Международный опыт и выводы для планирования защиты критической инфраструктуры

GUO Dongjun, WU Yanhua, ZHAO Hongxu, ZHU Xingping, CUI Tao, CHEN Zhilong

Аннотация: В современных войнах основные направления ударов постепенно смещаются от экономических объектов к критической инфраструктуре; ее защита напрямую влияет на структуру городских систем и планирование территориального пространства. В сфере гражданской противовоздушной обороны Китая существуют две базовые задачи: защита городского населения, которая уже реализуется через планирование и строительство сооружений гражданской обороны, и защита важных экономических объектов и критической инфраструктуры. Последняя задача на государственном уровне и в ряде провинций и муниципалитетов признана подлежащей включению в национальное комплексное планирование и планирование территориального пространства, однако практическая реализация пока ограничена. В статье уточняются понятия важного объекта, важного экономического объекта и критической инфраструктуры, рассматривается состояние планирования их защиты, а также подробно анализируется эволюция основных рамок четырех версий National Infrastructure Protection Plan США, опубликованных с 2006 г.: видение, миссия, цели и ключевые принципы, механизмы организации и реализации, партнерское управление рисками и практические действия. На основе международного опыта, прежде всего опыта США, предложены рекомендации для Китая, где планирование защиты критической инфраструктуры находится на начальном этапе, в части организационных механизмов, момента запуска, непрерывного совершенствования и первоочередных шагов.

Ключевые слова: критическая инфраструктура; планирование защиты; США; важный экономический объект; выводы

Классификационный номер Китайской библиотечной классификации: TU984; код документа: A

DOI: 10.16361/j.upf.202501015; номер статьи: 1000-3363(2025)01-0111-09

Сведения об авторах: GUO Dongjun, профессор, научный руководитель докторантов, Институт оборонной инженерии, Инженерный университет Сухопутных войск НОАК. Электронная почта: guo_dongjun@163.com; WU Yanhua, преподаватель, Институт оборонной инженерии, Инженерный университет Сухопутных войск НОАК; автор для корреспонденции. Электронная почта: yanhua_wu@foxmail.com; ZHAO Hongxu, магистрант, Институт оборонной инженерии, Инженерный университет Сухопутных войск НОАК; ZHU Xingping, доцент, Институт оборонной инженерии, Инженерный университет Сухопутных войск НОАК; CUI Tao, магистрант, Институт оборонной инженерии, Инженерный университет Сухопутных войск НОАК; CHEN Zhilong, профессор, научный руководитель докторантов, Институт оборонной инженерии, Инженерный университет Сухопутных войск НОАК, национальный мастер инженерных изысканий и проектирования.

Финансирование: Общий проект Национального фонда естественных наук Китая «Критерии, механизмы и ответные меры городского подземного планирования в контексте целей углеродного пика и углеродной нейтральности» (№ 52378083); общий проект Фонда естественных наук провинции Цзянсу «Микрообновление объектов и пространства для

активизации грузовой функции существующего метро: на примере линии S1/аэропортовой линии Нанкина» (№ BK20231488).

Защита критической инфраструктуры напрямую влияет на структуру городских систем и планирование территориального пространства. Планирование и строительство ряда советских промышленных городов-баз, перенесенных в район Урала до Второй мировой войны, а также китайское строительство «Третьей линии» в 1960-е гг. были практиками защитного планирования[1]. В Чунцине «Проект десятилетнего плана строительства временной столицы» 1946 г. предусматривал размещение в городе и его окрестностях многочисленных военных заводов и оборонительных сооружений, что значительно изменило городскую структуру и облик. Меры рассредоточения к пригородам сформировали и усилили пространственную организацию Чунцина по принципу «большое рассредоточение, малые концентрации, узлы в форме цветков сливы»[2]. В последних локальных войнах, а также в продолжающемся российско-украинском конфликте критическая инфраструктура неизменно становится ключевой целью ударов сторон; успех или неудача ее защиты уже может определять исход войны[1,3-4].

Защита критической инфраструктуры, рассматриваемая в данной статье, первоначально чаще называлась экономической защитой. Ее истоки восходят к периоду после Первой мировой войны, и развитие прошло три этапа. Первый, до окончания Второй мировой войны, был этапом раннего становления; показательными странами были Советский Союз, Германия и Япония. Второй, послевоенный этап, стал важным периодом развития экономической защиты: акцент сместился от противодействия воздушным налетам к защите от ракет и ядерного оружия; типичными примерами были Советский Союз, США и североевропейские страны. После краткой перестройки в 1990-е гг., по завершении холодной войны, эта сфера вступила в новый этап, характеризующийся соединением с антитеррористической защитой, предупреждением бедствий и концепцией устойчивого города[5-6]. США, в частности, приняли ряд мер политики, направленных на укрепление защиты критической инфраструктуры и обеспечение сохранения базовых функций правительства и общественных услуг в условиях преднамеренных атак, стихийных бедствий и иных чрезвычайных событий.

В целом экономическая защита эволюционировала от защиты от авиационных ударов к защите от ракетного и ядерного оружия, а объекты защиты расширились от «экономических объектов»[7] до «критической инфраструктуры и ключевых ресурсов»[8]. Многие страны с учетом собственной ситуации осуществляли планирование и практику защиты критической инфраструктуры; США, несомненно, являются пионером и типичным представителем в этой области. По открытым материалам, с момента публикации первой версии National Infrastructure Protection Plan (NIPP)[9] в 2006 г. план прошел три обновления - в 2007/2008, 2009 и 2013 гг.[10-12] - и стал руководством и опорой для защиты критической инфраструктуры США.

В Китае требования в этой сфере на государственном уровне последовательно были закреплены в Законе КНР о гражданской противовоздушной обороне[13], Законе КНР о национальной обороне[14], Законе КНР о мобилизации национальной обороны[15] и принятом Государственным советом Положении о безопасности и защите критической информационной инфраструктуры[16], где указано, что мобилизация и защита национальной экономики должны быть «включены в общие планы и программы национального развития». На уровне провинций и муниципалитетов приняты документы, например Положение Автономного района Внутренняя Монголия об управлении защитой важных экономических объектов[17], которое требует от органов гражданской обороны (развития и реформ) и отраслевых ведомств составлять общий план защиты и строительства важных экономических объектов и включать его в планы

социально-экономического развития и территориального пространства. Однако из-за отсутствия соответствующих норм планирования[18-19] практических реализаций пока немного. Опираясь на ранее выполненные авторами государственные, провинциальные и муниципальные исследования, данная статья главным образом представляет американский NIPP, чтобы содействовать разработке планов защиты критической инфраструктуры на государственном, провинциальном и муниципальном уровнях[20], а также поддержать реализацию китайских стратегий «устойчивого города» и «национальной безопасности»[21-22].

1 Критическая инфраструктура и смежные понятия

Любая теория может быть построена лишь на основе прояснения представлений и уточнения понятий. Только при общем понимании названий и понятий исследование проблемы становится ясным и последовательным, а внутренние закономерности и логические связи - более глубоко постижимыми[23]. В отношении критической инфраструктуры и смежных понятий существует множество терминов. В США последовательно использовались названия «промышленная база»[24], «экономический объект»[7], «важный объект» и «важный ресурс»[25]. В Китае эти понятия обычно объединяются выражением «важные экономические объекты». В данном разделе предпринимается попытка прежде всего уточнить содержание и объем понятий «важный экономический объект» и «критическая инфраструктура», а также их отношения с военными и политическими объектами.

Угрозы и приоритеты защиты важных экономических объектов в разных странах различаются; соответственно различаются и их определения и классификации[3]. По мере изменения военно-стратегической обстановки, экономической структуры и других факторов содержание и объем понятия важного экономического объекта также меняются. До 1990-х гг. китайское и зарубежное понимание в целом совпадало: обычно говорили об экономических объектах, а с точки зрения защитной функции основное внимание уделялось двум категориям, связанным с национальной обороной и экономической безопасностью.

С углублением понимания защитной функции объектов в зарубежной практике в сферу защиты постепенно включались цели и объекты, связанные с общественным здоровьем и безопасностью, национальным моральным духом, а также социальные объекты, относящиеся к экологической среде. В итоге было выделено 16 подсекторов, включая энергетику, критическое производство, оборонно-промышленную базу и транспортные системы[12]. Поскольку название «экономический объект» уже не охватывает больницы, относящиеся к общественному здоровью, или символические здания, влияющие на моральный дух населения, за рубежом в целом используется обобщающее понятие «критическая инфраструктура». Оно включает ресурсы и объекты, связанные с национальной обороной, экономической безопасностью, общественным здоровьем и безопасностью, моральным духом населения и экологической средой, как показано на рис. 1. Военные и часть политических объектов не относятся к гражданским объектам критической инфраструктуры.

Важные объекты в совокупности включают критическую инфраструктуру, политические и военные объекты. Между этими категориями существуют тесные связи и пересечения. Критическая инфраструктура, очевидно, включает важные экономические и социальные объекты, а также частично пересекается с важными политическими объектами, например с некоторыми правительственными объектами: низкоуровневые правительственные объекты уровня сообщества могут относиться к гражданским объектам критической инфраструктуры, тогда как органы высшего руководства следует считать политическими объектами. Взаимосвязи

между типами объектов показаны на рис. 2. В настоящей статье критическая инфраструктура понимается как гражданские объекты, имеющие значение для национальной обороны, экономической безопасности, общественного здоровья и безопасности, морального духа населения и экологической среды. Военные объекты и органы высшего руководства в эту категорию не входят.

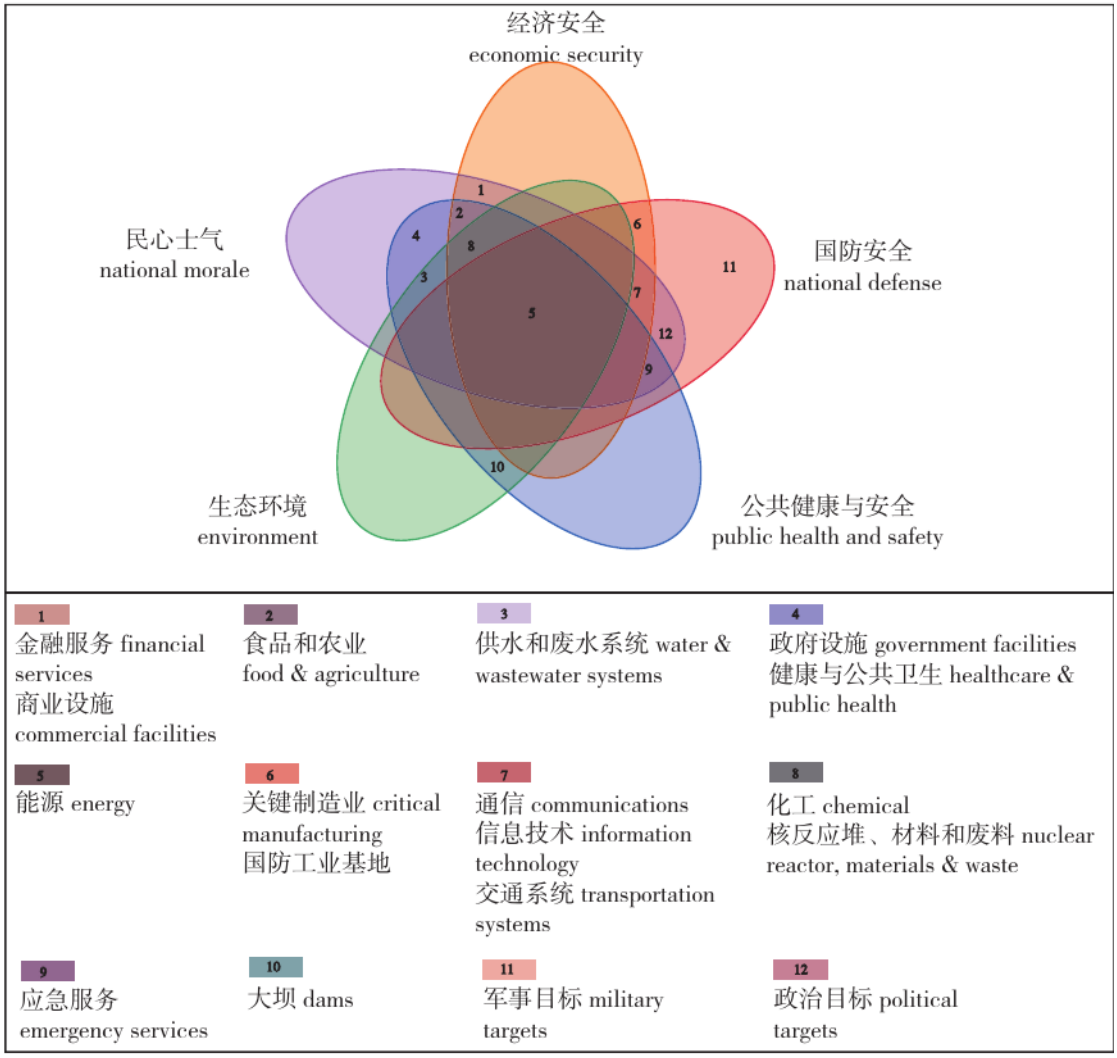

Рис.1 Классификация защитных функций критической инфраструктуры, военных и политических объектов[3,12,26]

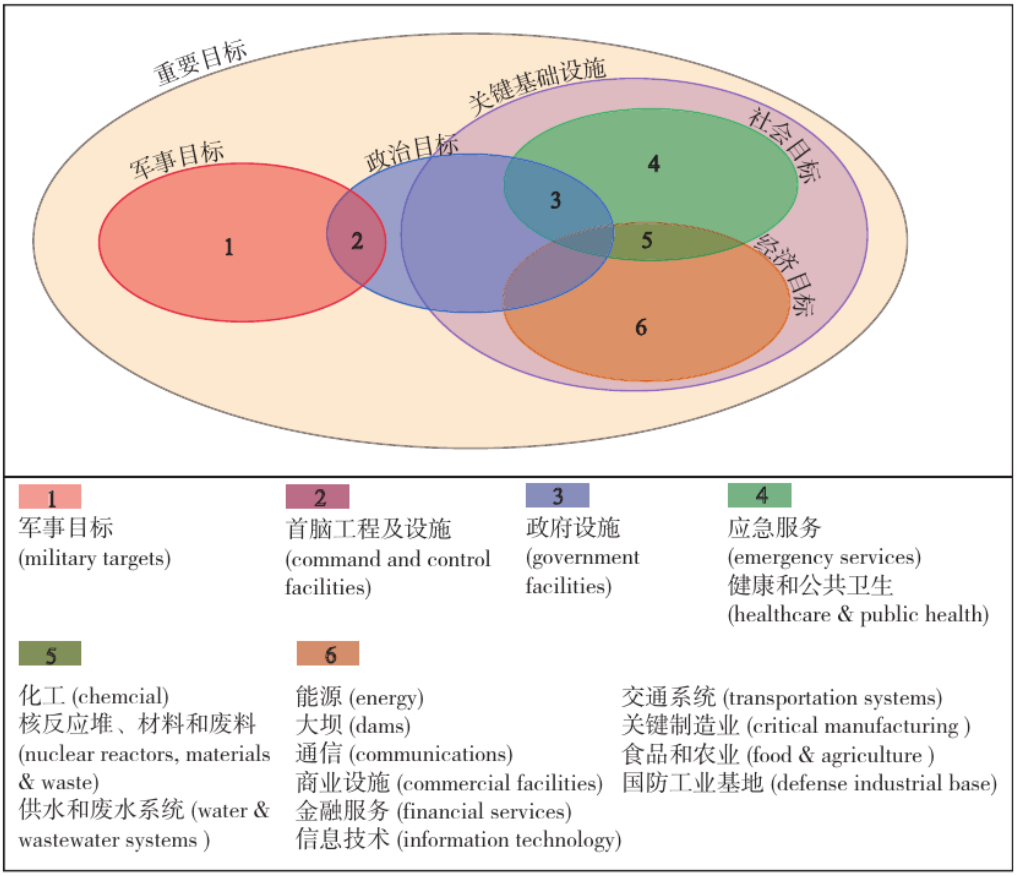

Рис.2 Соотношение критической инфраструктуры, политических объектов, военных объектов и важных объектов[3,12,26]

2 Обзор планирования защиты критической инфраструктуры в Китае и США

2.1 Планирование и строительство защиты критической инфраструктуры в Китае

Защита экономических объектов и защита населения являются двумя основными задачами гражданской противовоздушной обороны Китая[27]. С 1950-х гг., по мере принятия правил о технических мерах гражданской обороны на предприятиях, в 1960-1970-е гг. Китай сформировал и реализовал стратегию планирования и строительства «Третьей линии», основанную на принципах «опора на горы, рассредоточение, скрытность». Эта стратегия привела к перемещению значительного числа важных промышленных предприятий из приграничных и прибрежных районов во внутренние области страны. В городах одновременно строились многочисленные убежища для населения и подземные производственные цеха, сочетавшие использование в мирное время с защитой в военное время. Реализация таких планов защиты экономических объектов заметно повысила защитный потенциал страны и городов и оказала эффективное сдерживающее воздействие на возможность начала войны[28].

С 1980-х гг. до XXI в. развитие высокоточного оружия сделало стационарные экономические объекты крайне уязвимыми, что усилило значимость их защиты. Государственные органы и органы гражданской обороны неоднократно публиковали документы, призывающие укреплять защиту важных экономических объектов. Военно-гражданские исследовательские учреждения и ведомства, в свою очередь, проводили комплексные исследования интегрированной защиты, охватывающей традиционные технологии - рациональное размещение, перевод под землю, аварийно-спасательные и восстановительные работы, - а также информационные технологии

защиты, представленные помехами, ложными целями и уводом средств поражения, с целью повысить способность противодействовать воздушным ударам в военное время[28].

На уровне планирования и строительства защита критической инфраструктуры стала одной из первоочередных задач гражданской обороны[27]. Национальные законы и правила прямо требуют разработки планов защиты экономических объектов, а некоторые провинции и муниципалитеты уже начали соответствующие поиски и практики. Однако сфера защиты критической инфраструктуры чрезвычайно широка[29-30]; государственные пилотные работы все еще продвигаются в поисковом режиме, а для формирования целостной системы защиты не хватает адресных нормативных актов, эффективных организационно-управленческих механизмов и соответствующих стандартов планирования[31]. Поэтому фактических реализаций немного, а случаи включения таких планов в структуру городских систем и планирование территориального пространства еще более редки.

2.2 Планирование защиты инфраструктуры в США

В июне 2006 г. в соответствии с Директивой президента США по внутренней безопасности № 7[32] первая версия National Infrastructure Protection Plan определила распределение обязанностей между партнерами по безопасности, участвующими в защите критической инфраструктуры, создала в целом полную управленческую рамку и разработала относительно зрелую модель организационного взаимодействия и обмена информацией. План подчеркивал необходимость достижения консенсуса через широкую координацию и коммуникацию, чтобы интегрировать работу по защите критической инфраструктуры и повысить единство, непрерывность и согласованность планирования. Как важная политика обеспечения национальной безопасности и экономической стабильности США, NIPP был пересмотрен и обновлен в версиях 2007/2008, 2009 и 2013 гг. и стал значимой теоретической основой и практическим руководством по защите критической инфраструктуры США. В целом его эволюцию можно разделить на этап подготовки планирования, этап разработки и корректировки, а также этап реализации и совершенствования сопутствующей политики; ключевые временные узлы показаны на рис. 3.

Версия NIPP 2007/2008 была опубликована в конце 2007 г. и вступила в силу в 2008 г. Основная цель пересмотра состояла в лучшем реагировании на все более сложные и изменчивые киберугрозы, а также в укреплении сотрудничества и обмена информацией между различными ведомствами и отраслями для повышения общей безопасности функционирования национальной критической инфраструктуры. Хотя NIPP 2007/2008 был лишь «пакетной» корректирующей версией, он учел предыдущий практический опыт и мнения заинтересованных сторон, предложил актуальные оптимизации и стал важной опорой для переиздания NIPP в 2009 г.

Версия NIPP 2009 г. по сравнению с предыдущей не претерпела значительных изменений. Она главным образом уточнила распределение ответственности, подчеркнула модель государственно-частного партнерства, продвинула технологическое обновление и сделала акцент на долгосрочно эффективной реализации плана.

В 2013 г. Министерство внутренней безопасности США обобщило опыт практики планирования защиты инфраструктуры и впервые четко сформулировало видение, миссию, цели и принципы защиты критической инфраструктуры. Эта версия уделяет больше внимания управлению рисками, государственно-частному партнерству, обмену информацией и распределению ресурсов. Кроме того, она ясно определяет конкретные шаги реализации

защитных действий и тем самым обеспечивает важные ориентиры для долгосрочного обеспечения безопасности критической инфраструктуры США.

США продолжают исследовательскую работу над новой редакцией планирования, чтобы адаптироваться к меняющимся потребностям и вызовам защиты и безопасности. Так, в 2021-2024 гг. Агентство по кибербезопасности и безопасности инфраструктуры США (CISA) опубликовало несколько версий Infrastructure Resilience Planning Framework[41-43], помогающих правительствам штатов, местным и территориальным органам выявлять критическую инфраструктуру, оценивать риски и разрабатывать решения по обеспечению устойчивости.

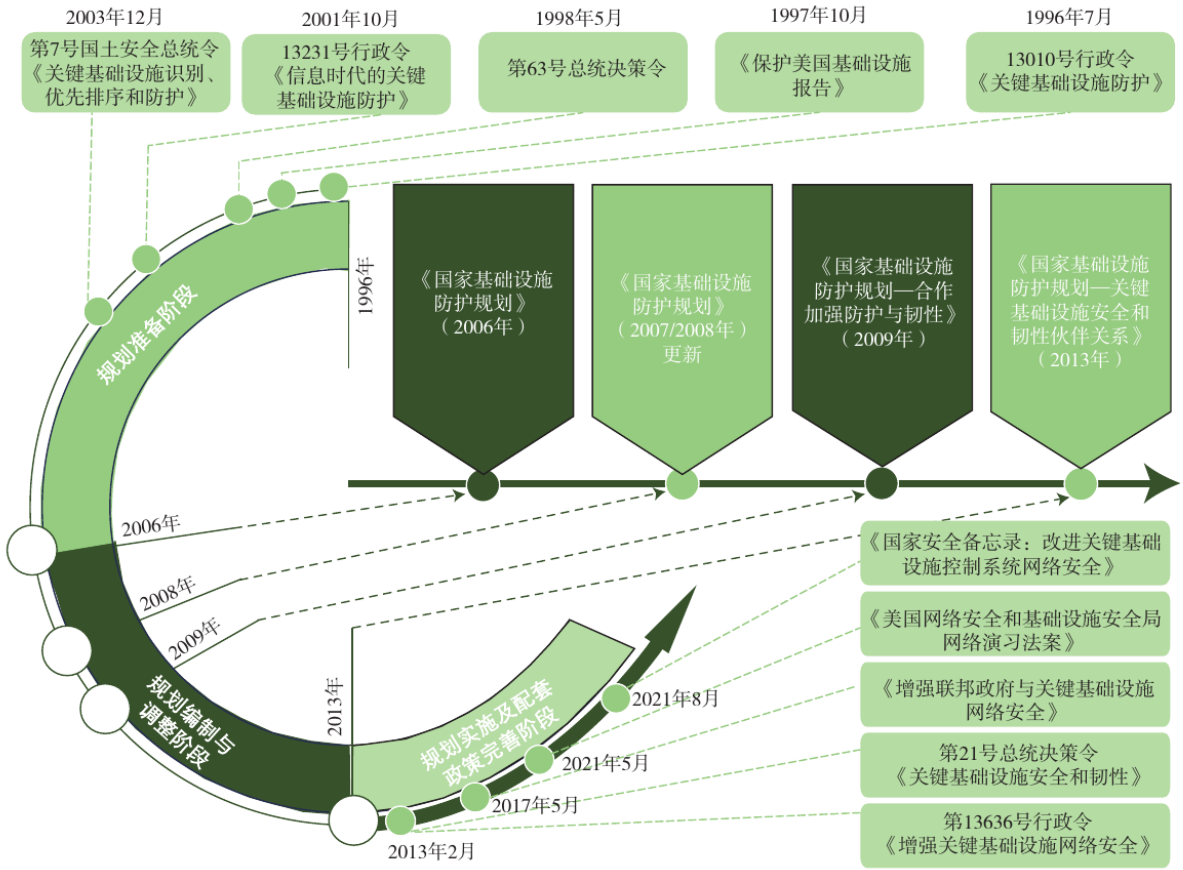

Рис.3 Основные вехи National Infrastructure Protection Plan США[8-12,32-40]

3 Основное содержание американского планирования защиты инфраструктуры

3.1 Эволюция основной рамки

NIPP прошел динамическое совершенствование и обновление в четырех версиях. Первая версия включала семь глав: введение; полномочия, роли и обязанности; стратегия планирования защиты и управление рисками; организация и партнерство для защиты критической инфраструктуры/ключевых ресурсов; интеграция защиты критической инфраструктуры и ключевых ресурсов в миссию внутренней безопасности; обеспечение долгосрочно эффективной и результативной программы; ресурсное обеспечение планирования защиты критической инфраструктуры и ключевых ресурсов. К четвертой версии число глав было сокращено с семи до шести, а содержание заметно изменилось: введение; видение, миссия и цели; среда критической инфраструктуры; ключевые принципы; партнерское управление рисками; призыв к действию (рис. 4).

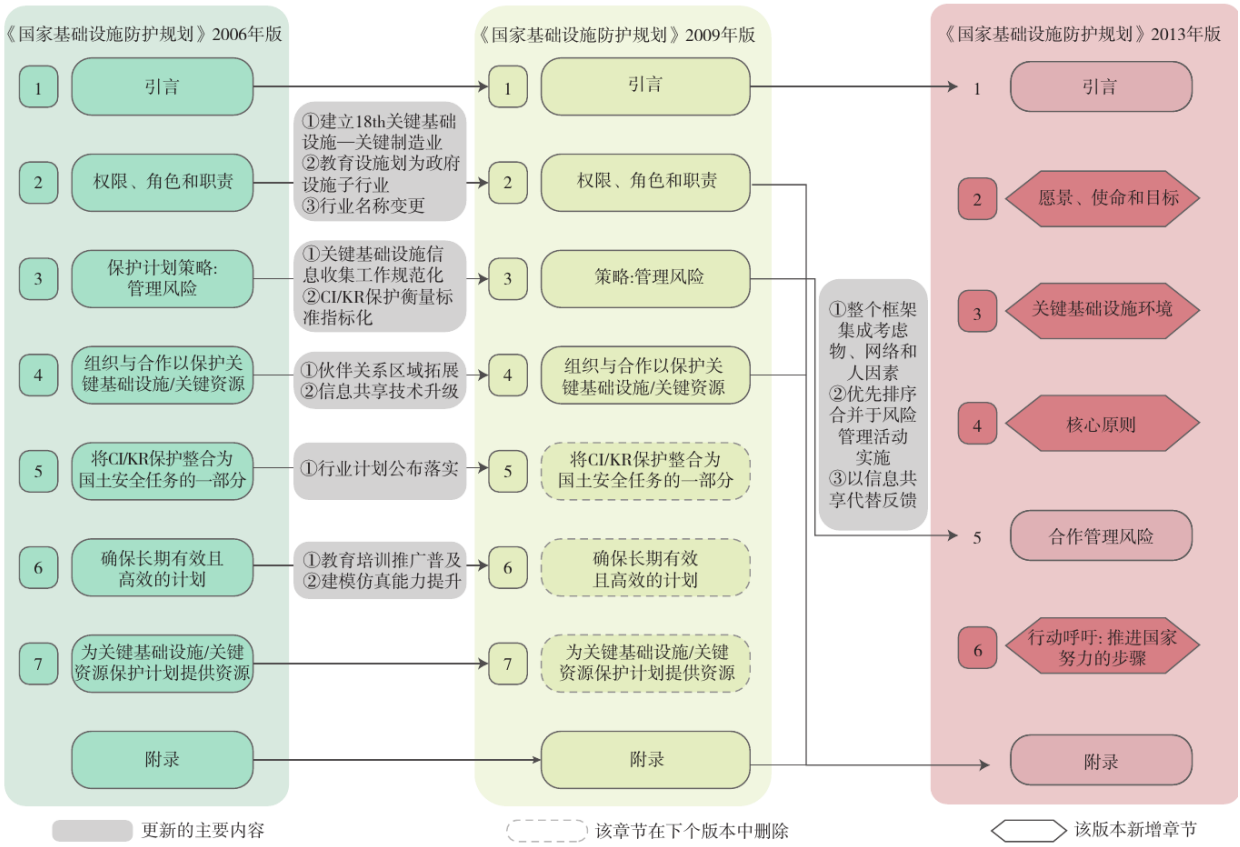

Рис.4 Эволюция основной рамки National Infrastructure Protection Plan США[9-12]

3.2 Видение, миссия, цели и ключевые принципы

Видение, миссия, цели и ключевые принципы NIPP были впервые четко изложены в версии 2013 г. Видение состоит в том, чтобы за счет снижения уязвимости, минимизации последствий бедствий, выявления и предотвращения угроз, а также усиления реагирования во время событий и восстановления после них сделать физические и киберпространственные компоненты критической инфраструктуры безопасными и устойчивыми. Миссия заключается в повышении безопасности и устойчивости национальной критической инфраструктуры через координированные и интегрированные усилия сообщества заинтересованных сторон критической инфраструктуры.

Для реализации видения и миссии NIPP выдвинул пять целей действий: обеспечивать информационную поддержку управления рисками; защищать критическую инфраструктуру от различных угроз и разрушений на основе соотношения затрат и выгод инвестиций в безопасность; укреплять устойчивость инфраструктуры через способность к быстрому восстановлению; предоставлять основу для решений посредством обмена информацией внутри сообщества критической инфраструктуры; повышать потенциал реагирования с помощью учений и тренировок.

NIPP также сформулировал семь ключевых принципов: комплексно выявлять и управлять рисками; понимать риски, связанные с зависимостями и взаимозависимостями между отраслями; обеспечивать обмен информацией между участниками инфраструктурного сообщества; учитывать особенности и преимущества различных инфраструктур; добиваться консенсуса партнеров при выявлении пробелов и улучшении безопасности и устойчивости критической инфраструктуры; укреплять международное сотрудничество; включать безопасность и устойчивость в проектирование критической инфраструктуры. Эти принципы

отражают ценности и предпосылки, которые сообщество критической инфраструктуры должно учитывать при разработке планов безопасности и устойчивости на национальном, региональном, штатном, местном, племенном и территориальном уровнях, а также на уровне собственников и операторов.

В соответствии с видением, миссией и целями NIPP заинтересованные стороны критической инфраструктуры должны сотрудничать при определении детальных приоритетов с учетом доступности ресурсов, уже достигнутых результатов, существующих технологических пробелов и возникающих рисков. Эти приоритеты стимулируют действия на национальном уровне и дополняются отраслевыми, региональными, штатными, местными и племенными приоритетами. На основе целей, приоритетов и хода реализации формируется общее понимание состояния работ по обеспечению безопасности и устойчивости критической инфраструктуры.

3.3 Механизмы планирования и реализации

Организационная архитектура защиты критической инфраструктуры была первоначально создана Директивой президента № 63, которая определила для каждой отрасли критической инфраструктуры соответствующее ведомство в качестве ведущего органа отраслевого взаимодействия, а федеральное правительство отвечало за выполнение защитных мероприятий. В 2006 г. NIPP заново классифицировал отрасли критической инфраструктуры. По мере углубления понимания их защиты отрасли переименовывались, корректировались и объединялись; при этом понятие «ключевые ресурсы» было упразднено, а единым термином стала «критическая инфраструктура». В конечном итоге было выделено 16 отраслей, и для каждой назначено федеральное ведомство или агентство в качестве основного координирующего органа - Sector-Specific Agency (SSA), как показано в табл. 1.

Табл.1 Классификация критической инфраструктуры и соответствующие курирующие органы в США[12]

关键基础设施行业分类	政府分管部门	关键基础设施伙伴关系咨询委员会					
		行业协调委员会		政府协调委员会			区域联协调委员
化工	国土安全部	√	关键基础设施跨行业委员会	√	联邦高级领导委员会	州、地方、部落和地区政府协调委员会	区域联协调委员
商业设施		√		√			
通信		√		√			
关键制造业		√		√			
大坝		√		√			
应急服务		√		√			
信息技术		√		√			
核反应堆、材料和废料		√		√			
政府设施	国土安全部、总务管理局	未设置行业协调委员会		√			
交通系统	国土安全部、交通部	按运输模式或分行业细分		√			
食品和农业	农业部、卫生和公众服务部	√		√			
国防工业基地	国防部	√		√			
能源	能源部	√		√			
健康和公共卫生	卫生和公众服务部	√		√			
金融服务	财政部	适用独立的协调实体		√			
供水和废水系统	环境保护署	√		√			

注：√表示该基础设施行业设置了行业协调委员会或者政府协调委员会

3.4 Партнерское управление рисками

Управление рисками является одним из наиболее важных разделов NIPP. За четыре версии обновленная рамка уточнила три элемента критической инфраструктуры - физические объекты, киберпространство и людей - и определила пять шагов: постановка задач и целей; выявление критической инфраструктуры; оценка и анализ рисков; реализация мер управления рисками; измерение эффективности (рис. 5). Кроме того, рамка подчеркивает важность обмена информацией на протяжении всего процесса управления рисками. Обмен информацией проходит через каждый шаг, способствует обратной связи и обеспечивает непрерывное совершенствование безопасности и устойчивости критической инфраструктуры.

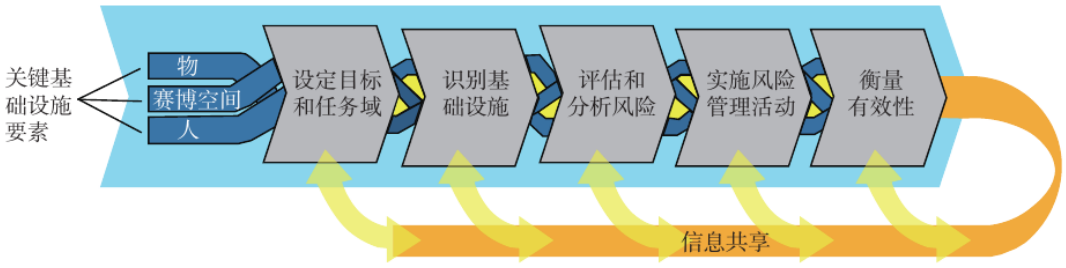

Рис.5 Американская рамка управления рисками критической инфраструктуры[12]

План определяет 31 ключевую способность, поддерживающую пять уровней задач защитного реагирования (табл. 2). Развитие многих из этих способностей способствует достижению безопасности и устойчивости критической инфраструктуры; сообщества, а также собственники и операторы могут применять их в выявленных мероприятиях по управлению рисками. Учет рисков критической инфраструктуры при постановке целевых показателей способностей усиливает меры по реализации этих целей.

Табл.2 Защитное реагирование 5-го уровня: 31 ключевая способность США[44]

预防	防护	减轻	响应	恢复
规划				
公共信息及警告				
运作协调				
取证和归因	访问控制和验证	社会韧性	关键运输	经济复苏
情报和信息共享	网络安全	长期脆弱性减少	环境响应/健康与安全	卫生和社会服务
阻断和中断	情报和信息共享	风险和灾害韧性评估	死亡管理服务	住房供给
筛查和检查	阻断和中断	威胁和危害识别	基础设施系统	自然和文化资源
	物理防护措施		大众护理服务	基础设施系统
	防护计划和活动的风险管理		大规模搜救行动	
	筛查和检查		现场安全和保护	
	供应链完整性和安全性		业务通信	
			公共卫生、医疗保健和紧急医疗服务	
			公共和私人服务与资源情况评估	

3.5 Действия по реализации плана

Реализация NIPP включает 12 действий, сгруппированных в три категории. Они направлены на повышение безопасности и устойчивости национальной критической инфраструктуры и призывают заинтересованные стороны критической инфраструктуры к скоординированному выполнению.

Во-первых, подчеркиваются усилия на основе партнерства: совместное определение приоритетов; выявление коллективных действий через совместное планирование; наделение местных и региональных партнерств полномочиями для формирования национальных способностей; использование стимулов для повышения безопасности и устойчивости.

Во-вторых, план призывает к инновационному управлению рисками: укреплять ситуационную осведомленность для принятия решений на основе рисков; глубоко анализировать зависимости, взаимозависимости и связанные каскадные эффекты между инфраструктурами; выявлять, оценивать и реагировать на каскадные эффекты инфраструктуры во время и после непредвиденных событий; содействовать восстановлению инфраструктуры, сообществ и регионов после инцидента; координировать разработку и реализацию технической помощи, обучения и образования. Продвижение научно-исследовательских решений должно дополнительно повышать безопасность и устойчивость критической инфраструктуры.

В-третьих, особое внимание уделяется результатам реализации: оценке прогресса в достижении целей, а также обучению и адаптации посредством тренировок и реальных событий.

4 Выводы для планирования защиты критической инфраструктуры в Китае

4.1 Организационная инновация: институционализировать исследования планирования и уточнить рабочие механизмы

Как указано выше, государство и некоторые провинции и муниципалитеты предусматривают, что органы гражданской обороны (развития и реформ) и отраслевые ведомства должны составлять общий план защиты и строительства важных экономических объектов и критической инфраструктуры. Однако по сравнению с другими специальными планами территориального пространства такие планы реализуются редко, поскольку защита критической инфраструктуры охватывает чрезвычайно широкую сферу и затрагивает очень сложные механизмы[30]. Опыт США показывает, что даже при четком лидерстве Министерства внутренней безопасности подготовка национального плана требует участия более десяти соответствующих ведомств - транспорта, энергетики, сельского хозяйства, торговли, охраны окружающей среды, финансов и др. - а также отраслевых советов, советов правительственной координации, региональных альянсов и иных организационных устройств и рабочих механизмов, обеспечивающих организацию и функционирование защиты критической инфраструктуры.

В исследованиях и планировании защиты критической инфраструктуры Китай должен использовать американский опыт с учетом собственных национальных условий. Рекомендуется, чтобы органы, отвечающие за гражданскую оборону (или развитие и реформы), возглавили процесс совместно с транспортными, энергетическими, промышленно-информационными, финансовыми и другими соответствующими ведомствами, координируя межотраслевые ресурсы и обеспечивая институционализацию, стандартизацию, интеграцию и преемственность политики. Следует также создать «правительственный координационный совет по критической инфраструктуре» и «отраслевые координационные советы». План должен уточнять механизмы и функции единого организационного руководства, бюджетного распределения, проектирования, надзора и проверки, а также реализации политики, чтобы эффективно совместно использовать защитные ресурсы различных отраслей. Необходимо дополнительно разграничить ответственность: органы гражданской обороны и отраслевые ведомства «руководят, осуществляют надзор и координируют защиту критической инфраструктуры», тогда как ответственные организации инфраструктуры «разрабатывают планы, программы и графики защиты»[45-46].

4.2 Приоритет планирования: запустить и непрерывно совершенствовать планы защиты критической инфраструктуры

Защита критической инфраструктуры относится к территориальной национальной обороне и является важной частью строительства национальной обороны. Поэтому она необходима для планирования территориального пространства и городского планирования. В Китае уже существуют ясные требования к защите городской инфраструктуры, сооружений гражданской обороны и согласованному развитию подземного пространства[47-48]. В некоторых общих планах территориального пространства и специальных планах гражданской обороны содержатся положения о защите «важных объектов», но они остаются разрозненными. С опорой на международный опыт Китай должен придерживаться принципа «планирование как основа», исходить из стратегической перспективы и как можно скорее запустить планирование защиты критической инфраструктуры с участием государства, провинций, муниципалитетов, отраслей,

межведомственных органов, сообществ и предприятий. План должен интегрировать ресурсы, задавать цели, проектировать мероприятия, определять приоритеты, распределять ответственность и постепенно повышать способность критической инфраструктуры реагировать на неопределенные риски.

Критическая инфраструктура многочисленна, охватывает множество отраслей и чрезвычайно сложна в управлении[18]. Все страны продолжают исследовать эту сферу; зрелой рамки или версии, которую можно было бы напрямую воспроизвести, не существует. Американский NIPP всего за семь лет прошел четыре версии и остается предметом непрерывной корректировки. Китай также не может завершить эту работу одним шагом. Следует сначала запустить планирование и решить вопрос самого существования таких планов, а затем непрерывно улучшать и обновлять их при сохранении преемственности политики.

При разработке и реализации планов защита конкретных категорий или отдельных объектов должна соблюдать принцип дифференцированной защиты. Ответственные субъекты критической инфраструктуры, правительства и отраслевые органы управления должны четко определить свои обязанности и обязательства. Правительства и отраслевые ведомства должны организовывать образование и обучение, формировать резервы технических экспертов и разрабатывать защитные нормы и стандарты. Ответственные субъекты инфраструктуры должны готовить и выполнять собственные планы защиты, проводить необходимые учения, а также создавать механизмы восстановления и системы резервирования критически важных функций.

4.3 Первый шаг: уточнить классификацию, ранжирование и соответствующие стандарты

Классификация и ранжирование, относящиеся к уточнению понятий, являются первым шагом в планировании защиты критической инфраструктуры. С начала XXI в. США расширили сферу защиты: от инфраструктуры, поддерживающей войну и экономическое функционирование, к системам общественного спасения и здравоохранения, связанным с общественным здоровьем и безопасностью, объектам, влияющим на национальный моральный дух, и далее к инфраструктуре, относящейся к экологической среде. Четыре версии NIPP демонстрируют непрерывную оптимизацию категорий и названий инфраструктуры (табл. 3). В Китае пока отсутствуют национальные стандарты классификации и ранжирования. Провинциальные и муниципальные классификации по-прежнему в основном сосредоточены на национальной обороне и экономической безопасности и еще недостаточно учитывают инфраструктуру, связанную с общественным здоровьем и безопасностью, национальным моральным духом и экологической средой. Международный опыт показывает, что подходы к классификации и ранжированию должны продолжать развиваться, а разработку соответствующих стандартов следует поставить во главу подготовительной работы по плану.

Табл.3 Процесс оптимизации классификации критической инфраструктуры в США[9-12]

关键基础设施分类	NIPP版本		
	2006年版本	2009年版本	2013年版本
食品和农业	√	√	√
国防工业基地	√	√	√
能源	√	√	√
健康与公共卫生	√	√	√
国家纪念碑和标志	√	√	× 合并到“政府设施”
银行和金融	√	√	√ 更名为“金融服务”
饮用水和水处理系统	√	√ 更名为“供水”	√ 更名为“供水和污水处理服务”
化工	√	√	√
商业设施	√	√	√
大坝	√	√	√
应急服务	√	√	√
商业核反应堆、材料和废物	√	√ 更名为“核反应堆、材料和废物”	√
信息技术	√	√	√
电信	√	√ 更名为“通信”	√
邮政和船运	√	√	× 合并到“交通系统”
交通系统	√	√	√
政府设施	√	√	√
关键制造业	×	√	√

注：①√表示在该版本中存在，×表示不存在；②NIPP的2007/2008年版本作为补充更新，变化较小，表中对该版本未体现

Ранжирование является одной из ключевых трудностей планирования защиты критической инфраструктуры. Провинции и муниципалитеты обычно классифицируют объекты с учетом местных условий и собственной «важности» объекта. Например, металлургическое предприятие на юге Китая, если оценивать его по выпуску и местному значению, несомненно может казаться критически важным; однако его национальная значимость спорна, если учитывать заменяемость со стороны северных провинций с развитой металлургией. Критическая инфраструктура функционирует как система и отражает общую социальную эффективность. NIPP и связанные американские исследования подчеркивают, что распространенной и серьезной ошибкой является недостаточное понимание зависимостей между различными категориями объектов. Жизнеобеспечивающие функции - связь, энергетика, транспорт и вода - находятся в центре этих зависимостей и взаимозависимостей. Отказ одной функции может вызвать каскадные нарушения, тяжелые последствия и ущерб планам и возможностям готовности. В городской чрезвычайной ситуации, например, система водоснабжения зависит от стабильного

электроснабжения; ремонт электросети зависит от доступности дорог; она, в свою очередь, ограничена системами командования и связи, а также службами аварийного реагирования и ремонта. В Китае при ранжировании пока недостаточно учитываются зависимости. Поэтому срочно необходимо создать научные методы и стандарты классификации и ранжирования, основанные на критериях зависимостей.

Прогностичность является важнейшей характеристикой планирования, и соответствующие стандарты должны в полной мере учитывать влияние новых технологий и их применения. Технологические итерации будут постоянно вести к изменениям. В условиях информационной и интеллектуализированной войны города сталкиваются с формами действий, нацеленными на парализацию всей системы путем ударов по ключевым узлам; стабильное функционирование критической инфраструктуры поэтому становится еще важнее и стимулирует развитие новых технологий, моделей и систем защиты. Особого внимания заслуживают три группы технологий. Первая - традиционные технологии, представленные заглублением или переводом под землю, например подземное защитное проектирование центра управления воздушным движением аэропорта Осло[49] или подземный банк крови гражданской обороны, завершенный в Израиле в 2022 г.[50-51]. Вторая - информационные технологии защиты, такие как постановка помех, создание ложных целей, увод средств поражения и инициированная детонация. Уже в 1990-е гг. академик Цянь Циху предлагал противодействовать высокотехнологичному информационному оружию путем сочетания сопротивляемости подземных сооружений, информационной защиты и других мер[23]. Третья - технологии, специфичные для отдельных категорий: для систем пресной воды и топливоснабжения необходимо развивать способность к быстрой диагностике и ремонту утечек трубопроводов; для химических заводов и иных объектов, способных вызвать вторичный ущерб, защита должна учитывать эффекты домино. Прогресс в этих трех направлениях существенно повлияет на нормы и стандарты планирования.

5 Заключение

Китайская система разработки планов защиты городской критической инфраструктуры все еще находится на исследовательской стадии. Хотя некоторые провинции и муниципалитеты уже начали практику, система пока не зрелая. Американский NIPP дает полезные ориентиры. По сравнению с США Китай сталкивается с более суровой средой безопасности. Можно предложить три первоочередные задачи. ① Организационная инновация: органы гражданской обороны должны проявлять инициативу, взаимодействовать с транспортными, энергетическими, финансовыми и другими ведомствами и создавать правительственные и отраслевые координационные советы, чтобы уточнить функции и рабочие механизмы. ② Приоритет планирования: следует придерживаться принципа «планирование как основа», как можно быстрее запускать планы, решая вопрос их наличия, а затем непрерывно совершенствовать их при сохранении преемственности политики. ③ Первые шаги: в приоритетном порядке развивать классификацию, ранжирование и соответствующие стандарты. Особое внимание следует уделять традиционным технологиям, представленным подземным размещением, информационным технологиям, таким как помехи, ложные цели, увод и инициированная детонация, а также технологиям, специфичным для разных категорий, особенно зависимостям между инфраструктурами.

При этом международный опыт должен использоваться избирательно, поскольку национальные условия различаются. США и другие страны обладают преимуществом первопроходцев, тогда как Китай имеет преимущество позднего обучения. Зарубежный опыт может служить ориентиром, но Китай должен строить систему планирования защиты

критической инфраструктуры исходя из собственных институтов и условий. Американский NIPP подчеркивает стратегическое планирование и сочетает стратегическое проектирование с планами действий, тогда как в Китае стратегическое планирование занимает важное место вне системы законодательно закрепленного планирования[52-53]. Поэтому способы адаптации такого опыта к китайскому контексту требуют дальнейшего изучения. Из-за конфиденциальности темы и ограничений времени доступная информация ограничена; приведенный анализ является предварительным и призван стимулировать обсуждение. Формирование системы планирования защиты критической инфраструктуры, соответствующей условиям Китая, требует еще значительной работы.

Список литературы

[1] MA Enshan, KOU Qingao. Исследование зарубежной экономической защиты [M]. Пекин: National Defense University Press, 2001. (на кит. яз.)

[2] Комиссия по планированию строительства временной столицы. Проект десятилетнего плана строительства временной столицы [Z]. Чунцин: Chongqing Planning Exhibition Gallery; Chongqing Library, составлено в 1946 г., переиздано в 2005 г. (на кит. яз.)

[3] GUO Dongjun, ZHAO Xudong, FENG Bing, et al. Зарубежный прогресс в классификации и ранжировании важных экономических объектов и его выводы [J]. Protective Engineering, 2016, 38(4): 69-78. (на кит. яз.)

[4] Saisi Think Tank. Анализ размещения, ударов и повреждений объектов в российско-украинском конфликте [R]. Hebei: Hebei Yipu Saisi Information Technology Co., Ltd., 2023. (на кит. яз.)

[5] RAN Jing, JIANG Xiaohui, HE Lei, et al. Типы, пространственные системы и приоритеты планирования и строительства городской общественной инфраструктуры двойного назначения для обычных и чрезвычайных ситуаций [J]. Urban Planning Forum, 2024(5): 98-105. (на кит. яз.)

[6] HE Lei, DAI Shenzhi, SONG Yan. Американский опыт разработки и оценки комплексных городских планов предупреждения бедствий и его значение для Китая [J]. Urban Planning Forum, 2011(5): 87-94. (на кит. яз.)

[7] LAMBETH B S, LEWIS K N. Economic targeting in modern warfare [R]. Santa Monica, California 90406: The Rand Corporation, 1982.

[8] Administration of Clinton W J. The Clinton administration’s policy on critical infrastructure protection: presidential decision directive No. 63 [R]. Washington, D.C.: The White House, 1998.

[9] The Department of Homeland Security. National infrastructure protection plan [R]. Washington, D.C.: The Department of Homeland Security, 2006.

[10] The Department of Homeland Security. National infrastructure protection plan - 2007/2008 update [R]. Washington, D.C.: The Department of Homeland Security, 2008.

[11] The Department of Homeland Security. National infrastructure protection plan - partnering to enhance protection and resiliency [R]. Washington, D.C.: The Department of Homeland Security, 2009.

[12] The Department of Homeland Security. National infrastructure protection plan - partnering for critical infrastructure security and resilience [R]. Washington, D.C.: The Department of Homeland Security, 2013.

[13] Закон Китайской Народной Республики о гражданской противовоздушной обороне [S]. 1996-10-29. (на кит. яз.)

[14] Закон Китайской Народной Республики о национальной обороне [S]. 1997-03-14. (на кит. яз.)

[15] Закон Китайской Народной Республики о мобилизации национальной обороны [S]. 2010-02-26. (на кит. яз.)

[16] Положение о безопасности и защите критической информационной инфраструктуры [S]. 2021-08-17. (на кит. яз.)

[17] Положение Автономного района Внутренняя Монголия о защите и управлении важными экономическими объектами [S]. Inner Mongolia Daily (китайская версия), 2022-09-07(006). (на кит. яз.)

[18] DAI Shenzhi, LIU Tingting, GAO Xiaoyu, et al. Стратегии планирования критической муниципальной инфраструктуры в китайских мегаполисах переходного периода: на примере Тайюаня [J]. Urban Planning Forum, 2019(S1): 212-219. (на кит. яз.)

[19] DAI Shenzhi, LIU Tingting. Стратегии трансформации планирования муниципальной инфраструктуры в новом раунде генеральных планов мегаполисов [J]. Urban Planning Forum, 2018(1): 58-65. (на кит. яз.)

[20] XIE Lei, ZHOU Yangjun. Исследование руководящих принципов комплексного планирования муниципальной инфраструктуры на основе анализа защитных расстояний [J]. Urban Planning Forum, 2012(S1): 245-250. (на кит. яз.)

[21] ЦК КПК. Рекомендации по разработке четырнадцатого пятилетнего плана социально-экономического развития страны и долгосрочных целей до 2035 г. [EB/OL]. [2020-10-29]. https://www.gov.cn/zhengce/2020-11/03/content_5556991.htm. (на кит. яз.)

[22] Политбюро ЦК КПК. Заседание по рассмотрению Стратегии национальной безопасности (2021-2025) [EB/OL]. [2021-11-18]. https://www.gov.cn/xinwen/2021-11/18/content_5651753.htm. (на кит. яз.)

[23] ZHU Daming, LI Xiaojun, WANG Zhenyu, et al. «Интегрированная защита» и «защита операционных систем» [J]. Protective Engineering, 2013, 35(3): 5-9. (на кит. яз.)

[24] Defense Production Act [S]. 1950-09-08.

[25] BOVEN T L. The DOD key asset protection program [R]. U.S. Army War College, Carlisle Barracks, PA 17013-5050: FEMA, 1989.

[26] Закон Китайской Народной Республики об охране военных объектов [S]. 1990-10-28. (на кит. яз.)

[27] GUO Yanpeng, QIN Youquan, ZHENG Ying, et al. Защита важных экономических объектов в информационной войне [J]. Science & Technology Review, 2020, 38(20): 106-112. (на кит. яз.)

[28] QIAN Qihu. Собрание статей академика Qian Qihu [M]. Пекин: Science Press, 2007. (на кит. яз.)

[29] ZHANG Shangwu, PAN Xin. Стратегические размышления о планировании и строительстве крупных межрегиональных инфраструктур в новый период [J]. Urban Planning Forum, 2021(2): 38-44. (на кит. яз.)

[30] DAI Shenzhi, LIU Tingting, GAO Xiaoyu, et al. Система планирования и механизм реализации предупреждения и снижения ущерба от бедствий в территориальном пространстве [J]. Urban Planning Forum, 2023(1): 48-53. (на кит. яз.)

[31] XIA Yu, REN Weiyang. Технические стандарты планирования интеллектуальной инфраструктуры Новой зоны Сюнъань [J]. Urban Planning Forum, 2022(5): 107-111. (на кит. яз.)

[32] Administration of Bush G W. Homeland security presidential directive/HSPD-7 - critical infrastructure identification, prioritization, and protection [R]. Washington, D.C.: The White House, 2003.

[33] Administration of Clinton W J. Executive Order 13010 - critical infrastructure protection [R]. Washington, D.C.: Federal Register, 1996.

[34] Administration of Obama B H. Presidential Policy Directive/PPD-21 - critical infrastructure security and resilience [R]. Washington, D.C.: The White House, 2013.

[35] Administration of Bush G W. Executive Order 13231 - critical infrastructure protection in the information age [R]. Washington, D.C.: Federal Register, 2001.

[36] The Department of Homeland Security. The report for the Department of Homeland Security [R]. Washington, D.C.: The Department of Homeland Security, 2002.

[37] OBAMA B H. Executive Order 13636 - improving critical infrastructure cybersecurity [R]. Washington, D.C.: Federal Register, 2013.

[38] TRUMP D J. Executive Order 13800 - strengthening the cybersecurity of federal networks and critical infrastructure [R]. Washington, D.C.: Federal Register, 2017.

[39] Cybersecurity and Infrastructure Security Agency Cyber Exercise Act [R]. 2021-01-01.

[40] Executive Office of the President of the United States. National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems [R]. Washington, D.C.: The White House, 2021.

[41] Cybersecurity and Infrastructure Security Agency. Infrastructure Resilience Planning Framework Version 1.0 [R]. Washington, D.C.: U.S. Government Publishing Office, 2021.

[42] Cybersecurity and Infrastructure Security Agency. Infrastructure Resilience Planning Framework Version 1.1 [R]. Washington, D.C.: U.S. Government Publishing Office, 2023.

[43] Cybersecurity and Infrastructure Security Agency. Infrastructure Resilience Planning Framework Version 1.2 [R]. Washington, D.C.: U.S. Government Publishing Office, 2024.

[44] Department of Homeland Security. National Preparedness Goal [R]. Washington, D.C.: Department of Homeland Security, 2011.

[45] Уведомление Управления гражданской противовоздушной обороны провинции Шаньдун об усилении защиты и управления важными экономическими объектами [J]. Gazette of the People’s Government of Shandong Province, 2021(3): 41-43. (на кит. яз.)

[46] Положение муниципалитета Пекина о гражданской противовоздушной обороне [S]. 2002-03-29. (на кит. яз.)

[47] YAO Wenqi. Методы планирования подземного пространства в городских центрах: на примере центрального района Баоань в Шэньчжэне [J]. Urban Planning Forum, 2010(S1): 36-43. (на кит. яз.)

[48] TANG Yuqing, ZHOU Bingyu. Планировочный контроль подземного пространства в центральных районах крупных китайских городов: на примере центрального делового района Хуандао в Циндао [J]. Urban Planning Forum, 2006(5): 89-94. (на кит. яз.)

[49] LITTLE R G, PATTAK P B, SCHROEDER W A. Use of underground facilities to protect critical infrastructures: summary of a workshop [R/OL]. Washington, D.C.: National Academy of Sciences, 1998. http://www.nap.edu/catalog/6285.html.

[50] JEFFAY N. Israel opens world's most protected blood bank, rocket-proof and underground [EB/OL]. [2022-05-02]. https://www.timesofisrael.com/israel-opens-worlds-most-protected-blood-bank-rocket-proof-and-underground/.

[51] NEHAMA-ABADI R, ADOM M D. A vision of dedication, determination to save lives [EB/OL]. [2022-09-25]. https://www.jpost.com/special-content/magen-david-adom-a-vision-of-dedication-determination-to-save-lives-718089.

[52] ZHENG Guo. Изменения поведения местных органов власти и эволюция городского стратегического планирования [J]. City Planning Review, 2017, 41(4): 16-21. (на кит. яз.)

[53] XU Ze, ZHANG Yunfeng, XU Ying. Десятилетний обзор и перспективы стратегического планирования: на примере стратегии городского развития Ningbo 2030 [J]. City Planning Review, 2012, 36(8): 73-79. (на кит. яз.)

Доработано: декабрь 2024 г.
(Настоящая статья переведена при содействии ИИ.)