

Научная статья. Исторические науки

УДК 323(597+596)

DOI: 10.31696/2072-8271-2025-2-2-67-248-262

СРАВНЕНИЕ КИБЕРБЕЗОПАСНОСТИ ВО ВЬЕТНАМЕ И КАМБОДЖЕ

Григорий Николаевич КУЧЕРЕНКО¹

¹ ИМЭМО РАН, Москва, Россия,

gri7595@yandex.ru, <https://orcid.org/0000-0002-8160-1662>

Аннотация: В статье рассматриваются подходы Камбоджи и Вьетнама в сфере кибербезопасности, борьбы с киберпреступностью и защите персональных данных. На данном этапе Вьетнам активно совершенствует законодательство, адаптируя его под меняющиеся угрозы в условиях нарастающего давления как внешних сил, так и внутренних. Камбоджа, в свою очередь, не проявляет соответствующей гибкости. Невзирая на принятие некоторых законодательных мер, страна не в состоянии адекватно ответить новым вызовам, что неизбежно сказывается на росте киберпреступности и ухудшении ситуации в сфере кибербезопасности. Важно отметить, что Вьетнам мог бы стать примером для Камбоджи в трансформации подхода к сетевым угрозам, а активизация международного сотрудничества со странами, обладающими соответствующим опытом, дала бы больший спектр инструментов.

Ключевые слова: кибербезопасность, Вьетнам, Камбоджа, киберпреступность, законодательство, международное сотрудничество

Для цитирования: Кучеренко Г.Н. Сравнение кибербезопасности во Вьетнаме и Камбодже // Юго-Восточная Азия: актуальные проблемы развития, 2025, Том 2, № 2 (67). С. 248–262. DOI: 10.31696/2072-8271-2025-2-2-67-248-262

Original article. Historical science

COMPARING CYBERSECURITY IN VIETNAM AND CAMBODIA

Grigory N. KUCHERENKO¹

¹ IMEMO RAS, Moscow, Russia,

gri7595@yandex.ru, <https://orcid.org/0000-0002-8160-1662>

Abstract: This article examines the approaches of Cambodia and Vietnam to cybersecurity, cybercrime, and personal data protection. Currently, Vietnam is actively improving its legislation and adapting to changing

threats in the face of increasing external and internal pressures. Cambodia, on the other hand, has not been flexible. Despite the adoption of some legislative measures, the country is unable to adequately respond to new challenges, which inevitably affects the growth of cybercrime and the deterioration of the cybersecurity situation. It is important to note that Vietnam could be a model for Cambodia in transforming its approach to online threats, and increased international cooperation with countries with relevant experience would provide a wider range of tools.

Keywords: cybersecurity, Vietnam, Cambodia, cybercrime, legislation, international cooperation

For citation: Kucherenko G.N. Comparing Cybersecurity in Vietnam and Cambodia. *Yugo-Vostochnaya Aziya: aktual'nyye problemy razvitiya*, 2025, T. 2, № 2 (67). Pp. 248–262. DOI: 10.31696/2072-8271-2025-2-2-67-248-262

Введение

Цифровизация экономики и повсеместное проникновение интернета приносят не только новые возможности, но и серьёзные угрозы, среди которых особенно выделяется стремительный рост киберпреступности. Согласно исследованиям МВФ, к 2027 г. мировой ущерб от киберпреступлений может достичь 23 трлн долл. США, что на 175% превышает показатели 2022 г.¹ Возрастающая зависимость от цифровых платформ делает общество уязвимым для таких угроз, как вредоносные программы, фишинговые атаки, атаки типа «отказ в обслуживании» (DDoS) и «человек посередине» (MITM). Страны Юго-Восточной Азии, включая Камбоджу и Вьетнам, особенно подвержены этим рискам из-за неравномерного развития законодательства и недостаточной эффективности мер борьбы с киберугрозами.

Вьетнам, занимающий 13-е место в мире по численности интернет-пользователей, демонстрирует высокий уровень цифровизации, однако этот прогресс сопровождается стремительным ростом киберпреступности². Увеличение числа пользователей и повышение технической подготовки хакеров создают благоприятные условия для атак. Только за первую половину 2023 г. в стране было зарегистрировано около 6 тыс. кибератак, а к концу года их число превысило 13 900, увеличившись более чем в два раза³. Особую тревогу вызывает тот факт, что из 554 взломанных сайтов 212 принадлежали государственным учреждениям, что ставит под угрозу стабильность государственного

управления. К 2024 г. примерно 20% населения оказались уязвимы к сетевым атакам, что подчёркивает масштаб проблемы⁴.

Данная тема привлекает всё большее внимание международных экспертов в связи с укреплением статуса Юго-Восточной Азии как двигателя мировой экономики и факторов, способствующих замедлению этого процесса. Налицо контраст^{5,6}: Вьетнам развивает инфраструктуру и законы, но сохраняет пробелы, а Камбоджа отстаёт в защите. Культурные факторы усугубляют риски: низкая цифровая грамотность в Камбодже⁷ и успехи вроде нового закона о цифровой торговле демонстрируют влияние регуляторных усилий. Отечественные учёные дополняют картину анализом международного сотрудничества как ключевого инструмента борьбы с угрозами⁸.

Результаты исследования показали, что, несмотря на схожесть в подходах к кибербезопасности, Вьетнам демонстрирует более высокие показатели в области законодательного регулирования и внедрения технологий защиты информации по сравнению с Камбоджей. Анализ выявил также значительные различия в уровне осведомленности и готовности организаций к реагированию на киберугрозы.

Статья представляет собой комплексное исследование, посвящённое сравнительному анализу кибербезопасности Вьетнама и Камбоджи в контексте их роли как быстро цифровизирующихся экономик Юго-Восточной Азии. Её основа заключается в синтезе правового, технологического и культурно-социального анализа, что позволило сформулировать универсальные рекомендации для развивающихся стран, включая необходимость международного сотрудничества и превентивных мер, ориентированных на локальные риски. Практическая значимость подкреплена актуальными данными и кейсами, такими как оценка нового камбоджийского закона о цифровой торговле, что делает статью отправной точкой для дальнейших исследований в области адаптивной кибербезопасности.

Законодательство во Вьетнаме

Ещё в 2005 г., задолго до того, как кибератаки стали массовой угрозой, Вьетнам принял закон о безналичных операциях, который заложил основы для будущей кибербезопасности. Этот документ не только ввёл ключевые понятия, такие как электронная подпись и электронный сертификат, но и чётко определил киберпреступления, включая незаконное изменение, удаление, подделку или копирование данных, установив за них строгие наказания⁹. Однако, несмотря на эти меры, в 2007 г. хакерам удалось взломать сайт министерства

иностранных дел страны, что стало первым крупным инцидентом во вьетнамском киберпространстве. Этот случай подчеркнул, что даже проактивные меры не всегда могут предотвратить угрозы, но продемонстрировал готовность властей к решительным действиям в борьбе за цифровую безопасность.

В 2010 г., спустя несколько лет после первого крупного инцидента с кибератаками, Вьетнам сделал значительный шаг вперёд в борьбе за цифровую безопасность. В Ханое был запущен Проект развития цифровой информационной безопасности до 2020 г., ставший первым стратегическим документом, который чётко определил приоритеты государственных органов в области защиты данных¹⁰.

До принятия этой дорожной карты меры по укреплению кибербезопасности носили фрагментарный характер, и лишь с её внедрением Вьетнам перешёл к системному подходу, который позволил не только реагировать на угрозы, но и предупреждать их.

В период с 2010 по 2016 г. Вьетнам столкнулся с резким ростом киберугроз. Согласно данным Азиатско-Тихоокеанской группы реагирования на компьютерные чрезвычайные ситуации (APCERT, 2016), за эти годы было зафиксировано более 190 тыс. кибератак, что в среднем составляет около 27 тыс. инцидентов ежегодно. Одной из ключевых причин такого роста стало стремительное увеличение числа пользователей онлайн-магазинов: если в 2015 г. их доля составляла 67% от общего числа пользователей интернета, то уже к 2016 г. этот показатель вырос до 94%¹¹. Однако развитие цифровой экономики происходило на фоне недостаточной готовности законодательной базы. На тот момент законы не охватывали многих критически важных аспектов, таких как защита конфиденциальности данных, вопросы совместимости систем и регулирование государственных закупок. Например, требования об обязательном уведомлении о нарушениях конфиденциальности данных были введены лишь в 2014 г., что значительно отставало от темпов технологического прогресса.

Ещё одной важной причиной роста киберугроз стало начало кибервойн между китайскими и вьетнамскими хакерами. Формальным поводом для их начала послужил инцидент 2011 г., когда китайские суда повредили кабельную систему вьетнамского гидрографического исследовательского судна¹². Хотя прямые последствия для вьетнамского интернета оказались относительно незначительными, атака подняла серьёзные вопросы о готовности Вьетнама к более масштабным киберугрозам. Уже в 2012 г. китайские хакеры атаковали ключевые вьетнамские организации, включая *PetroVietnam*, *Vietnam News Agency*

и *Vietnam Post*¹³. Эскалация конфликта продолжилась в 2014 г., во время противостояния вокруг нефтяных вышек, когда предположительно китайские хакеры атаковали 220 вьетнамских сайтов, включая шесть правительственных¹⁴.

Наконец, в июле 2016 г. китайская хакерская группа *1973cn* провела масштабную атаку на ключевые объекты вьетнамской авиационной инфраструктуры. Хакеры распространяли информацию, поддерживавшую территориальные претензии Китая в Южно-Китайском море. В тот же день, как заявили представители *Vietnam Airlines*, группа *1973cn* похитила и обнародовала конфиденциальные данные клиентов авиакомпании. Позднее, в 2018 и 2019 гг., китайская хакерская группировка *Mustang Panda* продолжила атаки, нацелившись на информационные системы пограничных служб Вьетнама¹⁵.

В ответ на растущие киберугрозы вьетнамское правительство в последующие годы приняло ряд новых законов, регулирующих сферу информационных технологий, борьбу со спамом и другие аспекты цифровой безопасности. Одним из ключевых шагов стало принятие в 2015 г. Закона о кибербезопасности — первого в истории страны документа, который комплексно регулирует вопросы защиты от киберугроз. Закон был направлен на укрепление потенциала в области кибербезопасности, а также стимулирование организаций и частных лиц к инвестициям в создание совместных предприятий и развитие образовательных программ. В частности, акцент был сделан на подготовку кадров через высшие и профессионально-технические учебные заведения, что должно было обеспечить Вьетнам квалифицированными специалистами в этой критически важной сфере. Однако международные эксперты выразили обеспокоенность по поводу нечётких формулировок закона, особенно в части защиты данных. По их мнению, такие формулировки могли затруднить выполнение требований закона владельцами данных и создать дополнительные риски¹⁶.

Вьетнам, как и многие страны (например, Австралия, Франция), криминализует использование программ-вымогателей (*ransomware*) в рамках национального законодательства, несмотря на отсутствие членства в Будапештской конвенции по киберпреступности. Уголовный кодекс 2015 г. включает раздел о «преступлениях против регулирования информационных технологий и телекоммуникационных сетей», где создание, распространение или использование программ-вымогателей, включая выплату выкупа, классифицируется как незаконное присвоение собственности (ст. 288, 289). Дополняют эту базу Закон о кибербезопасности (2018) и Закон о киберинформационной

безопасности (2015), предусматривающие дисциплинарные, административные и уголовные меры в зависимости от тяжести нарушений.

Гражданский кодекс 2015 г. теоретически допускает компенсацию ущерба жертвам, однако такие иски редко выделяются в отдельные дела, поскольку суды предпочитают рассматривать их в рамках уголовных процессов. Таким образом, Вьетнам демонстрирует жёсткий репрессивный подход к программам-вымогателям, частично компенсируя отсутствие международных соглашений внутренними законами, но эффективность этой системы зависит от технологической модернизации и подготовки следственных органов.

В 2018 г. был принят новый Закон о кибербезопасности, который вступил в силу в 2019 г. В отличие от закона 2015 г., он включал ряд важных нововведений. Среди них — чёткое определение актов, нарушающих национальную безопасность в киберпространстве, установление стандартов и технических регламентов в области кибербезопасности, а также введение механизма запроса на удаление незаконной или недостоверной информации, которая угрожает национальной безопасности, общественному порядку, законным правам и интересам граждан и организаций. Эти меры были направлены на усиление контроля над киберпространством и повышение уровня защиты от цифровых угроз.

Уделяя особое внимание государственной и национальной безопасности, новый закон имеет широкую сферу применения. Он потенциально налагает серьёзные обязательства как на внутренние, так и особенно на офшорные компании, предоставляющие онлайн-услуги вьетнамским клиентам. Например, закон требует, чтобы владельцы веб-сайтов, порталов и социальных сетей не предоставляли, не размещали и не передавали информацию, которая является пропагандой против правительства Вьетнама; подстрекает к насильственным беспорядкам, нарушает безопасность или общественный порядок; содержит унижительную или клеветническую информацию; или содержит сфабрикованную или неправдивую информацию (в определённых контекстах)¹⁷.

Стоит отметить, что, невзирая на развитие законодательства и ужесточение наказаний за правонарушение, ситуация остаётся сложной. Спикер министерства общественной безопасности Вьетнама отметил, что за первый квартал 2024 г. было зафиксировано более 20 млн предупреждений о кибератаках, что на 33% больше, чем в прошлом году¹⁸.

Несмотря на прогресс в создании жёсткой правовой базы, Вьетнам сталкивается с растущими вызовами киберпреступности, включая изощрённые атаки программ-вымогателей и трансграничные угрозы.

Перспективы улучшения ситуации связаны с усилением международного сотрудничества (вступление в Будапештскую конвенцию или альтернативные соглашения, заключение соглашений с со странами, обладающими развитыми средствами борьбы с киберугрозами, такими как Россия, инвестициями в ИИ-технологии для мониторинга угроз и подготовки специалистов по цифровой криминалистике¹⁹. Рекомендуется также развивать публично-частные партнёрства для защиты критической инфраструктуры и внедрять образовательные программы по кибергигиене для населения. Однако успех этих мер зависит от преодоления бюрократических барьеров и модернизации технологической базы правоохранительных органов, что позволит Вьетнаму не только противостоять текущим угрозам, но и стать региональным лидером в области кибербезопасности.

Вьетнамская киберпреступность

В настоящее время основными преступлениями во вьетнамском киберпространстве являются мошенничество и деятельность онлайн-казино. В октябре 2024 г. Министерство общественной безопасности Вьетнама сообщило о ликвидации преступной группировки, организовавшей онлайн-игры с общим объёмом ставок в 1,8 млрд донгов (около 71 160 млн долларов США)²⁰. Стоит отметить, что организация, содействие или участие в азартных играх и казино остаются во Вьетнаме незаконными, за исключением лицензированных казино и электронных игровых клубов, действующих в строго определённых рамках. Однако в стране отсутствует специализированный национальный регулирующий орган, контролирующий игорную индустрию, а также универсальная система лицензирования, которая позволила бы выявлять бенефициаров и исключать неподходящие компании или частных лиц из сферы владения и управления казино. В настоящее время регулирование азартных игр и предотвращение связанной с ними преступной деятельности распределено между Министерством финансов (*MOF*), Министерством общественной безопасности, Канцелярией премьер-министра и некоторыми провинциальными властями, что создаёт сложности в координации и эффективности контроля²¹.

Что касается мошенничества, то, согласно данным Вьетнамской Национальной Ассоциации Кибербезопасности (*NCA*), 1 из 220 пользователей стал жертвой мошенников. Основные методы включали: вовлечение в мошеннические инвестиционные схемы с обещаниями высоких доходов, выдачу себя за представителей государственных учреждений и организаций, а также рассылку фальшивых уведомлений о

выигрышах или крупных акциях²². Общий ущерб от таких атак к концу 2024 г. составил около 18,9 трлн донгов (примерно 742,28 млн долл. США)²³.

Законодательство в Камбодже

Ситуация в Камбодже значительно отличается от вьетнамской в силу того, что королевство всё ещё не разработало в достаточной степени законодательство по борьбе с киберугрозами. По-прежнему не принят закон, охватывавший бы в полной мере борьбу с киберугрозами, что негативно сказывается на способностях властей бороться с преступностью в этой области. В настоящий момент министерство информации Камбоджи утверждает, что количество кибератак в 2024 г. выросло на 28% в сравнении с предыдущим годом²⁴.

До 2009 г. законодательство никак не затрагивало вопрос кибербезопасности в стране, что поспособствовало большей активности преступников чем в других странах АСЕАН. Ситуация стала меняться лишь с принятием нового уголовного кодекса, в котором хоть и не было упоминания кибербезопасности, но в статьях 317–320 и 427–432 были включены преступления, связанные с компьютерами, которые называются «Нарушение тайны переписки и телекоммуникаций» и «Преступления в сфере информационных технологий». «Диффамация и оскорбление» также считаются разновидностью киберпреступлений, если они совершаются через компьютерные сети²⁵.

Дальнейшее развитие законодательства в данной области относится к 2015 г., когда был принят закон о телекоммуникациях. Целями данного закона являются определение полномочий Министерства почты и телекоммуникаций (МПТ), создание и описание обязанностей Телекоммуникационного регулятора Камбоджи (ТРК), классификация различных типов разрешений, сертификатов и лицензий, а также установление надзора за использованием инфраструктуры и сети, тарифов, честной конкуренции и защиты потребителей²⁶. В рамках данного закона МПТ получало право запрашивать данные пользователей у мобильных операторов и контроль над сетевой инфраструктурой, а также право на тайное наблюдение за сообщениями, если оно осуществляется с разрешения «законного органа власти»²⁷. Важно отметить, что данный законопроект подвергся критике со стороны правозащитников, специальный докладчик ООН по правам человека в Камбодже Рона Смит отмечала, что «закон требует от телекоммуникационных компаний передавать определенные данные правительству по запросу»²⁸.

В 2018 г. были приняты новые меры, ужесточающие контроль над мобильными операторами со стороны министерства. Правительство выпустило документ, согласно которому всем интернет-провайдерам нужно было установить программное обеспечение, необходимое для мониторинга, фильтрации и блокировки «незаконного» контента, включая аккаунты в социальных сетях²⁹.

В 2019 г. Камбоджа приняла Закон об электронной коммерции, регулирующий все коммерческие и гражданские акты, документы и сделки, совершаемые через электронную систему, за исключением тех, что связаны с доверенностями, завещаниями и наследованием, а также недвижимостью. Помимо обеспечения правовой определенности электронных сделок, закон регулирует внутреннюю и трансграничную деятельность в области электронной коммерции в стране и вводит важные меры защиты потребителей, включая защиту данных о потребителях. Примечательно, что Камбоджа стала последней страной АСЕАН, принявшей закон об электронной коммерции, что в очередной раз подчёркивает сугубо реактивную систему принятия решений в стране и крайне медленное развитие законодательства в сфере кибербезопасности.

По мнению международных исследователей, данный закон создаёт своего рода «безопасную гавань» для поставщиков услуг электронной торговли и посредников, согласно которой они не несут ответственности за незаконный контент третьих лиц на своих онлайн-платформах, при этом они должны соблюдать определенные обязательные процедуры удаления контента, когда им становится известно о таковом. Кроме того, они обязаны соблюдать кодекс поведения в сфере электронной коммерции³⁰.

В настоящий момент Камбоджа остаётся одной из немногих стран АСЕАН, до сих пор не принявших закон о кибербезопасности, который охватывал бы все ключевые моменты и лёг бы в основу дальнейшего развития законодательства. В 2018 г. правительство Камбоджи опубликовало черновой вариант закона о кибербезопасности. Закон устанавливает уголовную ответственность за различные виды активности в интернете и обеспечивает правовую основу для расследования и судебного преследования по делам о киберпреступлениях. Он важен тем, что в нём концептуально сформулированы ключевые понятия. Киберпреступность определяется как любое уголовное преступление, совершенное с использованием систем информационно-коммуникационных технологий (ИКТ), включая хакерство, фишинг, кражу личных данных и распространение вредоносных программ. Соответственно,

закон устанавливает и соответствующие наказания. Закон устанавливает наказания за киберпреступления, начиная от штрафов и заканчивая тюремным заключением. Например, максимальное наказание за несанкционированный доступ к компьютерной системе составляет три года лишения свободы и штраф в размере до 10 млн риелей (2,5 тыс. долларов США)³¹.

В экспертном сообществе присутствует точка зрения, согласно которой, закон может быть использован не только для борьбы с киберпреступностью, но и для зачистки интернет-пространства от несогласных. С этим тяжело спорить, с учётом того, что внутривнутриполитическое пространство Камбоджи вычищено практически до стерильного состояния и организованной оппозиции на данный момент толком нет.

В то же время камбоджийские власти не пытаются решить проблему киберпреступности в одиночку. В ноябре 2019 г. Генеральная Ассамблея ООН приняла резолюцию о борьбе с киберпреступностью, авторами которой являются Россия, Беларусь, Камбоджа, Китай, Иран, Мьянма, Никарагуа, Сирия и Венесуэла. Сама резолюция стала предметом ожесточённых дискуссий экспертов из разных стран, в частности, российские специалисты отмечали, что ранее действовавшая Будапештская конвенция по кибербезопасности устарела и не в состоянии обеспечивать эффективную борьбу с киберпреступностью. Западные эксперты, в свою очередь, утверждают, что возможные негативные последствия этой конвенции не ограничиваются правами человека, но могут серьезно угрожать глобальной кибербезопасности и национальной безопасности³².

В мае 2023 г. лидеры стран Юго-Восточной Азии договорились усилить пограничный контроль и правоохранительные органы, а также повысить уровень образования населения для борьбы с преступными синдикатами, которые переправляют работников в другие страны, где их заставляют участвовать в интернет-мошенничестве³³.

В рамках международного сотрудничества в области уголовного правосудия Камбоджа заключила ряд двусторонних и многосторонних соглашений, включая договоры об экстрадиции, передаче заключённых и взаимной правовой помощи (ВПП). Особое значение имеет Договор АСЕАН о взаимной правовой помощи по уголовным делам, который закрепляет многосторонний формат сотрудничества в регионе. Кроме того, Королевство Камбоджа подписало двусторонние уголовно-правовые соглашения с четырьмя странами: Южной Кореей, Вьетнамом, Индией и Россией. Эти договоры обеспечивают правовую основу для

эффективного взаимодействия в борьбе с транснациональной преступностью.

Камбоджийская киберпреступность

В Юго-Восточной Азии Камбоджа занимает одно из лидирующих мест по уровню криминогенной обстановки, уступая в этом отношении только Мьянме. Королевство сталкивается с целым рядом серьёзных проблем, включая торговлю людьми, незаконную торговлю ресурсами дикой природы, финансовые преступления и наркотрафик. Особое место в этом списке занимает кибермошенничество, которое сочетает в себе элементы как финансовых преступлений, так и торговли людьми, что делает его одной из наиболее сложных и многоаспектных угроз для страны.

Среди ключевых причин, способствующих широкому распространению киберпреступности в Камбодже, можно выделить слаборазвитую инфраструктуру кибербезопасности, отсутствие проработанного законодательства, высокий уровень коррупции среди руководства страны, а также тесные связи части элит с организованной преступностью, которая продолжает набирать силу и влияние. Эти факторы приводят к крайне низким темпам раскрытия преступлений и создают условия для эксплуатации тысяч иностранных граждан, вынужденных работать в колл-центрах мошенников в условиях, близких к рабству.

В сентябре Управление ООН по правам человека выпустило доклад, в котором утверждалось, что количество жертв подобного рода мошенничества в Камбодже достигает 100 тыс. человек, что подчёркивает серьёзность проблемы³⁴. По состоянию на июль 2023 г. центры онлайн-мошенничества действовали в крупных городах, например, в Пномпене и Кох Конга, казино, прибрежных городах, зонах отдыха и т.д. По данным Госдепартамента США, в Камбодже в таких комплексах застряли около 10 тыс. человек из разных стран мира, многие из них – жители Китая, Вьетнама, Малайзии и Таиланда³⁵. Правительства этих стран сотрудничают с Камбоджей в деле спасения своих граждан, однако эти усилия в основном носят индивидуальный характер.

Поскольку работники приносят от 1 до 10 тыс. долларов на одну жертву мошенничества в месяц и не менее двух новых жертв каждую неделю, индустрия мошенничества в Камбодже – стране с официальным ВВП чуть менее 31,8 млрд долл. – по оценкам, ежегодно приносит 12,5 млрд долл.³⁶ Это очень скромная оценка, рассчитанная исходя из того, что работники приносят 1 тыс. долл. на одну жертву мошенничества и две новые жертвы каждую неделю. Издание отмечает, что

бывшие работники оценивают приблизительный доход в 10 тыс. долл. на одну жертву мошенничества, таким образом, общая годовая сумма может достигать 125 млрд долларов³⁷.

Значительную роль в формировании сети организованной преступности в Камбодже играют иностранные преступные группировки, в частности китайские. Они активно вовлечены в такие виды незаконной деятельности, как торговля людьми, наркотрафик и отмывание денег через казино и строительные проекты. Эти группы часто устанавливают связи с местными криминальными структурами и налаживают сотрудничество с преступниками в соседних странах, что усиливает их влияние. Правительство Камбоджи предпринимает меры по борьбе с этим явлением, включая рейды и депортацию преступников³⁸. Однако, как отмечают международные эксперты, эти действия носят эпизодический характер и недостаточно эффективны, поскольку преступная деятельность возобновляется вскоре после завершения операций³⁹.

Стоит отметить, что камбоджийские власти запрашивали помощь других стран для борьбы с данной проблемой, в частности, у США и Австралии⁴⁰. Представляется наиболее вероятным, что эти две страны, обладая развитой инфраструктурой и проработанным законодательством, показали камбоджийским властям наиболее привлекательными с точки зрения потенциальной эффективности сотрудничества. Однако упоминаний о системной работе между правоохранительными органами Камбоджи и других стран найти не удалось, исходя из чего был сделан вывод, что оно носит спорадический характер и его эффективность находится на невысоком уровне.

Сравнение кибербезопасности во Вьетнаме и Камбодже подчеркивает значительные различия в подходах к регулированию и применению в области защиты информации и борьбы с киберпреступностью. Во Вьетнаме, благодаря более развитой правовой базе, включая Уголовный кодекс 2015 г. и закон о кибербезопасности 2018 г., наблюдается системный подход к решению проблем, связанных с киберугрозами. Это включает в себя четкое определение преступлений, связанных с информационными технологиями, и установление строгих мер ответственности для правонарушителей. Вьетнамская система также демонстрирует активное сотрудничество между правоохранительными органами и частным сектором, что способствует более эффективному выявлению и расследованию киберпреступлений.

В отличие от этого, Камбоджа сталкивается с рядом вызовов в области кибербезопасности, включая недостаточную правовую инфраструктуру и ограниченные ресурсы для борьбы с киберугрозами. Хотя

в стране также предпринимаются шаги к улучшению ситуации, такие как разработка законов о кибербезопасности, их реализация и соблюдение остаются на низком уровне. Это создает благоприятные условия для распространения киберпреступности и вымогательства, что ставит под угрозу как индивидуальные, так и государственные интересы.

Заключение

Таким образом, можно сделать вывод, что для повышения уровня кибербезопасности в Камбодже необходимо не только разработать и внедрить более строгие законы, но и обеспечить их эффективное исполнение. Вьетнам может служить примером для Камбоджи, демонстрируя, как комплексный подход к законодательству и правоприменению может значительно улучшить ситуацию в области кибербезопасности. Важно, чтобы обе страны продолжали развивать свои стратегии в этой области, учитывая быстро меняющийся ландшафт киберугроз и необходимость международного сотрудничества для защиты своих граждан и организаций от киберпреступлений.

ИНФОРМАЦИЯ ОБ АВТОРЕ

КУЧЕРЕНКО Григорий Николаевич, м.н.с. Сектора новых вызовов в Южной и Юго-Восточной Азии, ИМЭМО РАН, Москва, Россия

Статья поступила в редакцию 30.04.2025; одобрена после рецензирования 15.05.2024; принята к публикации 30.05.2025.

INFORMATION ABOUT THE AUTHOR

Grigory N. KUCHERENKO, Research Assistant, IMEMO RAS, Moscow, Russia

The article was submitted 30.04.2025; approved 15.05.2025; accepted to publication 30.05.2025.

¹ Key Cyber Security Statistics for 2025 // SentinelOne, 12.09.2024. URL: <https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/>

² Statista Search Department. Countries with the largest digital populations in the world as of February 2025 (in millions) // Statista. URL: <https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/#:~:text=Countries%20with%20the%20highest%20number%20of%20internet%20users%202025&text=As%20of%20February%202025%2C%20China,around%20322%20million%20internet%20users.>

³ Trinh V. D. Vietnam's struggle with cyber security // East Asia Forum, 20.03.2024. URL: <https://eastasiaforum.org/2024/03/20/vietnams-struggle-with-cyber-security/>

⁴ 20% of Vietnamese online vulnerable to cyberthreats // Vietnam News Agency, 18.09.2024.

URL: <https://vietnamnews.vn/economy/1663220/20-of-vietnamese-online-vulnerable-to-cyber-threats.html>

⁵ Chang L. Y. C. Legislative frameworks against cybercrime: The Budapest convention and Asia // The Palgrave Handbook of International Cybercrime and Cyberdeviance. June 6, 2020. – Pp. 327-343.

⁶ Gohwong S. G. The Cyber-attacks in Vietnam during 2010-2016 // Asian Political Science Review. 2017. Vol. 1. No. 1.

⁷ Dillon R., Tan K. L. Cybersecurity workforce landscape, education, and industry growth prospects in Southeast Asia // Journal of Tropical Futures. 2024. Vol. 1. No. 2. P. 172-181.

- ⁸ Кокушкина И.В., Макухин А.Г., Ле Минь Ха. Сотрудничество РФ и СРВ в XXI веке: SWOT-анализ особенностей, проблем и перспектив развития // Вьетнамские исследования. 2024. Т. 8. No 4. С. 18—32.
- ⁹ Luật Giao dịch điện tử nước Cộng hoà xã hội chủ nghĩa Việt Nam Số: 51/2005/QH11 ngày 29 tháng 11 năm 2005 [Закон об электронных сделках Социалистической Республики Вьетнам] №51/2005/QH11, 29.11.2005. URL: <https://thuvienphapluat.vn/van-ban/Thuong-mai/Luat-Giao-dich-dien-tu-2005-51-2005-QH11-6922.aspx>
- ¹⁰ Glennon M. J. State-level cybersecurity // Policy Review. 2012. No. 171.
- ¹¹ Gohwong S. G. The Cyber-attacks in Vietnam during 2010-2016 // Asian Political Science Review. 2017. Vol. 1. No. 1.
- ¹² Thai D. N. Vietnam has no choice but to counter China's cyber thuggery // VnExpress International, 01.06.2020. URL: <https://e.vnexpress.net/news/perspectives/vietnam-has-no-choice-but-to-counter-china-s-cyber-thuggery-4107109.html>
- ¹³ Chinese hackers accused of attacking Vietnamese websites // Báo Đà Nẵng, 14.05.2014. URL: <https://www.baodanang.vn/english/education-science/201405/chinese-hackers-accused-of-attacking-vietnamese-websites-2328550/>
- ¹⁴ Phuy, H. Two Chinese hackers blamed for attack on over 200 Vietnamese websites // Vietnamnet global. 14.05.2014. URL: <https://vietnamnet.vn/en/two-chinese-hackers-blamed-for-attack-on-over-200-vietnamese-websites-E102283.html>
- ¹⁵ Chinese hackers attack VN's airports and Vietnam Airlines' website // Việt Nam News. 29.07.2016. URL: <https://vietnamnews.vn/society/300416/chinese-hackers-attack-vns-airports-and-vietnam-airlines-website.html>
- ¹⁶ Dao, J., Tran, G.T.H. and Trinh, T.N. New law on cyber security in Vietnam // Tilleke & Gibbins International Ltd. 03.06.2016. URL: <https://www.tilleke.com/insights/new-law-cyber-security-vietnam/>
- ¹⁷ Cohen J., Ing C. Regional Guide to Cybersecurity and Data Protection in Mainland Southeast Asia // Tilleke & Gibbins, 10.07.2024. URL: <https://www.tilleke.com/insights/regional-guide-cybersecurity-and-data-protection-mainland-southeast-asia/>
- ¹⁸ Over 20 million cyberattacks warnings detected in Q1 // Vietnam News Agency, 04.04.2024. URL: <https://en.vietnamplus.vn/over-20-million-cyberattack-warnings-detected-in-q1-post283997.vnp>
- ¹⁹ Кокушкина И.В., Макухин А.Г., Ле Минь Ха. Сотрудничество РФ и СРВ в XXI веке: SWOT-анализ особенностей, проблем и перспектив развития // Вьетнамские исследования. 2024. Т. 8. No 4. С. 18—32.
- ²⁰ Ministry of Public Security of Socialist Republic of Vietnam. Police dismantle large-scale online illegal gambling group, 18.10.2024. URL: <https://en.bocongan.gov.vn/news-events/police-dismantle-large-scale-online-illegal-gambling-group-t11254.html>
- ²¹ Gushin F., Bromberg P. Vietnam gaming // Inside Asian Gaming. 16.11.2023. URL: <https://as-gam.com/2023/11/16/vietnam-gaming/>
- ²² Binh, T. Cybercrime in Vietnam inflicts losses of around US\$743 million // Sài Gòn Giải Phóng. 16.12.2024. URL: [https://en.sggp.org.vn/cybercrime-in-vietnam-inflicts-losses-of-around-us743-million-post114525.html#:~:text=In%202024%2C%20a%20concerning%20number,trillion%20\(US\\$24742.28%20million\)](https://en.sggp.org.vn/cybercrime-in-vietnam-inflicts-losses-of-around-us743-million-post114525.html#:~:text=In%202024%2C%20a%20concerning%20number,trillion%20(US$24742.28%20million))
- ²³ Binh, T. Cybercrime in Vietnam inflicts losses of around US\$743 million.
- ²⁴ Fourrage L. Cambodia Cybersecurity Job Market: Trends and Growth Areas for 2024. 24.12.2024. URL: <https://www.nucamp.co/blog/coding-bootcamp-cambodia-khm-cambodia-cybersecurity-job-market-trends-and-growth-areas-for-2024>
- ²⁵ Nguon S., Srun S. Cambodia v. Hackers: Balancing Security and Liberty in Cybercrime Law // Konrad Adenauer Stiftung, 27.01.2020. URL: <https://www.kas.de/en/web/kambodscha/single-title/-/content/cambodia-v-hackers-balancing-security-and-liberty-in-cybercrime-law>
- ²⁶ Royal Government of Cambodia, Sub-Decree on Implementation of Telecommunications and ICT Development Policy 2015. URL: https://data.opendevdevelopmentcambo-dia.net/km/laws_record/law-on-telecommunications/resource/6716c7ab-7ae0-4a7c-91c5-6cb02035054c
- ²⁷ Royal Government of Cambodia, Sub-Decree on Implementation...
- ²⁸ United Nations Commission on Human Rights Report by Special Rapporteur Rhona Smith, 24.08.2020. URL: <https://digitallibrary.un.org/record/3885831?v=pdf>
- ²⁹ Cambodia: Freedom on the Net 2024 Country Report // Freedom House. URL: <https://freedomhouse.org/country/cambodia/freedom-net/2018>

³⁰ Bunthan P., Cohen J. What Cambodia's New Law on Electronic Commerce Means for Business // Tilleke & Gibbins International Ltd. 02.03.2020. URL: <https://www.tilleke.com/insights/what-cambodias-new-law-electronic-commerce-means-business/>

³¹ Cybersecurity in Cambodia: Current development and challenges ahead // Library records OD Mekong Datahub. 03.12.2024. URL: https://data.opendevlopmentmekong.net/library_record/cybersecurity-in-cambodia-current-development-and-challenges-ahead

³² Novo, L. The UN finally advances a convention on cybercrime . . . and no one is happy about it // Atlantic Council. 14.08.2024. URL: <https://www.atlanticcouncil.org/blogs/new-atlantist/the-un-finally-adopts-a-convention-on-cybercrime-and-no-one-is-happy/>

³³ ASEAN leaders to agree to cooperate in fighting cyber scams // The Independent, 10.05.2023. URL: <https://www.independent.co.uk/news/asean-ap-myanmar-indonesia-people-b2336230.html>.

³⁴ United Nations Commission on Human Rights. Hundreds of thousands trafficked to work as online scammers in SE Asia. 29.08.2023. URL: <https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report>

³⁵ U.S. Department of State. 2023 Trafficking in Persons Report. 06.2023. URL:

<https://www.state.gov/reports/2023-trafficking-in-persons-report/>

³⁶ Kennedy L., Paul Southern N. Cambodia's Billion Dollar Scam // The Dial. 15.10.2024. URL: <https://www.thedial.world/articles/news/issue-20/cambodia-cyber-scams-human-trafficking>.

³⁷ Kennedy L., Paul Southern N. Cambodia's Billion Dollar Scam.

³⁸ Cambodia extradites 130 Chinese nationals in fraud crackdown, // China Daily, 13.04.2024.

URL: https://www.chinadaily.com.cn/a/202404/13/WS661a1070a31082fc043c1c7a_1.html.

³⁹ Keeton-Olsen, A. Cambodia: Chinese-linked scam industry persists in Sihanoukville despite raids // Business & Human Rights Resource Centre. 18.03.2024. URL: <https://www.business-humanrights.org/en/latest-news/cambodia-chinese-linked-scam-industry-persists-in-sihanoukville-despite-raids/>.

⁴⁰ Ravindran S. US to scale up cyber security ties with Cambodia // Khmer Times, 24.08.2023.

URL: <https://www.khmertimeskh.com/501348276/us-to-scale-up-cyber-security-ties-with-cambodia/>