цифровой сфере. Документ был принят Советом Европы 8 ноября 2001 года и вступил в силу 1 июля 2004 года. В документе выделены четыре вида киберпреступлений:

- против конфиденциальности, целостности и доступности данных;
- связанные с использованием компьютерных средств;
- относительно содержания данных;
- касающиеся нарушения авторского права и смежных прав.

Конвенция получила признание как лучшая практика договорно-правового регулирования международного сотрудничества в борьбе с киберпреступностью. Участниками конвенции являются не только члены Совета Европы, но и другие страны, такие как Япония, Филиппины, США, Канада.

Помимо основных представленных документов, можно продолжать углубляться в рассматриваемую тему и находить другие международные соглашения, которые затрагивают область цифровых прав и защиту персональных данных. Следует сделать вывод, что для защиты персональных данных в цифровой сфере и эффективного противодействия киберугрозам необходимо постоянное развитие международных механизмов сотрудничества и активное участие государств, международных организаций и частных лиц.

---

[7] Конвенция 108 Совета Европы. URL: https://rm.coe.int/1680078b37

[8] Дополнительный протокол к Конвенции 108. URL: https://rm.coe.int/1680080626

[9] Конвенция о преступности в сфере компьютерной информации. URL: https://rm.coe.int/1680081580

ГЛАВА 2. ДЕЯТЕЛЬНОСТЬ ООН В СФЕРЕ ЗАЩИТЫ ПРАВ ЧЕЛОВЕКА В УСЛОВИЯХ ЦИФРОВОЙ СЛЕЖКИ И УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Организация Объединенных Наций, как основная международная переговорная платформа по обсуждению общемировых проблем и универсальная по своему характеру, занимает центральное положение в формировании и поддержании норм многостороннего взаимодействия. В рамках органов и специализированных структур ООН все более пристальное внимание уделяется вопросам соблюдения и защиты прав человека в условиях цифровой трансформации, включая аспекты скрытого цифрового наблюдения и информационной безопасности.

Генеральная Ассамблея

С самого начала деятельности Генеральная Ассамблея ООН активно рассматривала вопрос защиты прав человека. Наиболее значимым документом, ставшим предтечей всех последующий резолюций ООН в области прав человека, является Всеобщая декларация прав человека, принятая резолюцией 217А (III) Генеральной Ассамблей ООН 10 декабря 1948 года[10].

16 декабря 1966 года Генеральная Ассамблея приняла Резолюцию 2200 (XXI), которая открыла для подписания следующие международные договоры: Международный пакт об экономических, социальных и культурных правах; Международный пакт о гражданских и политических правах; Факультативный протокол к Международному пакту о гражданских и политических правах[11].

Тема защиты персональных данных впервые получила широкое обсуждение в Генеральной Ассамблее только в начале 1990-х гг.: по итогам работы Комиссии по правам человека и Экономического и Социального Совета 14 декабря 1990 года Генеральная Ассамблея приняла резолюцию 45/95 «Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера»[12], закрепившая десять принципов-гарантий, которые должны предусматриваться в национальных законодательствах.

---

[10] Всеобщая декларация прав человека // Организация Объединенных Наций: официальный сайт. URL: https://undocs.org/ru/A/RES/217(III)

[11] Резолюция 2200 // Организация Объединенных Наций: официальный сайт. URL: https://undocs.org/ru/A/RES/2200(XXI)

[12] Резолюция 45/95 // Организация Объединенных Наций: официальный сайт. URL: https://www.un.org/ru/documents/decl_conv/conventions/computerized_data.shtml

Бурный рост масштабной цифровой слежки и кражи персональных данных побудили ООН обратить внимание на проблемы неприкосновенности частной жизни. Первая резолюция по рассматриваемой проблематике была принята Генеральной Ассамблеей в 2013 году[13]. Резолюция признала уязвимость права на личную жизнь в цифровой среде и инициировала миссию специальных докладчиков для оценки механизмов защиты и выработки соответствующих рекомендаций. Последующие резолюции актуализируют подходы защиты прав человека в цифровую эпоху, подчеркивают межсессионную преемственность и необходимость выработки новых правовых механизмом, регулирующих права человека в интернет-пространстве – A/RES/69/166[14], A/RES/71/199[15], A/RES/73/199[16], A/RES/75/176[17], A/RES/77/211[18], A/RES/79/175[19].

Кроме того, 22-23 сентября 2024 года в Центральных учреждениях Организации Объединенных Наций в Нью-Йорке был проведен Саммит будущего, который подчеркнул необходимость оказания надлежащей поддержки развивающимся странам для реализации предусмотренных в Пакте во имя будущего[20], в том числе в Глобальном цифровом договоре[21], действий, которые имеют отношение к праву на неприкосновенность частной жизни и преодолению цифровых разрывов внутри стран и между ними.

---

[13] Резолюция 68/167 // Организация Объединенных Наций: официальный сайт. URL: https://docs.un.org/ru/A/RES/68/167

[14]Резолюция 69/166 // Организация Объединенных Наций: официальный сайт. URL: https://undocs.org/ru/A/RES/69/166;

[15]Резолюция 71/199 // Организация Объединенных Наций: официальный сайт. URL: https://undocs.org/ru/A/RES/71/199;

[16]Резолюция 73/179 // Организация Объединенных Наций: официальный сайт. URL: https://undocs.org/ru/A/RES/73/179;

[17]Резолюция 75/176 // Организация Объединенных Наций: официальный сайт. URL: https://undocs.org/ru/A/RES/75/176;

[18]Резолюция 77/211 // Организация Объединенных Наций: официальный сайт. URL: https://undocs.org/ru/A/RES/77/211;

[19]Резолюция 79/175 // Организация Объединенных Наций: официальный сайт. URL: https://docs.un.org/ru/A/RES/79/175

[20] Резолюция 79/1 // Организация Объединенных Наций: официальный сайт. URL: https://undocs.org/ru/A/RES/79/1

[21] Там же.

Секретариат

Следует отметить инициативы действующего Генерального секретаря Антониу Гуттериша по новым технологиям, включая Призыв к действиям в области прав человека, с которым он выступил в 2020 году, дорожную карту по цифровому сотрудничеству[22], представленную в конце мая 2020 года, Глобальные принципы

Организации Объединенных Наций в отношении информационной добросовестност[23], создание в мае 2024 года Руководства по обеспечению должной осмотрительности в области прав человека при использовании цифровых технологий и учреждение Канцелярии Посланника Генерального секретаря по вопросам технологий и обсуждения, ежегодно организуемые в рамках Форума по вопросам управления Интернетом, который является многосторонним форумом для обсуждения вопросов управления Интернетом и мандат которого был продлен Генеральной Ассамблеей в 2015 году еще на 10 лет. Ожидается продление мандата на 80-й сессии Генеральной Ассамблеи ООН в декабре 2025 года.

Совет по правам человека

Первой попыткой Совета по правам человека ООН о продвижении и защите прав человека в Интернете, включая свободу выражения мнения и доступ к информации стала резолюция 20/8, принятая 16 июля 2012[24].

---

[22] Дорожная карта по цифровому сотрудничеству: осуществление рекомендаций Группы высокого уровня
по цифровому сотрудничеству. Доклад Генерального секретаря // Организация Объединенных Наций: официальный сайт. URL: https://undocs.org/ru/A/74/821

[23] Глобальные принципы информационной добросовестности Организации Объединенных Наций // Организация Объединенных Наций: официальный сайт. URL: https://www.un.org/ru/information-integrity/global-principles

[24] Резолюция 20/8 // Организация Объединенных Наций: официальный сайт. URL: https://digitallibrary.un.org/record/731540/files/A_HRC_RES_20_8-RU.pdf

26 марта 2015 году Совет по правам человека принял резолюцию 28/16[25], которая учредила первый мандат в отношении неприкосновенности частной жизни. Совет поручил Специальному докладчику получить достоверную информацию от государств, неправительственных организаций и других сторон, осведомленных о случаях, связанных с неприкосновенностью частной жизни. С июля 2021 года мандат принадлежит доктору Ане Браян Нугререс. Следует отметить, что на прошлой сессии третьего Комитета Генеральной Ассамблеи ООН Специальный докладчик представила проект актуализации резолюции 45/95: были предложены принципы в отношении цифровых прав, рекомендованные для включения в национальные законодательства[26].

Стоит отметить резолюцию A/HRC/34/L.7[27] от 17 марта 2017 – были установлены международные стандарты, включая запрет на вмешательство без оснований, поддержка шифрования, защита от дискриминации при автоматизации.

Управление Верховного Комиссара ООН по правам человека

В 2014 году Управление Верховного Комиссара ООН по правам человека подготовило доклад в соответствии с резолюцией Генеральной Ассамблеи 68/167. Доклад A/HRC/27/37[28] анализирует влияние цифровой слежки и сбор данных, предлагает рекомендации по международным механизмам надзора.

Таким образом, механизмы органов и институтов Организации Объединенных Наций постепенно формируют комплексную международную архитектуру, призванную обеспечить баланс между развитием цифровых технологий, защитой прав человека и устранением цифрового неравенства.

---

[25] Резолюция 28/16 // Организация Объединенных Наций: официальный сайт. URL: https://docs.un.org/ru/A/HRC/RES/28/16

[26] A/79/173: Report of the Special Rapporteur on the right to privacy, Ana Brian Nougrères- Proposal for the updating of General Assembly resolution 45/95 of 14 December 1990, entitled “Guidelines for the regulation of computerized personal data files” // Организация Объединенных Наций: официальный сайт. URL: https://www.ohchr.org/en/documents/thematic-reports/a79173-report-special-rapporteur-right-privacy-ana-brian-nougreres

[27] Резолюция 34/L.7 // Организация Объединенных Наций: официальный сайт. URL: https://digitallibrary.un.org/record/1307967/files/A_HRC_34_L.7-RU.pdf

[28] Ежегодный доклад Верховного Комиссара Организации Объединенных Наций по правам человека и доклады Управления Верховного комиссара и Генерального секретаря // Организация Объединенных Наций: официальный сайт. URL: https://docs.un.org/ru/A/HRC/27/37

ГЛАВА 3. НАЦИОНАЛЬНАЯ И РЕГИОНАЛЬНАЯ ДЕЯТЕЛЬНОСТЬ

Вопрос защиты прав человека в цифровую эпоху требует комплексного анализа действий государств, поскольку именно на национальном и региональном уровнях формируются ключевые подходы к регулированию цифровой среды. Сегодня мы наблюдаем парадоксальную ситуацию: с одной стороны, правительства внедряют законы и инициативы, направленные на защиту персональных данных и цифровых прав граждан, а с другой - развивают масштабные системы цифрового надзора, цензуры и слежки, что порождает серьезные вызовы для соблюдения международных правовых стандартов.

Многие государства демонстрируют двойственную позицию: под предлогом обеспечения кибербезопасности и защиты национального суверенитета они внедряют меры, которые на практике могут нарушать свободу слова, право на частную жизнь и другие фундаментальные свободы.

США являются одним из наиболее влиятельных акторов в сфере цифрового контроля. В 2013 году разоблачения Эдварда Сноудена вскрыли практику массовой цифровой слежки, реализуемой Агентством национальной безопасности при сотрудничестве с крупнейшими американскими IT-корпорациями в рамках программы PRISM. Дополнительной правовой основой слежки выступает Закон о наблюдении за иностранной разведкой в редакции 2008 года. В то же время, США предпринимают зеркальные меры по обеспечению защиты прав человека в цифровой среде. Так, Калифорнийский закон о защите прав потребителей укрепил права пользователей на контроль за своими данными, а принятый в 2018 году Clarifying Lawful Overseas Use of Data Act регулирует доступ властей к данным, хранящимся на зарубежных серверах. Также поддерживается принцип сетевого нейтралитета как фундаментальный для равного доступа к цифровым услугам.

Китайская политика цифрового управления характеризуется высоким уровнем централизации и контроля. С 2003 года действует проект «Золотой щит», включающий элементы всеобъемлющей интернет-цензуры и превентивного мониторинга в целях борьбы с преступностью и терроризмом. Одним из ключевых инструментов является «Великий китайский файрвол», ограничивающий доступ к иностранным интернет ресурсам и запрещающий использование негосударственных VPN-сервисов. «Золотой щит» является одним из двенадцати ключевых проектов Поднебесной в рамках программы электронного

правительства. Законодательная база Китая закреплена в Белой книге по вопросам интернета, которая устанавливает запрет анонимности в сети и обосновывает государственный контроль. Вследствие этого в стране развиваются собственные цифровые платформы - Weibo, WeChat и другие - функционирующие в условиях постоянного государственного надзора.

Российская политика в сфере цифрового регулирования основывается на концепции «цифрового суверенитета». В частности, действует Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 N 149-ФЗ, ограничивающий распространение данных и регулирующий цифровое пространство. Запрет на использование отдельных иностранных приложений объясняется необходимостью защиты от вмешательства иностранных разведывательных служб. Однако одновременно российские спецслужбы наделены широкими полномочиями: в соответствии с Федеральным законом «О Федеральной службе безопасности» от 03.04.1995 N 40-ФЗ, ФСБ имеет право на доступ к информации любых категорий. Таким образом, защитные меры в отношении иностранных угроз сочетаются с внутренними инструментами массового контроля.

Индия развивает стратегию цифрового развития с акцентом на государственные сервисы и программы идентификации. Проект Aadhaar, являющийся крупнейшей биометрической системой в мире, предоставляет государству доступ к данным граждан при обеспечении социальных выплат и услуг. С одной стороны, Aadhaar способствует цифровой инклюзии, с другой - вызывает критику со стороны правозащитных организаций ввиду риска утечки персональной информации и отсутствия достаточных гарантий анонимности.

Говоря о Корейском полуострове, Южная Корея сочетает развитую систему защиты прав человека с усиленным государственным надзором. В стране действует Национальная комиссия по правам человека, а также Комиссия по коммуникационным стандартам, регулирующая цифровой контент. Попытка внедрения системы «реального имени» в интернете была отменена решением Конституционного суда в 2012 году как нарушающая свободу слова и право на анонимность. В свою очередь, Северная Корея характеризуется практически полной цифровой изоляцией. Интернет-доступ крайне ограничен и контролируется государством, а использование глобальных сетей практически исключено, что исключает утечки данных, но полностью лишает граждан цифровых прав.

Европейский Союз выступает мировым лидером в области правовой защиты данных. Общий регламент по защите данных 2016/679 стал глобальным эталоном регулирования персональных данных. В 2016 году действовал механизм Privacy Shield в рамках сотрудничества с США, который в 2023 году был заменён на Data Privacy Framework. Ключевым субъектом защиты прав человека в цифровой сфере в Европе является организация «Европейские цифровые права», продвигающая конфиденциальность, свободу слова и анонимность в сети. В 2014 году организация для выборов в Европейский парламент составила Хартию цифровых прав с описанием 10 принципов защиты прав человека в Интернет-пространстве.

Япония демонстрирует высокий уровень цифровой грамотности и доступности интернета. Государство придерживается политики сетевого нейтралитета и активно развивает механизмы защиты прав человека. Особое значение имеет Бюро по правам человека в структуре Министерства юстиции, предоставляющее гражданам консультации по вопросам дискриминации и нарушения цифровых прав.

Сингапур, в свою очередь, выработал уникальную нормативную практику, направленную не только на защиту, но и на контроль информации. В частности, в 2019 году был принят Закон о защите от онлайн-лжи и манипуляций, предоставляющий государственным органам возможность корректировать или блокировать информацию в интернете. Меры позиционируются как направленные на борьбу с дезинформацией, однако вызывают вопросы в контексте свободы выражения мнений.

Основой для защиты личной информации и частной жизни населения Южной Америки и американского полушария является Межамериканская система прав человека, включающая Американскую конвенцию о правах человека или Пакт Сан-Хосе[29], принятая в 1969 году. Хотя Конвенция не регулирует права человека в эпоху цифровизации, но закладывает правовой фундамент для национальных законодательств. Одной из первых стран, рассмотревших вопрос обработки персональных данных, стала Аргентина. В 2000 году был принят закон № 25.326 “О защите персональных данных”[30], который установил правила обработки личных данных для защиты частной жизни.

---

[29] American Convention On Human Rights // Organization of American States: official website. URL: https://www.oas.org/dil/treaties_b-32_american_convention_on_human_rights.pdf

[30] Personal Data Protection Law 25.326 // United Nations: official website. URL: https://sherloc.unodc.org/cld/uploads/res/uncac/LegalLibrary/Argentina/Laws/Argentina%20Personal%20Data%20Protection%20Act%202000.pdf

Африканский континент, в связи с низкой интернет-доступностью большинства населения, представляет собой особенно привлекательный рынок для мировых цифровых гигантов. В этой связи за последнее десятилетие возросла значимость кибербезопасности как одного из ключевых факторов ускорения экономического роста и развития Африки. Данное положение закреплено в стратегическом документе Африканского союза «Повестка дня 2063»[31], который устанавливает 50-летний план развития континента. Ключевым действующим региональным правовым инструментом на сегодняшний день является Конвенция Африканского Союза по кибербезопасности и защите персональных данных (Конвенция Малабо)[32]. Документ был официально принят 27 января 2014 года. Конвенция в том числе охватывает сферу защиты персональных данных, обязывая государства-члены создавать правовые рамки для безопасного сбора, обработки и хранения персональных данных. По состоянию на июль 2024 года[33], Конвенцию ратифицировали 16 государств-членов Африканского Союза, включая Анголу, Бенин, Чад, Конго, Египет, Габон и другие.

[31] Agenda 2063: The Africa We Want // African Union: official website. URL: https://au.int/en/agenda2063/overview

[32] African Union Convention on Cyber Security and Personal Data Protection // African Union: official website. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[33] Там же.

ГЛАВА 4. УГРОЗЫ И РИСКИ, СВЯЗАННЫЕ С ЦИФРОВЫМ ШПИОНАЖЕМ И УТЕЧКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАКЖЕ НЕДОСТАТКИ СУЩЕСТВУЮЩИХ МЕХАНИЗМОВ ЗАЩИТЫ

В представленных нами условиях стремительного развития информационных технологий цифровой шпионаж становится все более распространенным явлением, а утечки персональных данных – непрекращающимися. Все эти процессы представляют серьезную угрозу для отдельных лиц, организаций и даже национальной безопасности.

Цифровые шпионы используют киберпространство для кражи конфиденциальной информации, коммерческих, и даже политических тайн. Такие действия серьезно подрывают конкурентоспособность и инновационный потенциал компаний и угрожают национальной стратегической безопасности. В то же время часто происходят масштабные утечки персональных данных, нарушающие право на неприкосновенность частной жизни. Хищение личных данных, финансовое мошенничество и другие преступления становятся всё более распространёнными, создавая значительную социальную нестабильность.

В этой главе будут подробно рассмотрены распространённые опасности цифрового шпионажа и проанализированы риски и последствия утечек персональных данных, а также будут представлены недостатки существующих механизмов защиты данных.

Сначала мы рассмотрим угрозы и риски утечки персональных данных для обычных пользователей Интернета. Финансовые потери, риск взлома аккаунтов, шантаж и многие другие последствия можно отнести к этому пункту.

О финансовых потерях. Утечки персональных данных являются распространенным способом получения финансовой информации киберпреступниками. После кражи информации о банковских картах и счетах преступники могут легко похитить средства жертв. Они также могут использовать эту информацию для создания поддельных удостоверений личности и подачи заявок на кредитные карты или займы, что возлагает на жертв тяжелое финансовое бремя. Несанкционированные транзакции могут привести к резкому сокращению баланса банковских счетов и даже к долговым кризисам. Еще большую тревогу вызывает то, что злоумышленники могут использовать украденную информацию для совершения крупных покупок, таких как предметы роскоши или инвестиции, в результате чего жертвы несут значительные убытки.

Эти незаконные действия не только истощают сбережения жертв, но и серьезно портят их кредитную историю. Отрицательная кредитная история может повлиять на будущие заявки на кредит, покупку жилья и даже на возможности трудоустройства. Жертвам может потребоваться немало времени и усилий, чтобы восстановить свою кредитную историю и финансовое положение. Поэтому защита личной финансовой информации крайне важна, чтобы не стать жертвой киберпреступности.

О риске взлома аккаунтов. Безопасность аккаунта критически важна в онлайн мире. После взлома аккаунта личная информация и конфиденциальность оказываются под серьезной угрозой. Многие пользователи используют один и тот же пароль на разных платформах для удобства запоминания, что создает возможности для преступников. После взлома пароля хакеры могут попытаться войти в другие аккаунты, похитив личные данные. Эти взломанные аккаунты могут включать аккаунты социальных сетей, электронной почты и банковских счетов, охватывая все аспекты жизни пользователя. Хакеры могут использовать взломанные аккаунты социальных сетей для получения всех важных данных, публикации ложной информации и нанесения ущерба репутации пользователя. Они также могут использовать аккаунты электронной почты для кражи личной информации пользователя и даже выдавать себя за него с целью совершения мошенничества. Риск кражи банковских счетов еще выше, поскольку преступники могут легко переводить средства, что приводит к финансовым потерям. Поэтому крайне важно использовать уникальные и сложные пароли для защиты собственных аккаунтов.

О шантаже. Преступники часто угрожают раскрыть личные данные жертвы в обмен на выкуп. Они крадут конфиденциальную информацию, такую как фотографии, видео, переписки и другие персональные данные, а затем используют их, чтобы потребовать внушительный выкуп. Если жертва отказывается платить выкуп, преступники могут опубликовать эти данные, что приведет к серьезным последствиям и ущербу для людей. Такие ситуации представляют серьезную угрозу не только для отдельных пользователей, но и для компаний и государственных учреждений. Утечка конфиденциальной информации из государственных органов может поставить под угрозу национальную безопасность и социальную стабильность. Поэтому крайне важно предотвращать атаки хакеров. Можно провести установку антивирусного ПО, регулярное резервное копирование данных и избегание переходов по сомнительным ссылкам.

Для бизнеса тоже есть угрозы, связанные с утечкой данных и шифрованием: экономические проблемы, ущерб репутации, повышенная угроза кибератак. Помимо потери клиентов, утечки персональных данных могут привести к судебным искам и значительным штрафам. Расходы на соблюдение нормативных требований, расходы на связи с общественностью в кризисных ситуациях и затраты на устранение технологических проблем также могут стать дополнительными финансовыми проблемами для бизнеса. Также потеря доверия может привести к переходу клиентов к конкурентам, что, в свою очередь, может привести к снижению продаж. И в продолжение, доступ к личным данным сотрудников или клиентов позволяет злоумышленникам проводить целенаправленные атаки, такие как фишинг, вымогательство или шантаж. Это может привести к более серьезным проблемам.

Теперь можно перейти к угрозам для государства и правительственных структур. Государственные органы располагают огромным объемом конфиденциальной информации, включая информацию о политических соглашениях и критически важной инфраструктуре. Утечки данных могут раскрыть эту конфиденциальную информацию иностранным державам, что представляет серьезную угрозу национальной безопасности. Иностранные державы могут использовать эту информацию для шпионажа и подорвать национальную стабильность. Государственным органам необходимо внедрять строгие меры безопасности для защиты конфиденциальной информации и предотвращения утечек данных. Проведение проверок безопасности сотрудников и ограничение доступа к конфиденциальной информации являются важнейшими мерами безопасности. Усиление мер кибербезопасности для предотвращения хакерских вторжений также является важным средством защиты конфиденциальной информации. Сотрудничество со спецслужбами может помочь своевременно выявлять потенциальные угрозы безопасности и принимать соответствующие меры.

Рассмотрим недостатки существующих механизмов защиты. Во-первых, существуют дефекты на уровне технической защиты. Современные атаки могут выполняться искусственным интеллектом, поэтому их становится тяжелее распознать. Традиционные системы безопасности зависят от заранее определенных правил и баз сигнатур для идентификации угроз.

Это делает их подверженными пропускам новых атак, которые не соответствуют установленным шаблонам. Искусственный интеллект способен распознавать аномалии и едва заметные отклонения в массивных наборах данных. Во-вторых, механизм мониторинга и реагирования все еще недостаточный. Существующим системам все еще сложно обнаруживать скрытые APT-атаки. В-третьих, отсутствие контроля со стороны властей медленно может усугублять ситуацию. Законодательное регулирование и стандарты в области кибербезопасности могут значительно отставать от развития технологий. В-четвертых, существует человеческий фактор. Пользователи используют устаревшие системы, отказываются от шифрования данных, и в-целом недостаточно осведомлены о правилах обработки, хранения и передачи информации. В результате, можно сделать вывод: недостатки существующих механизмов защиты заключаются в том, что новые технологии разрабатываются быстрее, чем средства их защиты.

В заключение главы, угрозы и риски, связанные с цифровым шпионажем и утечкой персональных данных, серьезны и могут привести к значительным потерям для пользователей. Чтобы сократить количество таких угроз и рисков нужно улучшать все механизмы защиты. И особенно следует улучшать систему законов и систему регулирования.

ЗАКЛЮЧЕНИЕ

В условиях стремительной цифровизации и роста глобальной взаимозависимости вопрос защиты прав человека в цифровом пространстве приобрел принципиальное значение для обеспечения международной стабильности и безопасности. Наряду с очевидными преимуществами, развитие цифровых технологий порождает новые угрозы, которые подрывают основы доверия между гражданским обществом и государствами.

Международно-правовая база, включающая фундаментальные документы ООН, региональные конвенции и специальные соглашения, сформировала каркас регулирования деятельности государственных и негосударственных акторов. Деятельность органов ООН и их специализированных учреждений установила прецедент по выработке новых подходов к текущим реалиям. Вместе с тем, данные инициативы пока не привели к выработке универсального механизма контроля, что ограничивает действенность таких инициатив.

Угрозы и вызовы, связанные с кибершпионажем, утечкой персональных данных, вмешательством в частную жизнь, падением доверия к цифровым платформам подтверждают несоответствие текущим глобальным рискам. Дополнительным препятствием на пути к выработке единого регуляторного документа в сфере цифрового регулирования остаются низкий уровень цифровой грамотности значительной части пользователей сети Интернет и недостаточная институциональная координация.

Таким образом, представляется необходимым реализация таких мер как:

1. Расширение международного сотрудничества через обмен информацией и противодействие киберугрозам и кибершпионажу;
2. Выработка универсальных международных стандартов, создающих основу для национальных законодательств в сфере защиты цифровых прав граждан;
3. Создание эффективных международных механизмов привлечения к ответственности за нарушения прав человека в цифровом пространстве;
4. Формирование независимых органов контроля с целью усиления мер в области кибербезопасности и предотвращения утечки персональных данных.

Комплексная реализация перечисленных механизмов смогла бы в полной мере заложить основы для формирования единой архитектуры правового цифрового регулирования, которая в то же время обеспечила бы развитие цифровых технологий и гарантировала защиту прав человека в условиях глобальной цифровой трансформации.

ГЛОССАРИЙ

Персональные данные — это любая информация, которая прямо или косвенно относится к конкретному физическому лицу и позволяет его идентифицировать.

Пользовательские права (права доступа пользователей) — это разрешения, которые позволяют пользователям взаимодействовать с объектами инфраструктуры: целевыми системами, приложениями, сетевым оборудованием, данными и другими ресурсами. Эти права определяют, какие действия пользователь может выполнять, а какие — нет.

Конфиденциальность — необходимость предотвращения разглашения, утечки какой-либо информации.

Утечка персональных данных — это несанкционированная передача конфиденциальной информации третьим лицам и организациям или её размещение в открытом доступе. Такая информация включает имена и номера телефонов пользователей, адреса электронной почты, паспортные данные, банковские реквизиты и другие личные сведения.

Цифровизация — это процесс внедрения цифровых технологий в рабочие процессы организации, в разные сферы жизни человека и бизнеса.

Цифровая слежка — это сбор данных о действиях пользователя в интернете, которые документируются и хранятся на серверах помимо воли пользователя.

Цифровая безопасность (кибербезопасность) — это совокупность мер и практик, направленных на защиту компьютерных систем, сетей, программ и данных от цифровых угроз, атак и несанкционированного доступа.

Киберпространство — виртуальный мир цифровой или электронной коммуникации, связанной с глобальной информационной инфраструктурой.

Киберпреступность — действие, нарушающее закон, которое совершается с использованием информационно-коммуникационных технологий и либо нацелено на сети, системы, данные, веб-сайты и/или технологии, либо способствует совершению преступления.

Кибератаки — попытка преднамеренного причинения ущерба лицу, группе лиц или организации путем преодоления защиты их цифровых систем (например, компьютеров) с целью хищения, взлома, нарушения доступности или уничтожения данных или приложений, которые, по мнению их пользователей, являются конфиденциальными или имеют важное значение для их работы.

Киберугроза — это потенциально вредоносная деятельность, способная повлечь нарушение функционирования компьютерных систем, неправомерное завладение, искажение, уничтожение либо незаконное использование данных и иной цифровой информации, охраняемой законом.

Кибершпионаж — использование информационно-коммуникационных технологий (ИКТ) отдельными лицами, группами лиц, компаниями, правительственными структурами, группами, финансируемыми или контролируемыми государством либо прочими лицами, действующими от имени правительства для получения несанкционированного доступа к системам и данным и сбора разведданных об интересующих их объектах.

Генеральная Ассамблея ООН — главный директивный орган Организации Объединенных Наций, состоящий из представителей всех государств-членов и представляющий собой уникальный форум для многостороннего обсуждения всего спектра международных вопросов, охватываемых Уставом ООН.

Секретариат ООН — один из шести главных органов Организации Объединенных Наций, который осуществляет оперативную и административную работу Организации. Его возглавляет Генеральный секретарь, который обеспечивает общее административное руководство.

Совет по правам человека — межправительственный орган системы ООН, в состав которого входят 47 государств, ответственных за поощрение и защиту всех прав человека по всему миру.

Управление Верховного Комиссара ООН по правам человека — агентство в системе ООН, которое следит за соблюдением и защитой прав человека, гарантируемых Всеобщей Декларацией прав человека.