УДК 321.01-049.5:[343.3/.7:004.056](100)

Б. И. ШУМСКАЯ,
магистр политических наук,
Институт социологии Национальной академии наук Беларуси,
Минск, Беларусь
E-mail: bsumskaa@gmail.com

МЕЖДУНАРОДНОЕ ПРОТИВОДЕЙСТВИЕ КИБЕРТЕРРОРИЗМУ В США, ГЕРМАНИИ, КИТАЕ И ФИНЛЯНДИИ

Выполнен анализ национальных киберстратегий Соединенных Штатов Америки, Федеративной Республики Германия, Китайской Народной Республики и Финляндской Республики в контексте противодействия кибертерроризму. Рассмотрены ключевые направления политики кибербезопасности, отвечающие за киберзащиту и нейтрализацию цифровых угроз. Выявлены особенности подходов, обусловленные политическими, экономическими и культурными факторами, определен баланс между свободой и контролем в цифровой сфере.

Ключевые слова: кибертерроризм, кибератаки, киберстратегия, национальная безопасность

B. SHUMSKAYA,
Master of Political Science,
Institute of Sociology of the National Academy of Sciences of Belarus, Minsk, Belarus
E-mail: bsumskaa@gmail.com

INTERNATIONAL COUNTERACTION TO CYBERTERRORISM IN THE USA, GERMANY, CHINA AND FINLAND

The analysis of the national cyber strategies of the United States of America, the Federal Republic of Germany, the People's Republic of China and the Republic of Finland in the context of countering cyberterrorism is carried out. The key areas of cybersecurity policy responsible for cyber defense and neutralization of digital threats are considered. The peculiarities of approaches determined by political, economic and cultural factors are revealed, and the balance between freedom and control in the digital sphere is determined.

Keywords: cyberterrorism, cyberattacks, cyberstrategy, national security

В XXI в. информационные технологии трансформируют ландшафт геополитики. Они эволюционировали из катализатора всемирного прогресса в поле битвы и эпицентр зарождения конфликтов нового поколения. Одной из острых и трудно прогнозируемых угроз современного мира выступает кибертерроризм – использование цифрового пространства с целью запугивания, разрушения критической инфраструктуры и подрыва общественно-политической обстановки. Исследование сфокусировано вокруг анализа международных подходов к противодействию этой угрозе в США, Германии, Китае и Финляндии. Выбор перечисленных государств обусловлен их разнообразным опытом

и приоритетами на политико-экономическом пространстве, что позволяет всесторонне оценить спектр стратегий противодействия кибертерроризму.

На данный момент международное регулирование борьбы против кибертерроризма находится на стадии формирования. Центральное место в системе занимает принятая в Будапеште в 2001 г. Конвенция о преступности в сфере компьютерной информации, которая устанавливает общие принципы национального уголовного законодательства в области киберпреступности и определяет механизмы международного сотрудничества [1].

Международная защита от киберугроз поддерживается и рядом других документов. Резолюции Генеральной Ассамблеи Организации Объединенных Наций (ООН) регулярно поднимают вопросы информационной безопасности, призывая к сотрудничеству в борьбе с использованием информационных и операционных технологий в преступных целях и задавая общие ориентиры. Принципы поведения государств в киберпространстве, разработанные Группой правительственных экспертов ООН, содержат рекомендации по ответственному поведению государств. Данные принципы ориентированы на уважение суверенитета, предотвращение конфликтов и вмешательства во внутреннюю политику государств [2].

Весомую роль в системе международной кибербезопасности играют международные стандарты. Международная организация по стандартизации (ISO) [3] и Международная электротехническая комиссия (IEC) [4] предлагают стандарты управления информационной безопасностью. Такого рода нормативные документы служат руководством по внедрению лучших практик и технологий защиты в системы инфраструктуры.

Международные усилия формируют общую рамку для борьбы с кибертерроризмом. Результативность предотвращения киберугроз зависит от национальной политики и целей государств.

Соединенные Штаты Америки традиционно занимают лидирующие позиции в разработке и реализации политики противодействия кибертерроризму. Принятая в марте 2023 г. Стратегия национальной кибербезопасности США является комплексным документом, отражающим эволюцию американского подхода к обеспечению безопасности в киберпространстве. Стратегия основана на пяти основополагающих принципах: защите критической инфраструктуры, разрушении цепочек киберпреступности, инвестировании в киберустойчивость, международном сотрудничестве и переформатировании вектора распределения ответственности за кибербезопасность [5, p. 4].

Американский подход исходит из государственно-частного партнерства – это и есть специфика политической и экономической системы США. Стратегия предусматривает перераспределение ответственности за кибербезопасность, возлагая больше обязанностей на наиболее технологически развитые и ресурсообеспеченные организации, включая операторов критической

инфраструктуры и разработчиков программного обеспечения. Новый подход ориентирован на устранение рыночных диспропорций, когда затраты на гарантии безопасности несут конечные пользователи, а не производители технологий.

В мае 2024 г. США выпустили еще один весомый документ – «Международное киберпространство США и стратегия цифровой политики», в котором указано: «США будут использовать все инструменты национальной мощи – дипломатические, экономические, правоохранительные, разведывательные и военные, для сдерживания и противодействия злонамеренным киберугрозам. США оставляют за собой право на “согласованный ответ” в случае кибератак на критическую инфраструктуру и другие ключевые цели» [6, p. 12].

Стратегия описывает действия и угрозы террористов, которые вероятны в киберпространстве: «Злонамеренная деятельность включает использование информационно-коммуникационных технологий для распространения пропаганды насилия; поощрение радикализации и мобилизации для совершения актов насилия; вербовку людей в террористические организации; подготовку, планирование и координацию атак и финансирование террористических актов» [6, p. 14]. Соединенные Штаты стремятся продвигать две международные нормы поведения в киберпространстве: запрет атак на критическую гражданскую инфраструктуру и злоупотребление информационно-коммуникационными технологиями для целей террора.

Анализ американской стратегии противодействия кибертерроризму выявляет ее тесную связь с общей внешнеполитической линией США, направленной на сохранение глобального лидерства. Стратегия рассматривает киберпространство как сферу стратегической конкуренции, в которой страна стремится доминировать и продвигать собственные политические ценности. В документе прямо указаны основные противники США в киберпространстве: Россия, Китай, Иран и Северная Корея, международные террористические организации. Соединенные Штаты возлагают ответственность на эти государства за кибертеррористические атаки, совершаемые с их территории. США намерены добиваться привлечения стран к ответственности санкциями, дипломатическим средствами и правовыми инструментами [6, p. 12–14].

Стратегия кибербезопасности Германии началась с одноименного документа 2011 г. Данный документ представляет собой первую комплексную попытку государства систематизировать и институционализировать политику в области кибербезопасности. Стратегия подчеркивает растущую зависимость всех сфер общественной жизни от киберпространства – от экономики и госуправления до личной безопасности граждан. Цель Германии – построить устойчивую и безопасную цифровую инфраструктуру, которая даст отпор внутренним и внешним угрозам, не нарушая при этом свободы слова и открытости киберпространства [7, p. 2].

В Стратегии отмечается, что кибератаки становятся всё более частыми, сложными и профессиональными. Их источниками могут быть как преступные группировки, так и государственные и негосударственные субъекты. Германия встревожена вирусом Stuxnet, который доказал уязвимость к целенаправленным атакам промышленных систем [7, p. 3–4].

Немецкая стратегия кибербезопасности 2011 г. охватывает в числе прочих следующие направления: защита критической инфраструктуры, безопасные информационные технологии для граждан и бизнеса, укрепление информационной безопасности в государственных органах, создание центра реагирования на киберинциденты и национального совета по кибербезопасности [4, p. 6–10]. Вырабатываются новейшие векторы борьбы с кибепреступностью, где существует международная координация сил, разработка высокозащищенных ИТ-решений и механизмов реагирования на атаки [7, p. 10–12]. Киберстратегия 2011 г. – структурированный план формирования комплексной системы кибербезопасности. Основными ее принципами являются: координация действий, международное сотрудничество, публично-частное партнерство, акцент на превентивных мерах и институциональное развитие. Германия выступает за кибербезопасность как за всеобщее благо.

Доклад «Ситуация с ИТ-безопасностью в Германии 2021 года» описывает более актуальное понимание киберугроз и отвечает острым вызовам с приходом глобальной цифровизации. В отличие от стратегии 2011 г., в которой основное внимание уделялось построению фундаментальной системы кибербезопасности, версия 2021 сфокусирована на конкретных угрозах, таких как кибератаки на критическую инфраструктуру, масштабные уязвимости программного обеспечения, атаки программ-вымогателей и социальная инженерия [8, p. 9–10]. Главное отличие от стратегии 2011 г. сводится к тому, что киберриски 2021 г. превратились в профессиональные, системные и разрушительные. Подчеркивается, что киберпространство используется не только преступниками, но и государственными структурами в целях шпионажа, саботажа и подрыва процессов в обществе.

Данный документ выделяет проблему безопасности критической инфраструктуры. В 2021 г. было зафиксировано более 1 000 случаев, связанных с ИТ-безопасностью в ее секторах, среди которых – энергетика, водоснабжение, здравоохранение, транспорт и финансы. Отмечено, что противодействие вредоносным атакам предъявляет все более высокие технические требования [8, p. 7].

Структуры национальной безопасности Германии рассматривают данные атаки как нетрадиционный элемент гибридной войны и признают риск террористических проявлений в будущем. Контрмеры и стратегия борьбы строятся вокруг пяти составляющих:

1) усиление систем раннего предупреждения отчетностью эпизодов атак;

2) массовое внедрение многофакторной аутентификации;

3) повышение информационной грамотности населения;

4) расширение сотрудничества с частным сектором;

5) устранение дефицита специалистов в области информационной безопасности.

В отличие от подхода Соединенных Штатов немецкая тактика модернизирует культуру кибеграмотности. Информационные кампании и образовательные программы формируют ответственное поведение в Сети. Данный аспект показывает ярко выраженную европейскую политическую культуру, где присутствует внимание к социальным аспектам национальной безопасности.

Цифровой суверенитет является визитной карточкой Германии. Акцент в нем поставлен на производство технологий и снижение зависимости от иностранных поставщиков программного и аппаратного обеспечения. Указанный аспект имеет важное политическое значение, поскольку отражает стремление страны к большей автономии в сфере кибербезопасности в контексте сложных отношений с США и растущих опасений в связи с китайским технологическим влиянием.

Немецкий подход придерживается высокой степени институционализации и четкого разграничения полномочий между органами в государстве. Ведущее место в системе кибербезопасности отводится Федеральному ведомству по информационной безопасности (Bundesamt für Sicherheit in der Informationstechnik, BSI), координирующему деятельность по предотвращению и нейтрализации киберугроз. Стратегия предусматривает укрепление потенциала BSI и развитие межведомственного взаимодействия. В центре внимания стратегии – оперативность, адаптивность, технологическая независимость и несокрушимость перед лицом цифровых угроз. Борьба с кибератаками и кибертерроризмом строится на сочетании превентивных мер, резкого реагирования, технологического обновления и международного взаимодействия.

Китайский подход к противодействию кибертерроризму существенно отличается от западных моделей и отражает специфику политической системы Китайской Народной Республики (КНР). Институциональная структура кибербезопасности страны централизована. Администрация киберпространства Китая (Cyberspace Administration of China, CAC) подчинена высшему руководству и наделена широкими полномочиями по регулированию Интернета и обеспечению кибербезопасности. Централизация позволяет координировать усилия и своевременно отвечать на атаки терроризма.

«Стратегия кибербезопасности Китая – 2014» строится вокруг идеи «национального суверенитета в киберсреде», то есть права государства контроли-

ровать информационное пространство в пределах своих границ. Ограничение идет на уменьшение влияния западных сил. Основополагающий тезис национальной стратегии – гарантия киберсуверенитета как основы национальной безопасности [9, p. 6–8].

Китай видит свое цифровое поле как арену геополитического противостояния, сравнимую с сушей, морем, воздухом и космосом, что отражается в милитаризации информационной политики и роли Народно-освободительной армии Китая (НОАК) в киберпространстве [9, p. 10–11]. Философия властных органов построена на механизме информационного контроля, где политическая и социальная стабильность возможны при надзоре за киберпространством. Западная модель считается хаотичной и угрожающей.

В декабре 2016 г. Китай опубликовал Национальную стратегию безопасности кибепространства. Борьба с кибератаками и террористическим воздействием в ней представлена следующим образом:

1) создана государственная киберсила в лице Единого бюро по сетевым операциям и отдела военной разведки, ответственных за наступательные и оборонительные кибероперации;

2) действует модель «Великого китайского файрвола», фильтрующего контент и ограничивающего доступ к иностранным ресурсам;

3) власти разрабатывают заменители западных технологий (ОС Kylin и платформы вместо Microsoft, Google, Apple);

4) правительство требует передачу данных от частных организаций;

5) сотрудничество китайских технологических гигантов с правительством в качестве национального «кибершита»;

6) построена стратегия борьбы с «трехглавой угрозой» – терроризмом, экстремизмом и сепаратизмом, включая киберсферу;

7) безопасный Интернет – база цифровой экономики, то есть защита деловых интересов, технологических разработок и интеллектуальной собственности [10].

1 июня 2017 г. вступил в силу Закон Китайской Народной Республики «О кибербезопасности». Он регулирует действия в Интернете, защиту персональных данных, киберинфраструктуру и цифровой суверенитет. В качестве примера приведем две статьи о борьбе с кибертерроризмом. Статья 37 затрудняет использование данных, собранных в Китае, для организации кибертеррористических атак извне, так как требует их хранения на территории страны и оценки безопасности при передаче за границу. Статья 47 позволяет мгновенно найти и заблокировать контент, который может быть использован для планирования, координации или пропаганды кибертеррористических действий [11].

Китайский подход к противодействию кибертерроризму тесно увязан со Стратегией национальной безопасности КНР. Кибербезопасность выведена

там как неотъемлемый компонент системной безопасности государства, а контроль над информационным пространством – как инструмент политической стабильности. Специфика политической системы Китая кроется в отношении к информационным угрозам как дестабилизирующему фактору.

Финляндия представляет научный интерес в контексте сравнительного анализа национальных стратегий противодействия кибертерроризму, так как страна признана лидером в области кибербезопасности. На данный момент в Финляндии разработано две киберстратегии: от 2019 г. и обновленная версия от 2024 г. Обе стратегии зациклены на обеспечении кибербезопасности в государстве. Различаются они лишь по приоритетам и подходам в зависимости от изменений в глобальной и национальной обстановке.

Стратегия от 2019 г. определила основные национальные цели в области развития киберсреды и защиты жизненных функций общества. Всего их три:

1) международное укрепление связей с зарубежными партнерами для защиты киберпространства без границ;

2) введение должности директора по кибербезопасности в Министерстве транспорта и коммуникаций, чтобы отслеживать и согласовывать национальное развитие в этой сфере;

3) развитие компетенций и навыков в цифровой среде, вовлечение университетов, исследовательских центров и частного сектора [12, p. 5–9].

Методы сопротивления киберугрозам построены по поверхностному принципу. Выполняется анализ кибератак, разрабатываются модели реагирования, принимаются правоохранительные и дипломатические контрмеры и осуществляется интеграция кибербезопасности в экономическое развитие.

Обновленная стратегия 2024 г. существенно расширила свои функции с учетом пандемии COVID-19, спецоперации России в Украине и вступления Финляндии в НАТО. Произошла интеграция в общую систему безопасности государства и были выполнены требования Директивы Европейского союза (ЕС) по кибербезопасности NIS2. В стратегии содержатся уже четыре стратегических фокуса в кибердеятельности:

1) создание компетентной и инновационной экосистемы на всех уровнях образования и труда. Ставка делается на искусственный интеллект, квантовые вычисления, криптографические технологии;

2) киберустойчивость общества на основе разработки стандартов для населения и критической инфраструктуры. Проводятся киберучения с акцентом на межсекторное сотрудничество;

3) надежная модель национального и международного сотрудничества по обмену данными и методами противостояния угрозам;

4) четкое распределение полномочий в реагировании на киберинциденты, в будущем – подготовка национальной доктрины киберзащиты [12, p. 6–8].

В 2024 г. борьба с кибератаками стала включать следующие направления: расширение прав правоохранителей, платформа мгновенного реагирования, усиленная защита критических секторов (энергетика, финансы, здравоохранение), поддержка отечественных ИТ-решений (open source, криптография) [13, p. 17–20].

Основное отличие между стратегиями Финляндии заключается в их фокусе и масштабе. Стратегия 2019 г. опирается на международное сотрудничество, координацию и развитие компетенций. В то время как стратегия 2024 г. расширяет эти направления, интегрируя кибербезопасность в общую концепцию национальной безопасности и уделяя особое внимание инновациям, устойчивости и международным обязательствам в рамках ЕС и НАТО.

Финский подход характеризуется высокой степенью децентрализации и вовлечением бизнеса, научного сообщества и гражданского общества. Стратегия предусматривает развитие государственно-частного партнерства, создание центров компетенций по кибербезопасности и формирование инновационной экосистемы. В противодействии кибертерроризму она отдает приоритет превентивным мерам, устойчивости критической информационной инфраструктуры, регулярному проведению киберучений, модернизации систем раннего предупреждения об угрозах и всестороннему международному взаимодействию. Защита демократических институтов и процессов от кибератак имеет первостепенное значение.

Национальные киберстратегии признают кибертерроризм одной из разрушительных угроз национальной безопасности. Различия в подходах в борьбе с ним зависят от политических, экономических и культурных факторов. Первая составляющая связана с политическими системами государств. Американская стратегия представлена либеральной моделью с государственно-частным партнерством и минимальным регулированием. Германский подход характеризуется большим вниманием к правовым аспектам и защите прав человека, что соответствует европейской политической традиции. Китайская стратегия демонстрирует более централизованный подход с сильным государственным контролем. Финский подход иллюстрирует скандинавскую модель с упором на децентрализацию, вовлечение различных заинтересованных сторон и развитие человеческого капитала.

Влияние экономических аспектов на формирование национальных киберстратегий очевидно. США рассматривают кибербезопасность как фактор конкурентоспособности и индустриального развития. Германия стремится к развитию национальной индустрии кибербезопасности как части стратегии цифрового суверенитета. Китай активно развивает собственные технологии и стремится к лидерству в ведущих областях. Финляндия позиционирует себя как центр компетенций в области кибербезопасности, стремясь привлечь международные инвестиции и талантливых специалистов.

Культурные факторы также влияют на киберстратегии. В США выбирают свободу слова и осторожный подход к регулированию Интернета. Германия делает ставку на строгую защиту данных граждан. Китай применяет более жесткий контроль, опираясь на ценности коллективизма. Финляндия пытается повысить цифровую грамотность и развить культуру ответственного поведения в Сети.

Связующим компонентом контртеррористических действий является отношение представленных стратегий к интеграции международного сотрудничества. США стремятся к повсеместному лидерству и продвижению собственных стандартов кибербезопасности, что отражает их общую внешнеполитическую линию. Германия делает акцент на региональном сотрудничестве и гармонизации подходов в рамках ЕС. Китай активно позиционирует концепцию «киберсуверенитета» и движется к массовому влиянию в мировом управлении Интернетом. Финляндия проявляет активность в международных инициативах и формирует коалиции единомышленников в сфере кибербезопасности.

Таким образом, анализ национальных стратегий противодействия кибертерроризму выявил общие элементы: защита критической инфраструктуры, развитие государственных компетенций и поддержка международного сотрудничества. Данные составляющие создают основу новой международной системы кибербезопасности. В то же время формирование стратегий определяется не только техническими аспектами, но и более широкими факторами: политическими, экономическими и культурными особенностями государств, их видением роли государства, баланса между безопасностью и свободой, а также места в международной политике.

Список использованных источников

1. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // Гарант.ру. – URL: https://base.garant.ru/4089723/ (дата обращения: 05.04.2025).

2. Организация Объединенных Наций (ООН) : [веб-сайт]. – URL: https://www.un.org/ (дата обращения: 05.04.2025).

3. International Organization for Standardization (ISO) : [website]. – URL: https://www.iso.org/ (date of access: 05.04.2025).

4. International Electrotechnical Commission (IEC) : [website]. – URL: https://www.iec.ch/ (date of access: 05.04.2025).

5. The White House USA. National Cybersecurity Strategy / The White House USA. – Washington, D. C. : The White House, 2023. – 39 p.

6. U. S. Department of State. United States International Cyberspace and Digital Policy Strategy / U. S. Department of State. – Washington, D. C. : DOS, 2024. – 61 p.

7. Cyber Security Strategy for Germany / Federal Ministry of the Interior. – Berlin : BMI, 2011. – 14 p.

8. The State of IT Security in Germany in 2021 / Federal Office for Information Security. – Bonn : BSI, 2021. – 94 p.

9. *Chang, A*. Warring state: China's cybersecurity strategy / A. Chang. – Washington : Center for a New American Security, 2014. – 43 p.

10. China's National Cyber Security Strategy 2016 // Cyberspace Administration of China. – URL: https://www.cac.gov.cn/2016-12/27/c_1120195926.htm (date of access: 05.04.2025).

11. Cybersecurity Law of the People's Republic of China 2017 // DIGICHINA. – URL: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (date of access: 05.04.2025).

12. Finland's Cyber Security Strategy / Security Committee of Finland. – Helsinki : SC, 2019. – 16 p.

13. Finland's Cyber Security Strategy 2024–2035 / Prime Minister's Office. – Helsinki : PMO Finland, 2024. – 44 p.

Поступила 15.04.2025 г.