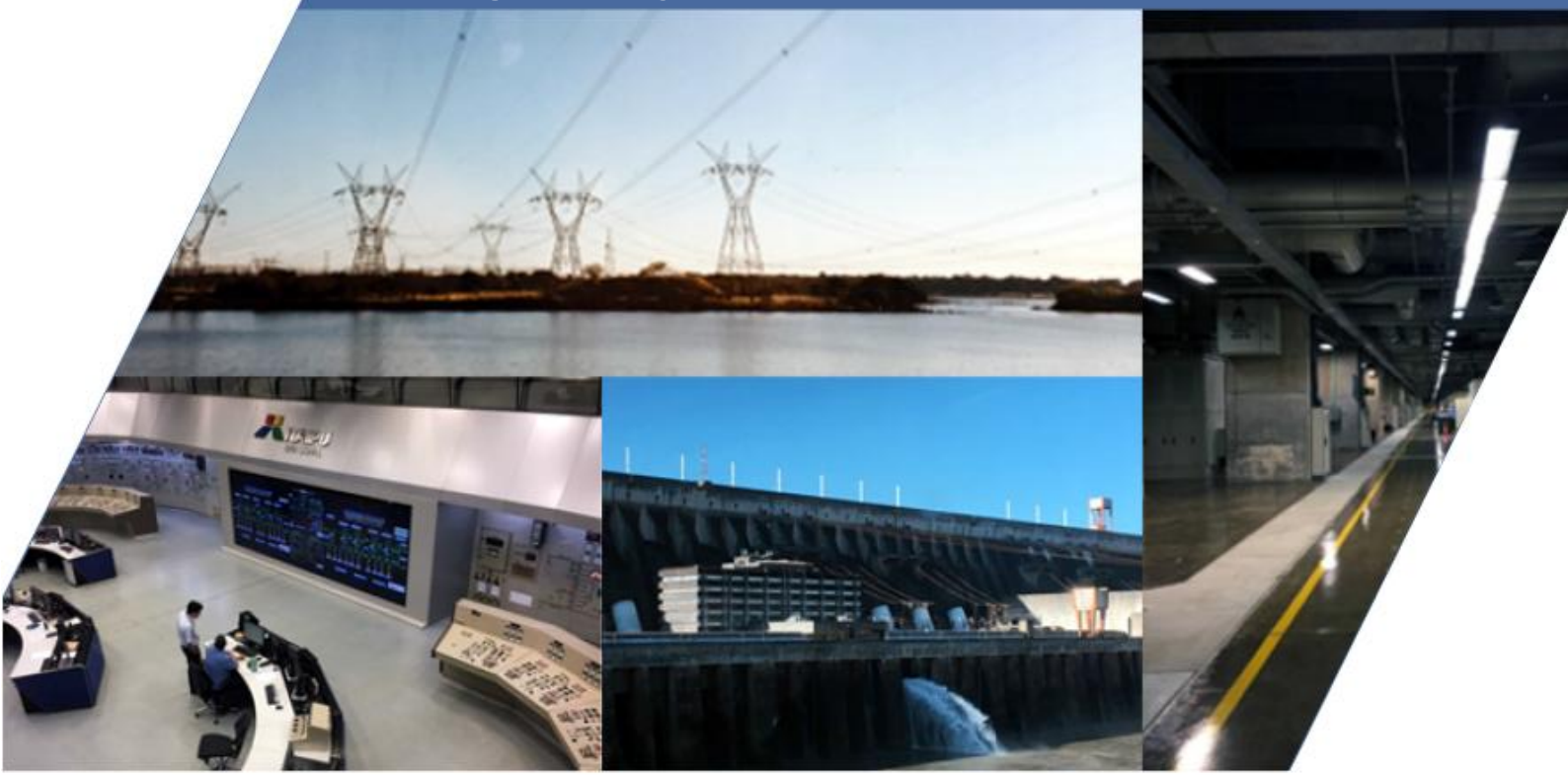
Контртеррористическое управление Организации Объединенных Наций (КТУ ООН)

Исполнительный директорат Контртеррористического комитета Совета Безопасности ООН (ИДКТК)

INTERPOL
/ИНТЕРПОЛ/

Защита критически важных объектов инфраструктуры от террористических атак: Сборник передового опыта



Составлен ИДКТК и КТУ ООН в 2018

ЗАЩИТА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФРАСТРУКТУР ОТ ТЕРРОРИСТИЧЕСКИХ АТАК:

СБОРНИК ПЕРЕДОВОГО ОПЫТА

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

17 февраля 2017 года Совет Безопасности Организации Объединенных Наций единогласно принял резолюцию 2341 о защите критически важных объектов инфраструктуры и расширении возможностей государств по предотвращению нападений на критически важные объекты инфраструктуры и призвал государств-членов противостоять опасности террористических атак на критически важные объекты инфраструктуры. Резолюция предлагает государствам-членам рассмотреть возможные превентивные меры при разработке национальных стратегий и политики.

В глобальной контртеррористической стратегии ООН, в рамках Раздела II «Меры по борьбе с терроризмом и его предотвращению», государства-члены решили «активизировать все усилия по повышению безопасности и защиты особо уязвимых объектов, таких как инфраструктура и общественные места, а также реагирование на террористические нападения и другие бедствия, в частности в области гражданской обороны, при этом признавая, что государствам может потребоваться помощь для этой цели.

Резолюция 1373 (2001) Совета Безопасности уже призвала государства-члены «принять необходимые меры для противодействия совершению террористических актов, в том числе путем раннего оповещения других государств посредством обмена информацией». В резолюции 1566 (2004) Совета Безопасности также содержится призыв к государствам предотвращать преступные действия, в том числе в отношении гражданских лиц, которые совершаются с целью спровоцировать состояние террора среди населения или группы лиц, запугать население или принудить правительство, или международную организацию совершить или воздержаться от каких-либо действий. Физическая защита критически важных объектов инфраструктуры может предотвратить совершение серьезных террористических атак. Более того, немедленное реагирование на террористическую атаку на критически важный объект инфраструктуры может предотвратить «каскадные» эффекты, которые зачастую связанны с такими атаками.

Резолюция 2341 (2017) Совета Безопасности поручает Контртеррористическому Комитету (КТК) при поддержке Исполнительного Директората Контртеррористического Комитета (ИДКТК) "изучить усилия государств-членов по защите критически важных объектов инфраструктуры от террористических нападений, имеющие отношение к осуществлению резолюции 1373 (2001), с целью выявления передового опыта, пробелов и уязвимостей в этой области". Данный мандат ИДКТК способствует проведению оценки и разработке анализа, в том числе тенденций в борьбе с терроризмом, который будет распространен в контексте этого важного проекта[1].

Резолюция 1373 также обязывает Целевую группу по осуществлению контртеррористических мероприятий (ЦГОКМ) в рамках Контртеррористического Управления (КТУ), Рабочую группу ЦГОКМ по защите критически важных объектов инфраструктуры, включая уязвимые цели, Интернет и безопасность туризма, и КТК (при поддержке ИДКТК) продолжать совместную работу по содействию в оказании технической помощи и в наращивании потенциала, а также повышению осведомленности в области защиты критически важных объектов инфраструктуры (ЗКВОИ) от террористических атак, в частности посредством: укрепления диалога с государствами, международными и региональными организациями (МРО) и работы с провайдерами технической помощи, в том числе посредством обмена информацией.

В Глобальной контртеррористической стратегии ООН, в рамках Направления II «Меры по борьбе с терроризмом и его предотвращению», государства-члены также решили «работать с Организацией Объединенных Наций с должным учетом конфиденциальности, уважения прав человека и соблюдения других обязательств по международному праву, исследовать пути и средства с целью координации усилий на международном и региональном уровнях по борьбе с терроризмом во всех его формах и

[1] КТК провел два открытых брифинга по этим вопросам: (i) открытый брифинг на тему «Защита критически важной инфраструктуры в туризме», состоявшийся 12 июня 2014 года, и (ii) открытый брифинг на тему «Укрепление реагирования на чрезвычайные ситуации после террористических инцидентов» состоялась 16 июня 2015 года. 21 ноября 2016 года Совет Безопасности провел заседание «Arria Formula» по «Защите критически важной инфраструктуры от террористических атак», на котором государства-члены представили свою озабоченность и мнения по ключевым аспектам этой темы.

проявлениях в Интернете; использовать Интернет как инструмент противодействия распространению терроризма, с учетом, что государствам может потребоваться помощь в этом отношении».

Под председательством Интерпола и КТУ ООН, Рабочая группа ЦГОКМ по «Защите критически важных объектов инфраструктуры, включая уязвимые цели, Интернет и безопасность туризма», приняла решение разработать Сборник передового опыта по защите критически важных объектов инфраструктуры от террористических атак. Сборник был разработан в рамках «Единого подхода ООН». Это способствует повышению осведомленности о требованиях резолюции 2341 (2017). В сборнике содержатся рекомендации для государств-членов и МРО, а также обобщен передовой опыт защиты критически важных объектов инфраструктуры от террористических атак (с показателями, установленными требованиями, мерами по оценке рисков, рекомендациями и т. д.). Он также предоставляет государствам-членам справочные материалы по разработке стратегий снижения рисков террористических атак на критически важные объекты инфраструктуры. Принимая во внимание различия в концептуальных и правовых рамках, применимых к «легким целям» и критически важным объектам инфраструктуры, в сборнике подчеркивается возможный элемент синергизма, учитывая, что очень часто одни и те же государственные учреждения имеют институциональные и оперативные обязанности в обеих областях. Кроме того, он дает государствам-членам, а также международным и региональным организациям, четкие указания о том, как разрабатывать и укреплять такие стратегии. Ссылки и показатели касаются предотвращения, готовности, смягчения последствий, расследования, реагирования, восстановления и других соответствующих концепций по ЗКВОИ.

В дополнение к требованиям резолюции 2341 (2017) Совета Безопасности, реализация различных элементов, включенных в сборник, осуществляется в контексте резолюции Генеральной Ассамблеи по Пятому обзору Глобальной контртеррористической стратегии Организации Объединенных Наций (A / RES / 70/291), которая "призывает все государства-члены сотрудничать с Контртеррористическим центром Организации Объединенных Наций и вносить вклад в осуществление его деятельности в рамках Целевой группы по осуществлению контртеррористических мероприятий, в том числе посредством разработки, финансирования и осуществления проектов по наращиванию потенциала в целях мобилизации более решительных и систематических мер по борьбе с терроризмом на национальном, региональном и глобальном уровнях".

Проект стал возможным благодаря щедрому гранту Контртеррористического центра ООН.

Владимир Воронков
Заместитель Генерального секретаря
Контртеррористического Управления ООН
Исполнительный Директор
Контртеррористического центра Организации Объединенных Наций

Мишель Конинкс
Помощник Генерального секретаря
Исполнительный директор Исполнительного директората Контртеррористического Комитета

ЗАЩИТА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ ОТ ТЕРРОРИСТИЧЕСКИХ АТАК - ТОЧКА ЗРЕНИЯ ИНТЕРПОЛА

Вступительное слово от Интерпола - председателя Рабочей группы ЦГОКМ по «Защите критически важных объектов инфраструктуры, включая уязвимые цели, Интернет и безопасность туризма»

Критически важные объекты инфраструктуры действуют в качестве системы жизнеобеспечения нашего повседневного существования. Наши сообщества поддерживаются очень комплексной и сложной сетью инфраструктурных систем. Наши граждане ожидают и полагаются на функционирующие учреждения и службы в отношении своего здоровья, безопасности, охраны и экономического благополучия.

Эта система жизнеобеспечения стала более эффективной и продуктивной благодаря технологическому прогрессу, взаимосвязям глобализации и потребностям постоянно растущего городского населения. Наступление *life 3.0* (*жизни 3.0)* - замещение физического мира цифровым - позволило нам следить и даже контролировать инфраструктуру из любой точки мира.

Тем не менее, вместе с сильной зависимостью и возможностью подключения в реальном времени появляются факторы уязвимости к угрозам. Взаимозависимость нашей инфраструктуры на уровне секторов и отраслей, между кибер и физическими областями, а также национальным границам означает, что атаки могут иметь далеко идущие последствия.

Одна атака на единственную точку сбоя может привести к нарушению или разрушению нескольких жизненно важных систем непосредственно в самой стране и, по цепной реакции, во всем мире. Это создает привлекательную цель для тех, кто намеревается навредить нам. И в то время как наши города и инфраструктура развиваются, то же самое происходит и с их оружием.

Тактика зоны конфликта, например, одновременные активные перестрелки; автомобильные самодельные взрывные устройства (автомобильные СВУ); самодельные взрывные жилеты; хакерские атаки; или портативные беспилотные воздушные системы с взрывчатым грузом могут шлифоваться с целью использования на улицах нашего города и против ключевых объектов.

Итак, как мы можем защитить жизненно важные органы нашей системы жизнеобеспечения от этой постоянно адаптирующейся угрозы?

Короткий ответ: путем предоставления всем соответствующим субъектам возможности подготовиться предотвратить; и реагировать на такие атаки.

Эти императивы лежат в основе усилий Интерпола по содействию обмену разведывательными данными, наращиванию потенциала и повышению устойчивости в некоторых важных областях.

Во-первых, мы сосредоточены на усилении безопасности критически важных объектов с помощью стандартов и процедур обеспечения готовности к чрезвычайным ситуациям.

Например, команда Интерпола по уязвимым целям работает с нашими странами-членами в Западной Африке с целью повышения физической безопасности лабораторий, в которых размещаются опасные патогенные микроорганизмы, и их защиты от террористических атак. Этот проект, щедро финансируемый правительством Канады, направлен на создание планов действий по обеспечению биобезопасности посредством совместных межучережденческих действий.

Во-вторых, мы продолжаем призывать страны защищать свои границы и противодействовать террористической мобильности.

В период с января 2017 года по апрель 2018 года Интерпол отметил более чем 200-процентное увеличение числа профилей иностранных боевиков-террористов, доступных в режиме реального

времени через свою систему криминальной информации, и 750-процентное увеличение обмена информацией между странами-членами посредством их каналов.

Это просто беспрецедентный случай в столь деликатном деле - призыв Совета Безопасности создал переломный момент.

В-третьих, важно сохранять бдительность и наращивать усилия по пресечению материалов и инструментов прежде, чем они станут следующим оружием.

В этом контексте Интерпол тесно сотрудничает с МАГАТЭ в деле борьбы с незаконным оборотом радиологических и ядерных материалов, проводя обучение по вопросам мониторинга и обнаружения, а также трансграничных операций.

И, наконец, самое главное, Интерпол поощряет межучережденческое и международное сотрудничество как фактор усиления. Обмен информацией, обнаружение угроз, требующих безотлагательных действий, и передовой опыт по выявлению факторов уязвимости, методологий и извлеченных уроков имеют решающее значение.

В правоохранительных органах мы в полной мере осознаем трагический парадокс: террористический акт часто является одной из лучших возможностей для обучения и совершенствования. Совместное использование этих уроков означает взять на вооружение преимущества, не неся при этом потерь. Это беспроигрышный сценарий.

Вместе мы можем создать глобальный инструментарий безопасности инфраструктуры и механизмы реагирования на инциденты, основываясь на реальном опыте работы. Параллельно мы можем проверить себя с вероятными сценариями, с которыми нам, возможно, придется столкнуться в будущем.

С этой целью Интерпол организует мероприятия для экспертов от всех заинтересованных сторон. Наши задачи в области цифровой безопасности вместе со специалистами частного сектора являются примером того, как мы работаем со странами-членами и донорами над подготовкой, предотвращением и реагированием на физические, цифровые или и те и другие угрозы.

Во взаимосвязанном мире нам не удастся защитить национальную инфраструктуру по отдельности. Вот почему глобальные инициативы, поддерживаемые Организацией Объединенных Наций и Интерполом, и шаги, которые в результате будут предприняты международным сообществом, имеют важное значение.

СПИСОК СОКРАЩЕНИЙ

ХБРЯ	Химическое, биологическое, радиологическое и ядерное оружие
КВОИ	Критически важные объекты инфраструктуры
КИИ	Критически важная информационная инфраструктура
ЗКВОИ	Защита критически важных объектов инфраструктуры
CIPRNet	Сеть исследования готовности и устойчивости критически важных объектов инфраструктуры
МНБ	Министерство национальной безопасности
ЕОБ	Европейская организация по безопасности
ИКАО	Международная организация гражданской авиации
СПК	Система промышленного контроля
ИКТ	Информационные и коммуникационные технологии
ММО	Международная Морская Организация
Кодекс ISPS	Международный кодекс безопасности судов и портовых средств
МСЭ	Международный союз электросвязи
DoS атака	Атака типа "отказ в обслуживании"
ИВУ	Импровизированное взрывное устройство
ИГИЛ	Исламское Государство Ирака и Леванта
ISO	Международная организация по стандартизации
ПЗРК	Переносной зенитный ракетный комплекс
ЦЗНИ	Центр по защите национальной инфраструктуры
ОЗХО	Организация по запрещению химического оружия
ОБСЕ	Организация по безопасности и сотрудничеству в Европе
ГЧП	Государственно-частное партнерство
ЮНИКРИ	Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия
МСУОБ	Бюро по сокращению риска бедствий ООН
КТУ ООН	Контртеррористическое управление ООН

Указатель таблиц

УКАЗАТЕЛЬ ПО ИЗУЧЕНИЮ КОНКРЕТНЫХ СИТУАЦИЙ

СОДЕРЖАНИЕ, ЗАДАЧИ И МЕТОДОЛОГИЯ

В этом сборнике рассматривается тема, которая все еще в значительной степени находится в стадии становления. Темпы, с которыми современные экономики стали неразрывно взаимосвязанными за последние два десятилетия, особенно благодаря огромным шагам, достигнутым в сфере информационных и коммуникационных технологий, подвергли наше общество целому ряду беспрецедентных угроз и факторов уязвимости. Многие из них происходят от террористических групп, которые стремятся дестабилизировать сообщества и создают широкомасштабную панику, вмешиваясь в те самые активы и процессы, от которых зависит выживание нашего общества. Эти активы и процессы являются центральными узлами, известными как «критически важные объекты инфраструктуры» (КВОИ).

Однако, растущее осознание того, что мы сейчас сталкиваемся с новым типом безопасности окружающей среды, не подходит соответствующим уровням готовности. Тем не менее, недавние атаки Аль-Каиды и ИГИЛ на транспортные системы, неоднократные диверсии против плотин, нефтепроводов, мостов и т. д. являются свежими напоминаниями о постоянной заинтересованности террористических групп в подрыве КВОИ.

Именно в этом контексте резолюция 2341 (2017) Совета Безопасности была принята как первый в мире глобальный нормативный документ, целиком посвященный защите КВОИ от террористических нападений. Ее положения отражают вновь выраженную готовность международного сообщества разработать и модернизировать механизмы, необходимые для минимизации рисков для КВОИ, вызванных террористическими атаками, а также для адекватного реагирования и восстановления после таких атак.

Этот сборник создан в качестве инструмента для поддержки широкого круга участников (от политиков до правоохранительных органов и заинтересованных сторон из частного сектора), которые несут ответственность за разработку, совершенствование или реализацию политики и мер по защите КВОИ от террористических атак в соответствии с резолюцией.

Он состоит из тематических блоков, которые в целом соответствуют структуре резолюции. Каждая глава представлена одним или несколькими пунктами постановляющей части и сопутствующим анализом рассматриваемого предмета. Особое внимание было уделено тому, чтобы не учитывать предыдущие знания концепций по КВОИ со стороны читателя. Этот подход основан на признании того, что «Защита критически важных объектов инфраструктуры» является относительно новым приобретением в глобальном публичном политическом дискурсе.

Основные практические и правовые проблемы, с которыми сталкиваются государства, рассматриваются с точки зрения нынешних и потенциальных решений, принимаемых конкретными правительствами и организациями. Прагматичный подход, которому следует сборник, иллюстрируется множеством ситуационных исследований, которые предоставляют конкретные примеры и варианты реализации. Добавлен ряд таблиц, позволяющих странам быстро сравнивать меры, принятые другими странами, и, в конечном итоге, помочь сформировать те, что лучше всего соответствуют их институциональному контексту в рамках, установленных резолюцией.

Несмотря на то, что в сборнике основное внимание уделяется защите КВОИ от террористических атак, в нем признается, что ряд стран решили принять широкие и комплексные стратегии, учитывающие необходимость повышения устойчивости КВОИ против всех опасностей, будь то техногенных или природных. Таким образом, в сборнике представлены концептуальные инструменты, которые позволят странам принять, если они того пожелают, всеобъемлющие стратегии, уделяя особое внимание террористической угрозе и соответствующим механизмам оценки и смягчения последствий.

В соответствии с резолюцией 2341 (2017) в сборнике рассматривается вопрос ЗКВОИ, при этом не уделяя особого внимания на какой-либо конкретный тип инфраструктуры. Поперечный подход направлен на то, чтобы выделить общие принципы, процессы и методологии, которые странам рекомендуется воплощать в конкретные стратегии, планы действий и меры, затрагивающие специфичные области. В то же время примеры конкретных мер по смягчению последствий

предлагаются по всему документу. Кроме того, в главе 9 представлен обзор основных инициатив, предпринятых ведущими международными организациями в отдельных секторах.

Наконец, предоставляя инструкции странам, сборник поддерживает принцип, согласно которому вопросам по правам человека должно быть уделено особое внимание и широкое внедрение во всех мерах защиты КВОИ и в соответствующих стратегиях.

1. ПОНИМАНИЕ ПРОБЛЕМЫ

Резолюция Совета Безопасности 2341 (2017)
Пункт 2 постановляющей части

Совет безопасности (...)

Призывает все государства прилагать согласованные и скоординированные усилия, в том числе посредством международного сотрудничества, повышения осведомленности, информированности и понимания угроз, исходящих от террористических нападений в целях повышения готовности отражать нападениям на критически важные объекты инфраструктуры.

1.1 Терроризм как особая угроза для критически важных объектов инфраструктуры (КВОИ)

В то время как КВОИ подвержены множеству типов опасностей, включая природные явления, человеческие ошибки, технические сбои и преступные действия в широком смысле, рождение защиты КВОИ как особой области политики было прямым следствием событий 11 сентября 2001 года.

За последние несколько десятилетий террористы, несомненно, проявили интерес к КВОИ как потенциальным целям для достижения своих задач. Уже в 2002 году отмечались явные признаки того, что Аль-Каеда стремилась использовать факторы уязвимости в государственных и частных коммунальных службах США. Обнаружение в Афганистане компьютера, содержащего программы структурного анализа плотин, побудило Национальный центр защиты инфраструктуры США выпустить Предупреждающий информационный бюллетень (NIPC 2002).

Важно отметить, что едва ли каждый сектор избежал последствий террористической деятельности или хотя бы не затронул внимание террористических групп. Примеров предостаточно. В транспортном секторе последние события включают в себя одновременные нападения в 2016 году на аэропорт и метро Брюсселя двумя группами боевиков ИГИЛ. В целом 32 человека погибли и около 300 получили ранения.

Энергетический сектор стал свидетелем устойчивой террористической деятельности в результате нападений, совершенных Аль-Каидой и ее филиалами на объекты и персонал нефтяных компаний в Алжире, Ираке, Кувейте, Пакистане, Саудовской Аравии и Йемене.

Ключевые водные инфраструктуры были объектом особого внимания со стороны ИГИЛ. В период с 2013 по 2015 год ИГИЛ совершило около 20 крупных нападений на сирийские и иракские объекты. В дополнение к разрушению трубопроводов, санитарно-технических сооружений и мостов, ИГИЛ стратегически использовало водную инфраструктуру, например, перекрыв плотины и отключив водоснабжение (Vishwanath 2015).

В некоторых случаях предпринимались попытки нападения на инфраструктуры, содержащие опасные материалы. 26 июня 2015 года смертник врезался на автомобиле в площадку химического завода под Лионом и в газовые баллоны, спровоцировав взрыв. В 2016 году две атомные электростанции в Бельгии были заблокированы по подозрению в попытке ИГИЛ атаковать, проникнуть или провести диверсию на объектах с целью получения ядерных / радиоактивных материалов.

Несмотря на то, что массовые атаки против КВОИ, охватывающие значительные каскадные эффекты / сбои, не были проведены, угроза, создаваемая этим типом сценария, все еще очень велика и призывает страны разработать адекватные планы по предотвращению и реагированию в чрезвычайных ситуациях. Действительно, террористические акты, совершенные до сих пор, выявили внутреннюю уязвимость ряда КВОИ. Кроме того, на горизонте вырисовывается вероятность того, что новые поколения террористов будут все более и более осведомлены об ИКТ. Хотя кибертеррористические атаки еще не осуществлены, повышение уровня «ноу-хау» в области ИКТ, скорее всего, повысит вероятность их возникновения. По мнению Группы правительственных экспертов по достижениям в области

информатизации и телекоммуникаций в контексте международной безопасности, «использование ИКТ в террористических целях, помимо вербовки, финансирования, обучения и подстрекательства, в том числе для террористических атак против ИКТ или ИКТ-зависимой инфраструктуры, увеличивает вероятность того, что, если это оставить без внимания, может возникнуть угроза всеобщему миру и безопасности» (ГПЭ 2015, стр.6).

1.2 КВОИ и «легкие мишени»

Понятие «легкие мишени» обычно ассоциируется с местами, где люди собираются в большом количестве, такими как музеи, кинотеатры, религиозные объекты, торговые центры и т. д. Легкие мишени противопоставляются так называемым «трудным целям», которые в широком смысле определяют места, где высокий уровень защиты обеспечивается зачастую вооруженными людьми и / или там, где доступ общественности ограничен или подвергается строгому контролю (например, военные объекты, посольства, аэропорты).

Как свидетельствуют недавние атаки в пешеходных зонах Ниццы и Барселоны, на рождественском базаре в Берлине и других местах, открытая среда и высокая степень доступности легких целей делают их особенно уязвимыми для террористических атак. В то же время легкие цели предоставляют террористам идеальную площадку для нанесения ударов с небольшими организационными усилиями и приводя к массовым жертвам.

В этом контексте в резолюции 2396 (2017) Совета Безопасности конкретно признается опасность того, что иностранные боевики-террористы, связанные с ИГИЛ, планируют и осуществляют нападения на легкие цели после возвращения из зон боевых действий.

Хотя между КВОИ и «легкими» целями существуют четко совпадающие характеристики, при этом отдельные страны несут ответственность за определение и разработку соответствующих стратегий защиты для обоих типов, эти две концепции нельзя использовать взаимозаменяемо. Ключевой элемент различия касается вопроса «критичности». Легкие цели не обязательно имеют решающее значение для предоставления основных социальных услуг. Более того, легкие цели могут включать инфраструктуру (как например, стадион), но не во всех случаях (например, когда люди собираются на площади в связи с концертом под открытым небом). Несмотря на концептуальные различия, в Разделе 2.3.1 рассматривается целесообразность для стран развивать синергизм между этими двумя понятиями как часть их общей политики защиты от террористических актов.

1.3 Конкретные террористические угрозы для КВОИ

Связанные с терроризмом угрозы в отношении КВОИ имеют много аспектов. В следующих разделах такие угрозы разбиты на части в зависимости от характера (физические и кибернетические), происхождения (внутренние и внешние) и контекста, в котором они происходят (отдельные или множественные цели). Понимание типов угроз, которым подвержены КВОИ, является первым шагом в процессе разработки адекватных стратегий защиты, как обсуждалось в Главе 2.

1.3.1 Физические угрозы в сравнении с киберугрозами

Физические угрозы, нацеленные на КВОИ, могут принимать различные формы. Их общая характеристика заключается в том, что они нацелены на разрушение инфраструктуры, ослабление или полное, или частичное выведение из строя путем вмешательства в ее физическую структуру, механические компоненты и т. д.

Наиболее интуитивные физические угрозы для КВОИ включают использование взрывчатых веществ или зажигательных устройств, транспортных средств, ракет, ПЗРК, гранат и даже простых инструментов (например, спичек или зажигалок для поджога) и т.д. для достижения полного или частичного коллапса, или разрушение инфраструктуры. Атаки могут также включать в себя преднамеренную модификацию или манипулирование системами и процессами КВОИ (например, включение и выключение средств, открытие и закрытие затворов в системах трубопроводов, подавление технологических сигналов, сигналов об ошибках или аварийных сигналов). Развертывание химического, биологического, радиологического или ядерного оружия, или веществ представляет собой еще один особый тип угрозы для КВОИ. Оно может варьироваться от распространения инфекционных болезнетворных микроорганизмов в сетях снабжения продовольствием, водопроводах и т. д. до использования ядовитого газа на основных транспортных развязках и перекрестках. Также уместно отметить, что нападение на критически важный объект, содержащий химические, биологические, радиологические или ядерные материалы, также может привести к выбросу таких материалов.

Хотя киберугрозы отличаются от физических угроз по своей природе, конечный результат может быть одинаковым. Киберугрозы различаются, но могут включать, например, атаки, которые:

- манипулируют системами или данными - такими как вредоносные программы, использующие уязвимости в программном и аппаратном компонентах компьютеров, необходимых для работы КВОИ;
- отключают критически важные системы, такие как атака типа "отказ в обслуживании"[2];
- ограничивают доступ к критически важным системам или информации - например, с помощью атак в целях вымогательства выкупа.

Как показано в Разделе 2.4.2, в то время как взаимосвязанные и интегрированные компьютеризированные системы управления значительно упростили методы работы КВОИ и повысили эффективность рынка, расширение возможностей сетевого взаимодействия также может увеличить площадь атаки и, следовательно, подвергнуть КВОИ высокому риску манипулирования.

Согласно результатам опроса частного сектора, в котором приняли участие 200 руководителей отраслей, работающих в КВОИ в секторе электроэнергетики в 14 странах, «[в 2010 году] почти половина респондентов указали, что они никогда не сталкивались с атаками, связанными с крупномасштабными отказами оборудования или проникновением в сеть. К [2011] эти цифры резко изменились: 80 процентов столкнулись с атаками, связанными с крупномасштабными отказами оборудования, а 85 процентов испытали проникновение в сеть» (McAfee 2011, стр.6).

Таблица 1: Топ 10 угроз для промышленных систем управления

№	Угроза	Объяснение
1	Несанкционированное использование точек доступа удаленного обслуживания	Точки доступа для технического обслуживания -это специально созданные внешние входы в сеть ИКТ, которые зачастую недостаточно защищены.
2	Сетевые атаки через офисные или корпоративные сети	Офисные ИТ обычно связаны с сетью несколькими способами. В большинстве случаев сетевые соединения из офисов в сеть ИКТ также существуют, поэтому злоумышленники могут получить доступ по этому маршруту
3	Атаки на стандартные компоненты, используемые в	Стандартные ИТ-компоненты (коммерческие готовые продукты (COTS)), такие как системное программное

[2] Недавним примером атаки типа "отказ в обслуживании", непосредственно затрагивающей КВОИ, было нападение на датскую систему бронирования железнодорожных билетов 14 мая 2018 года.

	сети ИКТ	обеспечение, серверы приложений или базы данных, часто содержат недостатки или уязвимости, которые могут быть использованы злоумышленниками. Если такие стандартные компоненты также используются в сети ИКТ, риск успешной атаки на сеть ИКТ возрастает.
4	Атаки типа "отказ в обслуживании"	(Распределенные) атаки типа "отказ в обслуживании" могут ослабить сетевые соединения и важнейшие ресурсы и привести к отказу систем, например, для нарушения работы ИКТ.
5	Человеческая ошибка и саботаж	Преднамеренные действия, совершаемые как внутренними, так и внешними злоумышленниками, представляют собой серьезную угрозу для всех целей защиты. Небрежность и человеческая ошибка также представляют собой большую угрозу, особенно в отношении конфиденциальности и доступности целей защиты.
6	Внедрение вредоносного ПО через съемные носители и внешнее оборудование	Использование съемных носителей и мобильных ИТ-компонентов внешнего персонала всегда влечет за собой большой риск заражения вредоносным ПО
7	Чтение и опубликование новостей в сети ИКТ	Большинство компонентов управления в настоящее время используют протоколы с открытым текстом, поэтому связь не защищена. Это позволяет относительно легко читать и вводить команды управления
8	Несанкционированный доступ к ресурсам	Внутренние злоумышленники и последующие атаки после первоначального внешнего проникновения делают это особенно простым, если службы и компоненты в сети процессов не используют методы аутентификации и авторизации или если эти методы небезопасны.
9	Атаки на сетевые компоненты	Злоумышленники могут манипулировать сетевыми компонентами, например, для проведения атак «злоумышленник в середине» или для облегчения прослушивания.
10	Технические неисправности или форс-мажорные обстоятельства **Источник:** ОБСЕ 2013, стр.34	Перебои, вызванные экстремальной погодой или техническими неисправностями, могут произойти в любое время - риск и потенциальный ущерб могут быть сведены к минимуму только в момент возникновения таких случаев

1.3.2 Инсайдер в сравнении с внешними угрозами

В то время как защита КВОИ от внешних атак пользуется значительным количеством рекомендаций со стороны национальных и международных регулирующих органов, внутренние угрозы стали объектом сравнительно меньшего внимания. По сравнению с внешними субъектами, которые могут получить доступ к КВОИ только с помощью насильственных действий или ухищрений, инсайдеры имеют бесспорные преимущества. Инсайдерами часто являются сотрудники компании или поставщики. Они могут быть либо главными заговорщиками, либо выступать в качестве соучастников (например, информаторов) для сторонних участников. Они часто могут наблюдать за процессами, будучи не разоблаченными в течение определенного периода времени. Их знания (или легкость, с которой они могут получить знания) о соответствующем объекте могут быть легко использованы в преступных целях.

Принимая данное во внимание, методологии для проведения оценки рисков на конкретных объектах должны включать рассмотрение каждой роли в системе, и внутренние факторы уязвимости не должны рассматриваться как отдельная категория. Вместо этого типы угроз должны рассматриваться вместе с инсайдерским элементом, включенным в каждую категорию. Например, при рассмотрении категории угрозы, такой как персональное ИЭУ, используемое для нападения на самолет, тем, кто проводит оценку, следует отдельно рассмотреть как пассажирское ИЭУ, используемое для нападения на самолет, так и персональное ИЭУ, вносимое экипажем и / или сотрудниками, используемое для нападения на самолет.

В Разделе 2.8 приведены некоторые примеры мер по защите КВОИ от угроз такого типа. В этой области ключевую превентивную роль могут играть операторы КВОИ, начиная с осуществления эффективного отбора персонала и процедур осмотра.

1.3.3 Отдельные цели в сравнении с групповыми целями

Угрозы в отношении КВОИ могут быть либо отдельными или случайными действиями, либо частью более широкого плана по атаке на инфраструктуру в одном и том же секторе (например, атомные электростанции), принадлежащую одному владельцу / оператору или находящуюся в той же географической зоне. Можно вполне представить, что действия, мотивированные террористами, нацелены на КВОИ во многом таким же образом, как и в случае промышленного шпионажа, когда кибератаки часто начинаются как «кампании» или серийные атаки. Например, в 2011 году так называемая атака «LURID» была направлена, в частности, на системы ИКТ ряда дипломатических миссий и связанных с космосом правительственных учреждений.

Выявление закономерностей в подобных сценариях часто требует сильных аналитических инструментов и обработки информации из обширных и разнородных источников. Чтобы еще больше усложнить ситуацию, как подчеркивает ОБСЕ, в отношении энергетического сектора, информация о большинстве кибератак не публикуются, поскольку соответствующие операторы не хотят сообщать об этих инцидентах. Тем не менее, способность распознавать основную динамику и методы как можно раньше является ключевым фактором, позволяющим властям обмениваться оперативной информацией. Это повышает способность более эффективно реагировать на текущие атаки и предотвращать неизбежные атаки против вероятных жертв (ОБСЕ, 2013 г.).

В некоторых случаях то, что выглядит как отдельная атака, направленная на относительно «неважные» цели, в действительности может являться частью более амбициозных и постепенных криминальных стратегий[3].

[3] В совместном отчете МНБ/ФБР, опубликованном в 2017 году, отмечается, что определенные сети правительства США в энергетическом, ядерном, водном, авиационном и критически важным секторах промышленности подвергаются риску целенаправленных действий развитых устойчивых угроз (APT). МНБ оценило эту деятельность как «многоэтапную кампанию по вторжению, осуществляемую субъектами угроз, нацеленными на системы с низким уровнем безопасности и небольшими сетями, чтобы получить доступ и двигаться со стороны к сетям крупных владельцев ценных активов в энергетическом секторе». Согласно отчету, «субъекты угрозы активно преследовали свои конечные цели в течение долгосрочной кампании», а такие компании, как сторонние поставщики, изначально были целевыми объектами. (См. МНБ, Развитая устойчивая угроза деятельности, направленной на секторы энергетики и другие критически важные инфраструктуры, 20 октября 2017 г., по адресу: www.us-cert.gov/ncas/alerts/TA17-293Амм. См. также: Коннер Форрест, «МНБ, ФБР предупреждают о кибератаках, направленных на энергетическую инфраструктуру, государственные структуры ", 23 октября 2017 года, TechRepublic, на: www.techrepublic.com/article/dhs-fbi-warn-of-cyberattacks-targeting-energy-infrastructure-government-entities).

1.4 Террористические мотивы нападения на КВОИ

Разнородная природа КВОИ, а также различные географические и институциональные условия, в которых они расположены и функционируют, крайне затрудняют принятие общих выводов относительно того, что побуждает террористов совершать нападения на КВОИ в отличие от некритических целей. И все же, анализ мотивов терроризма может дать полезную информацию в рамках более широкой оценки угроз, требуемых в рамках национальных стратегий по ЗКВОИ.

В рамках ограниченного эмпирического исследования, проведенного в этой области (Акерман, 2007), выясняется, что КВОИ являются привлекательными по ряду причин. Во-первых, они могут быть привлекательной целью из-за их стратегической ценности для общества, особенно в высокоиндустриальных странах западного полушария. Вмешательство в функционирование КВОИ, в идеале с возможностью генерирования каскадных эффектов, позволяет террористам максимизировать ущерб всего одним выстрелом и вселять страх до уровней, которые не могли бы быть достигнуты так же легко, напав на «обычные» цели. Таким образом, было сообщено, что члены Аль-Каиды потратили значительное количество времени на слежку за штаб-квартирой различных американских финансовых фирм и международных организаций. Можно утверждать, что эта основательная деятельность последовала за указом Усамы бен Ладена 2001 года, призывающим его филиалы «сосредоточиться на том, чтобы поразить экономику США всеми возможными средствами».

Другие КВОИ могут быть направлены на демонстрацию бессилия государственных учреждений. Например, террористические организации могут принять решение атаковать энергетические объекты, нефтепроводы и т. д., чтобы перекрыть поставки базовых услуг и выявить хрупкость государственных органов и связанной с ними политики правительства (Акерман 2007, стр.170).

Третьей возможной мотивацией, связанной с двумя предыдущими, было бы желание получить более высокий уровень общественной огласки, чем это было бы возможно, сосредоточившись на «низкопрофильных» целях.

Как это ни парадоксально, террористы могут добиваться контроля над КВОИ не для того, чтобы причинять ущерб или запугивать, а совершенно по противоположной причине - желания установить свою собственную легитимность / социальную приемлемость. Как уже отмечалось, несмотря на то, что большинство операций, проводимых ИГИЛ с использованием водной инфраструктуры, были направлены на то, чтобы помешать передвижению войск и борьбе с военными, «такие усилия также часто [имели] дополнительное преимущество в плане активизации усилий по набору персонала, позволяя воде течь в города, симпатизирующие делу Исламского государства, или даже просто делая лучшую работу по предоставлению необходимых услуг, организация [могла] привлечь больше мужчин и женщин в свои ряды» (Vishwanath 2015).

Скорее всего, в нескольких случаях существует совокупность факторов, побуждающих террористические группы совершать нападения с участием КВОИ. Эти стимулы также должны быть сбалансированы с рядом ограничений. Окончательное решение относительно целевой инфраструктуры будет зависеть от оперативных возможностей группы для запуска конкретной атаки. Защитные меры, принятые на определенном КВОИ, будут, естественно, влиять на такое решение. Это не означает, что террористы будут атаковать КВОИ только тогда, когда они уверены, что смогут вмешаться в ее работу. Простая попытка, даже неудачная или та, которая наносит очень ограниченный ущерб, может обеспечить желаемый уровень резонанса в обществе, особенно когда цель выбрана для символического значения.

1.5 Противодействие террористическим угрозам для КВОИ с помощью правозащитного подхода

Терроризм создает серьезную угрозу для самих принципов верховенства права, защиты прав человека и их эффективного осуществления. В контексте своих обязательств по международному праву в сфере прав человека, государства обязаны защищать лиц, находящихся под их юрисдикцией, от ненадлежащего вмешательства в их права со стороны третьих лиц, включая террористических структур. Эта обязанность особенно важна, учитывая потенциальное воздействие от нападения на КВОИ могут оказать на население, учитывая роль, которую такая инфраструктура часто играет в поддержании или выполнении жизненно важных функций общества. Ущерб, нарушение или разрушение критически важных объектов инфраструктуры может привести к далеко идущим последствиям для широкого спектра прав человека: от права на жизнь и безопасность человека до права на здоровье и здоровую окружающую среду, права на образование, а также водоснабжение, санитарию и другие аспекты права на адекватный жизненный уровень.

Обязанность государств защищать права человека подразумевает обязательство принимать необходимые и адекватные меры для предотвращения, противодействия и наказания за действия, которые ставят под угрозу эти права, такие как угрозы национальной безопасности или насильственные преступления, включая терроризм. В этом отношении государства должны руководствоваться, среди прочего, глобальной контртеррористической стратегией (ГКТС), в которой подчеркивается, что эффективная борьба с терроризмом и обеспечение уважения прав человека являются не конкурирующими, а взаимодополняющими и взаимоподкрепляющими целями. Действительно, продвижение и защита прав человека являются независимой опорой и всеобъемлющей необходимостью для обеспечения успешного осуществления всех четырех компонентов ГКТС. Кроме того, соответствующие положения резолюций Совета Безопасности требуют, чтобы любые меры, принимаемые для предотвращения терроризма и борьбы с ним, соответствовали обязательствам государств по международному праву, в частности международному праву по правам человека, праву беженцев и международному гуманитарному праву.

В интересах борьбы с террористическими угрозами для КВОИ государственные органы могут временно принимать меры, которые могут привести к ограничению определенных прав, что приведет к ограничению некоторых прав, при условии, что эти ограничения соответствуют условиям, установленным в международном праве по правам человека. Меры, принимаемые в этом отношении, должны быть действенным ответом на имеющуюся угрозу, которые требуются в зависимости от ситуации, иметь четкую правовую основу, необходимую и соразмерную для эффективного устранения угрозы. Государства должны обеспечить создание удовлетворительных гарантий для защиты от произвольного и непропорционального вмешательства в права человека в этом контексте. Для осмысленного соблюдения этих обязательств государствам настоятельно рекомендуется регулярно проводить оценку мер в отношении прав человека, принятых для борьбы с угрозой терроризма для критически важных объектов инфраструктуры, и обеспечить, чтобы такие меры основывались на фактических данных и, следовательно, были эффективными.

2. РАЗРАБОТКА НАЦИОНАЛЬНЫХ СТРАТЕГИЙ В ЦЕЛЯХ СНИЖЕНИЯ РИСКОВ ДЛЯ КВОИ

Резолюция Совета Безопасности 2341 (2017)
Пункт 2 постановляющей части

Резолюция Совета Безопасности (...)

Призывает государства-члены рассмотреть возможность разработки или дальнейшего совершенствования своих стратегий уменьшения рисков террористических нападений на критически важные объекты инфраструктуры — стратегий, которые должны предусматривать, в частности, оценку и улучшение понимания соответствующих рисков, принятие мер по обеспечению готовности, в том числе эффективного реагирования на такие нападения, а также содействие повышению оперативной совместимости в области безопасности и ликвидации последствий и поддержку эффективного взаимодействия всех заинтересованных сторон;

2.1 Почему национальная стратегия?

Большинство стран обеспечивает меры безопасности для своих КВОИ задолго до того, как защита КВОИ утвердилась в качестве самостоятельного политического поля. Защитные меры в основном принимались поэтапно и по частям в форме нормативных актов, охватывающих конкретные сектора или угрозы, или с акцентом на определенных частях процессов управления рисками. Иногда государственная политика достигала значительного уровня сложности и соответствовала самым высоким международным стандартам. Например, в атомной энергетике после окончания холодной войны Украина разработала современную и эффективную систему физической защиты ядерных объектов и материалов.

В результате можно спросить, почему странам следует разрабатывать общие общенациональные стратегии ЗКВОИ, когда зачастую в них уже введены подробные нормативные акты, политика и практика, охватывающие большинство, если не все, критически важные сектора. Наиболее веская причина заключается в том, что в современных обществах защита КВОИ является все более сложной задачей. Взаимозависимость между секторами с потенциалом для каскадных эффектов в случае аварий (будь то природного происхождения или техногенных) требует способности «видеть общую картину» как условие для эффективной координации действий по предотвращению, реагированию и восстановлению между секторами. Кроме того, использование чисто отраслевых или «вертикальных» подходов может привести к чрезмерному увеличению заинтересованных учреждений, дублированию работы и растрате ресурсов. Таким образом, всеобъемлющая стратегия направлена на рационализацию рабочих потоков, создание "экономии от масштаба" и более эффективное распределение финансовых и людских ресурсов вокруг ряда заранее определенных целей.

Это не означает, что общегосударственные стратегии по ЗКВОИ должны автоматически заменять существующие отраслевые меры защиты, особенно когда эти меры оказались успешными или соответствуют обязательным международным нормативным рамкам. Однако необходимо, чтобы страны объединяли различные элементы мозаики под общей эгидой и сделали их частью единой системы управления. Поскольку ЗКВОИ завязана с несколькими сферами деятельности (такими как энергетическая политика, транспортная политика, политика безопасности и т. д.), основными целями общегосударственной стратегии являются:

- определение организационных структур;
- установление измеримых целей и сроков;
- закладка основы для эффективного предотвращения и управления инцидентами путем гармонизации задачи между различными областями политики.

В этой связи, стратегии ЗКВОИ можно адаптировать к конкретным потребностям и подходам отдельных стран. Как указано в Разделе 2.5, страны приняли различные институциональные модели, отражающие не только их конкретные правовые традиции, но и различное культурное отношение к роли закона в обществе, взаимоотношениям между правительством, гражданами и деловым сектором.

Страны имеют значительные возможности для маневра в определении способов защиты своих КВОИ. Однако все они должны иметь концептуальные строительные блоки (стратегию), чтобы соединить точки и обеспечить гладкие рабочие отношения между всеми заинтересованными участниками.

2.2 Подходы с учетом всех факторов риска в сравнении с конкретными рисками

КВОИ подвержены полиморфным типам угроз. Эти угрозы могут быть естественными: например, 11 марта 2011 года землетрясение, вызванное цунами, спровоцировало крупную атомную аварию на Фукусиме, Япония.

Угрозы могут быть вызваны небрежным человеческим поведением: в 2006 году 10 миллионов человек по всей Европе испытали отключение электричества после действий оператора по передаче электроэнергии, который отключил кабель питания через реку Эмс, чтобы пропустить круизное судно.

Другие угрозы могут быть вызваны террористическими целями или другими преступными целями. Кибератаки с целью получения выкупа являются примером коммерческой деятельности, которая может серьезно повлиять на КВОИ, зашифровывая данные пользователей и требуя оплаты в обмен на разблокировку данных. Угрозы КВОИ также могут быть связаны с преступным поведением более тонким и косвенным образом. В Европе, Французская строительная ассоциация («Федерасьон Франсез дю Батиман») неоднократно предупреждала о причастности преступных сетей к незаконному обороту контрафактных и нестандартных материалов, используемых для строительства зданий. По сообщениям, многие компании в строительном секторе закупают несоответствующие, некачественные материалы, которые влияют на прочность инфраструктуры и подвергают их более высокому риску обрушения.

Поскольку страны призваны защищать КВОИ от множественных уровней риска, ключевой вопрос заключается в следующем: должны ли правительства принять единый план, охватывающий все возможные угрозы, или, скорее, предусмотреть принятие стратегий, связанных с конкретной опасностью / риском? В принципе, любой подход соответствует международно-правовой базе.

Среди стран, которые приняли стратегии ЗКВОИ, большинство придерживается подхода с учетом всех опасностей[4]. Это означает, что стратегические цели и организационные структуры сформированы таким образом, чтобы учитывать случайные, преднамеренные и естественные угрозы для КВОИ в целом. Подход, основанный на всех опасностях, часто рассматривается как предпосылка для наилучшего использования ограниченных доступных ресурсов и предотвращения ненужного дублирования. Основное обоснование заключается в том, что одни и те же процессы управления рисками и сотрудничества, а также механизмы реагирования на кризисы могут широко использоваться для реагирования на все виды угроз взаимозаменяемым образом. Подходы с учетом всех опасностей применяются такими странами, как Канада и Великобритания.

Другие страны применяют смешанный подход. Австралия, например, разработала специфичные руководящие принципы защиты КВОИ от террористических актов. Руководящие принципы дополняют общую стратегию страны по ЗКВОИ, которая расширяет ее сферу охвата прочих опасностей. В Испании институциональная архитектура для ЗКВОИ изложена в законе 8/2011 «Об установлении мер для защиты критически важных объектов инфраструктур». В отличие от других

[4] В контексте авиации, ИКАО применяет слово «опасности» для обозначения вопросов, связанных с безопасностью полетов. Связанные с безопасностью события более точно определены как «инциденты».

стран, испанский закон направлен на противодействие террористической угрозе, хотя он применяется и к другим (неуказанным) рискам.

В соответствии с резолюцией 2341 (2017) Совета Безопасности необходимо, чтобы террористическая угроза полностью и в срочном порядке отражалась при подготовке стратегических планов правительств по защите КВОИ. Имея это в виду, каждая страна может определять в рамках национальной политики наилучшие формы и способы защиты КВОИ от террористических актов в среде с множественными угрозами.

2.3 Стратегии ЗКВОИ в отношении других национальных политик

Большинство стран, в том числе те, которые не имеют специальных стратегий, посвященных ЗКВОИ, рассматривают вопросы, связанные с ЗКВОИ, в различных политических нормативных документах, введённых различными правительственными учреждениями. Эти документы обычно включают в себя национальные (в том числе кибер) стратегии и политику в области борьбы с терроризмом. Хотя эти различные политики могли быть приняты в разное время и различными государственными учреждениями, крайне важно, чтобы они стали всеми частями связного послания и подхода к ЗКВОИ. Это требует, в частности, чтобы страны определили:

- взаимодействие между этими другими политиками и специальной стратегией ЗКВОИ;
- степень, в которой эти другие политики и / или сама стратегия ЗКВОИ необходимо скорректировать и оптимизировать, чтобы избежать конфликтов и обеспечить общую координацию политики на национальном уровне.

В следующих разделах представлен обзор национальной политики, которая оказывает значительное влияние на ЗКВОИ, но не обязательно (или полностью) посвящённая целям ЗКВОИ.

2.3.1 Политика в отношении «легких мишеней»

В резолюции 2396 (2017) Совета Безопасности подчеркивается, что государствам-членам необходимо разрабатывать, пересматривать или вносить поправки в национальные оценки рисков и угроз с учетом легких целей с тем, чтобы разработать соответствующие планы действий в нештатных и чрезвычайных ситуациях при террористических атаках. В том же году Европейская комиссия разработала план, сфокусированный на общественных местах как ключевой категории легких целей (Европейская комиссия 2017).

Как упоминалось в Разделе 1.2, понятие легких целей концептуально отличается от понятия КВОИ. Основным следствием этого является то, что политика стран в отношении легких целей автоматически не удовлетворяет условиям и требованиям защиты КВОИ, особенно когда речь идет об осуществлении резолюции 2341 (2017) Совета Безопасности.

Однако это не означает, что эти две области должны обрабатываться разобщено. Национальная политика и практика, разработанные для легких целей, вполне могут оказаться полезными и послужить источником передовой практики в области КВОИ и наоборот. Это явный подход, принятый ЕОБ, организацией, представляющей европейскую индустрию безопасности и исследовательское

сообщество. Признавая дублирующие функции между политиками по легким целям и КВОИ, ЕОБ работает с обеими в одной и той же рабочей группе.

Изучение конкретной ситуации **1**
Федеральные объекты инфраструктуры Бельгии

Закон Бельгии от 1 июля 2011 года о защите критически важной инфраструктуры содержит понятие Места Федерального значения («Points d'Interet Federal»). Они определяются как «места, не обозначенные как критически важная инфраструктура, но представляющие особый интерес для общественного порядка, для особой защиты людей и имущества, для управления чрезвычайными ситуациями или для военных интересов, и которые могут потребовать защитных мер, принятых Генеральной дирекцией антикризисного центра (ГДАЦ).

Этот закон представляет собой пример единой нормативной базы, учитывающей как КВОИ, так и легкие цели. Хотя федеральные объекты инфраструктуры не соответствуют условиям, которые следует рассматривать как КВОИ, они все же заслуживают особого внимания и защиты.

Вместо того, чтобы использовать раздельный подход, следует изучить потенциал взаимодополняемости. Принимая во внимание различия в концептуальных и нормативных рамках, применимых к «легким» целям и КВОИ, странам рекомендуется развивать взаимодействие, принимая во внимание, что зачастую одни и те же государственные учреждения несут институциональные и оперативные обязанности в обеих областях одновременно.

2.3.2 Политика национальной безопасности

Национальная безопасность - это изменчивая концепция. Страны переводят его на различные подпункты и подходы в зависимости от ряда факторов и представлений, связанных с их конкретной историей, географическим положением или геополитическим контекстом. В большинстве случаев национальная безопасность включает в себя принципы, политику, процедуры и функции, которые направлены на то, чтобы гарантировать независимость, суверенитет и целостность страны, а также права граждан.

Некоторые страны явно включают ЗКВОИ в число своих приоритетов национальной безопасности. Тесная привязка ЗКВОИ к сфере задач национальной безопасности может помочь обеспечить усиленную политическую поддержку для последующей разработки специализированных стратегий по ЗКВОИ и облегчить их реализацию.

Изучение конкретной ситуации **2**
Стратегия национальной безопасности Польши 2014 года

В документе дается явная ссылка на ЗКВОИ в разделе «Защитные меры». Хотя этот раздел не раскрывает тему подробно и не определяет конкретные роли и обязанности, он имеет значение однозначной идентификации ЗКВОИ в качестве приоритета национальной безопасности. Другие части Стратегии устанавливают цели, которые актуальны для ЗКВОИ, как широко, так и в конкретных секторах, включая:

- Улучшение и развитие национальной системы антикризисного управления с целью обеспечения внутренней сплоченности и целостности, а также для обеспечения неискаженного сотрудничества в рамках систем антикризисного управления международных организаций, членом которых является Польша;

- Обеспечение энергетической и продовольственной безопасности;

- Повышение осведомленности общественности в области безопасности и расширение компетенций граждан, что позволяет им адекватно реагировать на кризисные ситуации.

2.3.3 Контртеррористическая политика

Хотя в большинстве контртеррористических стратегий конкретно не упоминаются КВОИ, ряд целей и институциональных механизмов, изложенных в них, способствуют сохранению целостности КВОИ и жизненно важных социальных функций, выполняемых ими. Например, контртеррористические стратегии косвенно затрагивают проблемы ЗКВОИ, когда они устанавливают процедуры общего антикризисного управления после террористической атаки. Более того, стратегии борьбы с терроризмом часто устанавливают широкие рамки для предотвращения совершения террористических преступлений (например, путем изучения подготовительных законодательных актов, создания взаимодействия между разведывательными и правоохранительными органами и т. д.).

Глобальная контртеррористическая стратегия Интерпола[5] включает область КВОИ в свой поток действий 4.6 «Оружие и материалы», определяя мандат Организации с точки зрения «повышения способности государств-членов защищать свою критически важную инфраструктуру и уязвимые цели от физических и кибертеррористических атак»[6].

Стратегии ЗКВОИ должны объединять концепции и процедуры, изложенные в основах политики борьбы с терроризмом, путем их адаптации к конкретным потребностям и условиям ЗКВОИ.

[5] AG-2016-RES-03

[6] Конкретная реализация потока действий 4.6 приводит к тесному сотрудничеству между контртеррористической дирекцией Интерпола, базирующейся в Генеральном секретариате в Лионе, Франция, и инновационным центром Организации, расположенным в глобальном комплексе инноваций Интерпола, Сингапур.

Изучение конкретной ситуации **3**
Контртеррористическая стратегия Швеции

Швеция формулирует свою контртеррористическую стратегию в трех направлениях: предотвращать, упреждать и защищать. В частности, в рамках «защиты» цель состоит в том, чтобы «обеспечить надежную защиту людей, информации, функций и средств - люди должны чувствовать себя в безопасности, защищенными и свободными в обществе». В стратегии конкретно упоминается Шведское агентство по гражданским ситуациям, которое официально играет координирующую роль по ЗКВОИ в Швеции. Контртеррористическая стратегия Швеции была опубликована в 2014 году, в том же году, когда был также выпущен план действий по ЗКВОИ. Разработка связанных программных документов на близком расстоянии друг от друга способствует принятию единых языков, терминологии и подходов в различных нормативных документах.

2.3.4 Политика кибербезопасности

Кибербезопасность можно определить как «набор инструментов, политик, концепций безопасности, мер безопасности, руководств, подходов к управлению рисками, действий, обучения, передового опыта, гарантий и технологий, которые можно использовать для защиты кибер-среды, организации и активов пользователя» (GFCE-Meridian 2016, стр.8). Политики в области кибербезопасности занимают центральное место в защите КВОИ, поскольку они обеспечивают основу, в которой страны определяют цели и средства защиты критически важных информационных инфраструктур (КИИ). Эта концепция более подробно рассматривается в разделе 2.4.2.

Ряд региональных инструментов отчетливо связывают концепции кибербезопасности с КВОИ. Например, Конвенция Африканского союза о кибербезопасности (2014 г.) требует, чтобы государства-члены «обязались разработать, в сотрудничестве с заинтересованными сторонами, национальную политику в области кибербезопасности, в которой признается важность критически важной информационной инфраструктуры (КИИ) для нации, определяет риски, с которыми сталкивается нация при использовании подхода всех опасностей, и определяет, как должны быть достигнуты цели такой политики»[7].

Другим примером является стратегия кибербезопасности Европейского Союза 2013 года, в соответствии с которой Европейская комиссия обязалась «продолжать свою деятельность, проводимую совместным исследовательским центром в тесной координации с властями государств-членов и владельцами и операторами критически важной инфраструктуры, по выявлению [сети и информационной безопасности] уязвимости европейских критически важных объектов инфраструктуры и стимулированию развития отказоустойчивых систем» (Европейская комиссия 2013). В соответствии с директивой Европейского Союза о сетевой и информационной безопасности[8], (Директива NIS), государства-члены ЕС должны назначить операторов услуг жизнеобеспечения (OES) и ввести новые требования к безопасности и отчетности для таких организаций.

Учитывая это, не все национальные стратегии кибербезопасности обеспечивают одинаковое место и «вес» для КВОИ, и между странами существуют значительные различия. Как уже отмечалось, «некоторые стратегии были написаны только с точки зрения киберпреступности или только с точки зрения интернета. Они, как правило, упускают из виду (национальные) явления дестабилизации и антикризисное управление для КИИ, а также межотраслевые воздействия. Стратегии, написанные с точки зрения кибербезопасности, основанные на национальной оценке риска, примут более широкую перспективу, которая даст место для ЗКВОИ и ЗКИИ» (GFCE-Meridian 2016, стр.8).

[7] Ст.24, Структура национальной кибербезопасности.
[8] Директива (ЕС) 2016/1148 о мерах по обеспечению высокого общего уровня безопасности сетевых и информационных систем по всему Союзу.

Полезным инструментом, предлагаемым МСЭ, является хранилище национальных стратегий по кибербезопасности (NSC). Оно включает в себя обширную коллекцию национальных стратегий по кибербезопасности, будь то в форме одного или нескольких документов или как часть более широких стратегий в области ИКТ или национальной безопасности[9]. Ввиду разнообразия подходов между различными существующими стратегиями по ЗКВОИ и кибербезопасности, МСЭ в настоящее время возглавляет усилия с различными глобальными участниками по созданию общего справочного руководства национальных стратегий по кибербезопасности. Этот документ призван дать странам четкое представление о цели и содержании национальной стратегии по кибербезопасности, обрисовать в общих чертах существующие модели и ресурсы и направлять страны в процессе разработки своих стратегий и оценки стратегии[10].

Изучение конкретной ситуации **4**
Законопроект о кибербезопасности Сингапура

Этот законопроект формализует политику страны в этой области и напрямую включает защиту КИИ в концепции по кибербезопасности и защитные меры. Законопроект преследует четыре цели:

- Обеспечить нормативную базу, формализующую обязательства владельцев КИИ по обеспечению кибербезопасности своих КИИ;
- Возложить на агентство по кибербезопасности Сингапура (CSA) полномочия по управлению угрозами и инцидентами кибербезопасности и реагированию на них;
- Создать основу для обмена информацией о кибербезопасности с CSA и защиты такой информации;
- Создать упрощенную систему лицензирования для поставщиков услуг кибербезопасности.

Источник: законопроект о кибербезопасности, по адресу:
www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.pdf

[9] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx
[10] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx

Изучение конкретной ситуации **5**

США – Департамент инициатив по обеспечению национальной безопасности

В Соединенных Штатах Америки Департамент инициатив по обеспечению национальной безопасности (ДИОНД) возглавляет усилия федерального правительства по обеспечению безопасности важнейших объектов инфраструктуры страны. Для предотвращения угроз, смягчения их последствий и реагирования на них инициативы ДОНБ включают:

- Разработку технологически нейтральной структуры добровольной кибербезопасности;
- Поощрение и стимулирование внедрения практики кибербезопасности;
- Увеличение объема, своевременности и качества обмена информацией о киберугрозах;
- Внесение строгой защиты частной жизни и гражданских свобод в каждую инициативу по обеспечению безопасности критически важных объектов инфраструктуры;
- Разработка ситуационной осведомленности, которая учитывает как физические аспекты, так и кибер-аспекты о том, как инфраструктура функционирует практически в реальном времени;
- Понимание каскадных последствий сбоев объектов инфраструктуры;
- Оценка и развитие государственно-частного партнерства;
- Обновление национального плана защиты объектов инфраструктуры;
- Разработка комплексного плана исследований и развития.

ДОНБ поощряет принятие системы кибербезопасности национального института стандартов и технологий (NIST) для улучшения кибербезопасности критически важных объектов инфраструктуры. Пересмотренная в апреле 2018 года структура NIST содержит руководство по четырем ключевым функциям, улучшающим управление рисками кибербезопасности:

Идентификация - разработать организационное понимание управления риска кибербезопасности для систем, людей, активов, данных и потенциала;
Защита - разработка и реализация соответствующих мер безопасности для обеспечения предоставления критически важных услуг;
Обнаружение - разработка и реализация соответствующих действий для выявления случаев кибербезопасности;
Реагирование - разработка и реализация соответствующих действий для принятия мер в отношении обнаруженного инцидента кибербезопасности;
Восстановление - разработка и реализация соответствующих действий для поддержания планов устойчивости и восстановления возможностей или услуг, которые были повреждены из-за инцидента кибербезопасности.

Источники:

Министерство национальной безопасности, информационный бюллетень: EO 13636 «Улучшение кибербезопасности критически важных объектов инфраструктуры, безопасности и устойчивости критически важных объектов инфраструктуры PPD-21», по адресу: www.dhs.gov/sites/default/files/publications/eo-13636-ppd-2f-fact-sheet-508.pdf;

Министерство национальной безопасности, Программа добровольной помощи кибер-сообщества критически важных объектов инфраструктуры, по адресу: www.us-cert.gov/ccubedvp
Структура NIST по улучшению кибербезопасности критически важных объектов инфраструктуры, Версия 1.1, 16 апреля 2018, по адресу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.041620t8.pdf

2.3.5 Другие национальные политики

Когда разрабатывается национальная стратегия по ЗКВОИ, важно составить полный перечень всех национальных политик, имеющих к ней отношение. Могут существовать некоторые политические и нормативные структуры, касающиеся инфраструктуры в целом. Например, в 2017 году Сингапур принял закон об охране инфраструктуры. Закон, специально посвященный защите инфраструктур от террористических действий, вводит ряд понятий, таких как «охраняемая зона», «охраняемое место» и «охраняемая инфраструктура». Тем не менее, в нем не содержится прямой ссылки на «критически важные» объекты инфраструктуры с точки зрения активов или систем, выполняющих важные функции для сообщества. В подобных случаях необходимо определить роль и место существующих нормативных рамок в общих целях ЗКВОИ.

Некоторые политики могут не упоминать КВОИ просто потому, что они были приняты в то время, когда само понятие ЗКВОИ еще не вошло в основные политические дискуссии или по другим причинам. Если они затрагивают существенные вопросы, связанные с КВОИ, они должны подвергаться тщательному анализу с целью обеспечения их совместимости и взаимодополняемости с недавно разработанными национальными стратегиями по ЗКВОИ.

Другая соответствующая политика вытекает из международных обязательств стран в различных областях. Например, для соблюдения соответствующих международных документов[11], страны разработали целый ряд политик, законов, положений, стратегий, планов и мер по укреплению безопасности материалов ХБРЯ, объектов и связанной информации.

Изучение конкретной ситуации **6**
Федеральная программа Швейцарии по национальному экономическому снабжению (NES)

NES находит свою правовую основу в ст. 102 Конституции, согласно которой « Конфедерация обеспечивает снабжение страны жизненно важными товарами и услугами на случай угрозы насилия или войны, а также тяжелых состояний дефицита, с которыми экономика сама не может справиться. На эти случаи она принимает меры предосторожности.». Как уточняется в Национальной стратегии Швейцарии по защите критически важных объектов инфраструктуры, «NES охватывает примерно половину критически важных секторов и подсекторов национальной стратегии по ЗКВОИ и, таким образом, вносит решающий вклад в достижение целей этой последней. [...] NES фокусируется, главным образом, на долгосрочном дефиците на национальном уровне, в то время как стратегия по ЗКВОИ также учитывает краткосрочные или локальные нарушения (например, региональные перебои или сбои в работе).

[11] К таким документам относятся: конвенция о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсического оружия; конвенция о запрещении разработки, производства, накопления и применения химического оружия и его уничтожении; конвенция о физической защите ядерного материала; международная конвенция о борьбе с актами ядерного терроризма; глобальная контртеррористическая стратегия Организации Объединенных Наций и резолюция 1540 (2004) Совета Безопасности Организации Объединенных Наций).

2.4 Какие объекты инфраструктуры являются критически важными?

В резолюции 2341 (2017) прямо признается, что «каждое государство определяет, что составляет его критически важные объектов инфраструктуры». Тем не менее, она не рекомендует какой-либо конкретный метод выбора для выделения КВОИ среди множества объектов инфраструктур, расположенных на их территориях. Другие международные документы также не дают никаких указаний. Например, конвенция Африканского союза о кибербезопасности ограничивается требованием о том, чтобы «каждое государство-участник принимало такие законодательные и / или регулирующие меры, которые они сочтут необходимыми, для определения секторов, которые считаются чувствительными для своей национальной безопасности и благосостояния экономики, а также системы информационно-коммуникационных технологий, предназначенных для функционирования в этих секторах в качестве элементов критически важной информационной инфраструктуры [...]»[12]

Таким образом, странам предоставляется большая свобода действий при выборе критериев для определения того, какие объекты инфраструктуры, действующие на их территории, соответствуют порогу "критичности". Задача не тривиальная. Различие между важными / значимыми объектами инфраструктуры и теми, которые должны получить статус «критически важными», является ключевым фактором, позволяющим расставить приоритеты в отношении ограниченных ресурсов для защиты огромных активов, систем и процессов. С одной стороны, включение слишком большого количества инфраструктур в категорию «критически важных» может стать неуправляемой задачей (к тому же является финансово неустойчивой). С другой стороны, слишком ограничительный подход рискует оставить ряд ключевых активов и процессов незащищенными с потенциально катастрофическими последствиями в случае аварии. Один автор подчеркнул тенденцию правительств расширять довольно узкие национальные списки КВОИ. Это произошло бы потому, что «слишком мало лиц, принимающих решения, готовы принять политический риск, который может возникнуть при удалении элемента из «критически важного» списка, и возникает соблазн постоянно расширять круг объектов, которые считаются критически важными. Двусмысленность расточительна, поскольку ресурсы не направляются туда, где они могут оказать наибольшее влияние [...] «(Клементе 2013, стр.ix)

Несмотря на отсутствие общепримени мых критериев, можно найти руководства по конкретным секторам. Например, в то время как в инструментах ИКАО отсутствует определение «критически важные объекты инфраструктуры» как таковой, в руководстве по авиации ИКАО упоминается понятие «уязвимая точка» как «любой объект в аэропорту или связанный с ним, который, в случае повреждения или разрушения, может серьезно нарушить функционирование аэропорта. Неисправные пункты управления воздушным движением, средства связи, радионавигационные средства, силовые трансформаторы, первичные и вторичные источники питания и топливные установки как в аэропорту, так и за его пределами, должны рассматриваться как уязвимые точки. Средствам связи и радионавигации, которые могут быть повреждены, необходимо обеспечить более высокий уровень безопасности».[13]

В морском секторе кодекс ISPS определяет активы, которые правительственные учреждения, местные администрации, судоходство и портовые отрасли должны защищать от угроз безопасности, затрагивающих суда или портовые объекты, используемые в международной торговле. Соответственно, «планы безопасности судна» понимаются как «планы, разработанные для обеспечения применения на борту судна мер, направленных на защиту лиц на борту, груза, грузовых транспортных единиц, складов судна или судна от рисков инцидента безопасности». Ожидается, что также будут подготовлены планы обеспечения безопасности «для защиты портового объекта и судов,

[12] Ст.24, Легальные меры.
[13] Руководство по авиационной безопасности (Doc 8973 - ограничен).

людей, грузов, грузовых транспортных единиц и судовых складов в пределах портового объекта от риска инцидента безопасности»[14]

2.4.1 Определение «критичности»

Первым шагом в процессах идентификации КВОИ обычно является принятие всеобъемлющего определения того, что подразумевается под КВОИ. Это полезно для создания площадки, на которой будут разрабатываться дальнейшие политические и нормативные рамки. CIPRNet[15] выделил более 100 таких определений, из которых в таблице [число] приводится выборка. В целом, в то время как определения некоторых стран подчеркивают конечность или назначение инфраструктуры (т. е. критичность связана с выполнением основных социальных функций), другие делают упор на последствия разрушения или сбоя (т. е. критичность обусловлена конкретными последствиями прерывания обслуживания).

КВОИ могут быть определены, среди прочего, с учетом той роли, которую они играют в продвижении и защите прав человека (например, инфраструктуры, которая жизненно важна для функционирования систем оказания медицинской помощи; систем аварийного обслуживания, систем водоснабжения и канализации и т. д.), а также влияние на права человека, которое может случиться из-за повреждений, нарушений или разрушений объектов инфраструктуры (например, неспособность предоставить адекватные или даже жизненно важные медицинские услуги, ущерб окружающей среде, который может привести к гибели людей, вынужденное перемещение, негативно влияющее на право на здоровье и т. д.). Такой подход соответствует духу существующих определений. Например, ЕС определяет «критически важные объекты инфраструктуры» как «актив, систему или ее часть», которая «необходима для поддержания жизненно важных функций общества, здоровья, безопасности, сохранности, экономического или социального благополучия людей», нарушение или разрушение которых окажет значительное влияние «в результате несоблюдения этих функций»[16]. В том же духе закон о вооруженных конфликтах предоставляет особую защиту инфраструктуре, которая необходима для выживания гражданского населения или разрушение которого может привести к серьезным жертвам или нанести ущерб здоровью и выживанию населения (Первый дополнительный протокол к Женевским конвенциям, ст. 54-56, 1949 года).

Таблица 2: Национальные определения КВОИ

Австрия	Критически важные объекты инфраструктуры - это те объекты инфраструктуры или их части, которые имеют решающее значение для обеспечения важных социальных функций. Их отказ или разрушение оказывает серьезное воздействие на здоровье, безопасность или экономическое и социальное благополучие населения или функционирование правительственных учреждений (Стратегия кибербезопасности Австрии, 2013г.).
Канада	К критически важным объектам инфраструктуры относятся процессы, системы, средства, технологии, сети, активы и услуги, необходимые для здоровья, безопасности, охраны или экономического благосостояния канадцев и эффективного функционирования правительства (Управление по чрезвычайным ситуациям Канады, 2011 г.)
Франция	Жизненная инфраструктура - это любое учреждение, объект или структура, для которых повреждение, недоступность или разрушение в результате злонамеренного действия, диверсии или террористического акта могут прямо или косвенно: если ее деятельность трудно поддается замене или совместимости, серьезно отяготить военный или экономический потенциал, национальную безопасность или выживаемость нации, или серьезно повлиять на здоровье или жизнь населения (Генеральная межведомственная инструкция

[14] www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

[15] См., в частности, CIPedia, онлайн сервис сообщества подобный Википедии, фокусирующийся на проблемах защиты и устойчивости критически важной инфраструктуруы, разработанной проектом FP7 EC CIPRNet и продолженной волонтерами (https: // publicwiki-01.fraunhofer.de/CIPedia /index.php/Critical_Infrastructure).

[16] Директива Совета 2008/114/ЕС, статья 2.

	по безопасности жизнедеятельности, Генеральный секретариат по обороне и национальной безопасности).
Германия	Критически важные объекты инфраструктуры (КВОИ) - это организационные и физические структуры и объекты такой жизненной важности для общества и экономики страны, когда их отказ или деградация приводят к устойчивой нехватке поставок, значительным нарушениям общественной безопасности и сохранности или другим драматическим последствиям (Национальная стратегия защиты критически важных объектов инфраструктуры, 2009 г.)
Италия	Система, ресурс, процесс, структура, даже виртуальная, уничтожение прерывание или даже частичная или временная недоступность которых приводит к значительному ослаблению эффективности и нормального функционирования страны, а также безопасности и экономической, финансовой и социальной систем, включая органы центрального и местного публичного управления (Агентство гражданской защиты, глоссарий)
Кения	Критически важные объекты инфраструктуры описывают активы, которые необходимы для функционирования общества и экономики Кении (например, электросеть, телекоммуникации, водоснабжение) (Национальная стратегия кибербезопасности Кении)
Норвегия	Критически важные объекты инфраструктуры - это строительство и системы, необходимые для поддержания функций, которые охватывают основные потребности общества и чувство безопасности населения (Стратегия кибербезопасности для Норвегии)
Пакистан	Критически важные объекты инфраструктуры Пакистана включают в себя объекты инфраструктуры, указанные любым правительством Пакистана и такие прочие активы, системы и сети, как физические, так и виртуальные, настолько жизненно важные для государства или его органов, включая судебные органы, что их недееспособность или разрушение могут оказать разрушительное воздействие на национальную безопасность, экономику, здравоохранение, безопасность или связанные с этим вопросы (Законопроект о киберпреступности 2015)
Катар	Физические активы, системы или установки, которые в случае их разрушения, компрометации или уничтожения могут оказать серьезное влияние на здоровье, безопасность, сохранность или экономическое благосостояние Катара или на эффективное функционирование правительства Катара. Стратегия кибербезопасности Катара, 2014
Саудовская Аравия	Критически важные объекты инфраструктуры определяются как система и активы, как физические, так и виртуальные, настолько жизненно важные для Саудовской Аравии, что неспособность или разрушение таких систем и активов может оказать разрушительное воздействие на безопасность, национальную экономическую безопасность, национальное здравоохранение или сохранность, или любую их комбинацию. Разработка Национальной стратегии информационной безопасности для Королевства Саудовская Аравия Проект NISS 7
Тринидад и Тобаго	Критически важные объекты инфраструктуры означают компьютерные системы, устройства, сети, компьютерные программы, компьютерные данные, настолько жизненно важные для страны, что неспособность или разрушение или вмешательство в такие системы и активы могут оказать разрушительное воздействие на безопасность, оборону или международные отношения государства; или предоставление услуг, непосредственно связанных с национальной или экономической безопасностью, банковскими и финансовыми услугами, инфраструктурой связи, национальным здравоохранением и безопасностью, общественным транспортом, ключевой государственной инфраструктурой или их любой комбинацией (Национальная стратегия кибербезопасности, 2012)

Российская Федерация	Критически важные объекты инфраструктуры Российской Федерации является объектом, нарушение функционирования которого (или прекращение) приводит к потере контроля, разрушению инфраструктуры, необратимым негативным изменениям (или отказу) экономики субъекта Российской Федерации или административно-территориальных единиц или значительному ухудшению здоровья и безопасности людей, проживающих в этих районах, на длительный срок (Национальная безопасность России - Информационная безопасность (3 февраля 2012 г., N. 803)
Испания	КВОИ являются стратегическими инфраструктурами (объектами, сетями, системами и физическим и ИТ-оборудованием, на котором базируется работа основных служб, работа которых необходима) и где альтернативные решения невозможны, так что их нарушение или разрушение может серьезно повлиять на основные услуги (Закон 8/2011).
Швейцария	Под критически важным объектом инфраструктуры понимается инфраструктура, разрушение, отказ или нарушение которой будет иметь серьезные последствия для общества, частного сектора и государства (Национальная стратегия защиты Швейцарии от кибер риска, 2012)
Украина	(машинный перевод): критически важные объекты инфраструктуры - предприятия, учреждения и организации независимо от формы собственности, чья деятельность напрямую связана с технологическими процессами и / или предоставлением услуг, имеющих большое значение для экономики и промышленности, функционирования общества и безопасности населения, нарушение или неправильное функционирование которого может оказать негативное влияние на состояние национальной безопасности и обороны Украины, окружающую среду, вызвать имущественный шок и / или создать угрозу для жизни и здоровья (Закон Украины, Об основных принципах обеспечения кибербезопасности Украины, 2163-19)
США	Системы и активы, как физические, так и виртуальные, настолько жизненно важные для США, что неспособность или разрушение таких систем и активов окажет разрушительное воздействие на безопасность, национальную экономическую безопасность, национальное здравоохранение или сохранность, или их любую комбинацию (Закон о борьбе с терроризмом в США, 2001)

Второй этап в идентификации КВОИ является наиболее сложным, поскольку именно здесь происходит «расстановка приоритетов». В частности, этот этап направлен на выявление секторов и подсекторов (или услуг), которые рассматриваются как критически важные. Первоначальный подход мог бы заключаться в рассмотрении других стран, которые имеют сходство в социальных, географических особенностях, а также сопоставимый уровень технического и экономического развития.

Ряд секторов, скорее всего, будет рассматриваться как «критически важные» во всех странах. Энергетический сектор является ярким примером этого. Страны зависят от снабжения электроэнергией для выполнения почти всех социальных и экономических функций, от электросвязи до перекачки воды и предоставления жизненно важных медицинских услуг. В то же время важно отметить, что определенный сектор или подсектор может иметь решающее значение для одной нации, но не для другой. Размер и особенности определенной национальной экономики вполне могут определить, что является критичным, а что менее критичным. Например, некоторые страны могут в значительной степени зависеть от индустрии туризма в получении доходов и, в конечном итоге, в качестве условия для поддержания социальной сплоченности и внутренней стабильности. Для этих стран защита индустрии туризма как «критически важной» может сыграть важную роль в обеспечении предоставления основных услуг обществу.

Кроме того, тот факт, что определенный сектор обозначен как критически важный, не должен автоматически означать, что все базовые службы являются критически важными. Например, в энергетическом секторе «служба централизованного теплоснабжения», скорее всего, не будет

включена в число критически важных на национальном уровне, но поставка электроэнергии будет включена. Принимая во внимание эти различия, страны в значительной степени приходят к аналогичным выводам. В таблице 3 приведен список из 11 секторов и 37 соответствующих подсекторов, определенных ЕС.

Таблица 3: Ориентировочный список секторов и подсекторов, определенных ЕС

I Энергетика	1 Добыча, переработка, обработка и хранение нефти и газа, включая трубопроводы 2 Производство электроэнергии 3 Передача электроэнергии, газа и нефти 4 Распределение электроэнергии, газа и нефти
II Информационные, коммуникационные технологии, ИКТ	5 Информационная система и защита сети 6 Инструменты автоматизации и управления системами (SCADAetc.) 7 Интернет 8 Предоставление фиксированных телекоммуникационных услуг 9 Предоставление мобильной связи 10 Радиосвязь и навигация 11 Спутниковая связь 12 Телерадиовещание
III Вода	13 Обеспечение питьевой водой 14 Контроль качества воды 15 Забойка скважин и контроль количества воды
IV Еда	16 Обеспечение продовольствием и продовольственной безопасности
V Здравоохранение	17 Медицинская и больничная помощь 18 Лекарства, сыворотки, вакцины и фармацевтика 19 Биолаборатории и биоагенты
VI Финансирование	20 Платежные услуги / платежные структуры (частные) 21 Государственное финансовое ассигнование
VII Общественный и правовой порядок и безопасность	22 Поддержание общественного и правового порядка, охраны и безопасности 23 Исполнение правосудия и содержание под стражей
VIII Гражданская администрация	24 Правительственные функции 25 Вооруженные силы 26 Услуги гражданской администрации 27 Службы спасения 28 Почтовые и курьерские услуги
IX Транспорт	29 Дорожный транспорт 30 Железнодорожный транспорт 31 Воздушное сообщение 32 Водный транспорт внутреннего сообщения 33 Морской и каботажный транспорт
X Химическая и атомная промышленность	34 Производство и хранение / переработка химических и атомных веществ 35 Трубопроводы опасных грузов (химические вещества)
XI Космос **Источник:** Европейская комиссия 2005	36 Космос 37 Исследования

Изучение конкретной ситуации **7**

Подход Нидерландов: от критически важных секторов к критически важным процессам

В 2014 году политика Нидерландов по КВОИ претерпела значительные реформы. Это привело к переходу от понятия «критически важные сектора» к понятию «критически важные процессы». Критически важными процессами являются те, которые могут привести к серьезным социальным нарушениям в случае их отказа или нарушения. Поскольку не все процессы в секторе являются критически важными, в настоящее время основное внимание уделяется критически важным процессам, а не критически важным секторам. Определение критически важных процессов позволяет более эффективно и целенаправленно использовать инструменты и ограниченные ресурсы. Оценка уровня критичности выполняется на основе установленных критериев воздействия, таких как экономический ущерб и физические последствия. Изменения в обществе, такие как изменение угроз и оценка инцидентов, могут привести к оценке новых процессов. В оценке проводится различие между двумя критически важными категориями, A и B. Отказ A-критически важных процессов имеет больший потенциальный эффект, чем отказ B-критически важных процессов. Различие между критическими значениями A и B может быть полезным для определения приоритетности инцидентов или развития потенциала, повышающего устойчивость. Расстановка приоритетов путем классификации критически важной инфраструктуры на две категории, A и B, чтобы иметь возможность расставлять приоритеты во время инцидентов и индивидуальные решения для мер по повышению устойчивости.

Категория A:
- Национальная транспортировка и распределение электроэнергии
- Добыча природного газа
- Поставки нефти
- Хранение, производство или переработка ядерных материалов
- Питьевое водоснабжение
- Управление водными ресурсами

Категория B
- Региональное распределение электроэнергии и газа
- Управление полетами и самолетами
- Управление морскими и внутренними перевозками
- Крупномасштабное хранение, производство или переработка нефтехимических ресурсов
- Финансовый сектор (банковские услуги, электронные переводы между банками, а также между банками и населением)
- Взаимодействие с аварийными службами и между ними
- Мобилизация полиции
- Государственные услуги, которые зависят от надежных, доступных цифровых информационных систем и систем данных

Каждое министерство несет ответственность за проведение оценки критически важных процессов, которые находятся в его ведении. Координирующее министерство юстиции и безопасности будет регулярно изучать методологию, чтобы убедиться в ее актуальности, и определит, имеются ли признаки возможных новых критически важных процессов.

Источник: Нидерланды 2018

Третий шаг связывает ранее установленные секторы и подсекторы со списком отдельных инфраструктурных активов, систем и процессов. Числа могут значительно варьироваться от незначительного числа до нескольких тысяч, в зависимости от размера стран, уровня экономического развития и т. д. Страны разработали множество наборов показателей для определения определенных инфраструктур как «критически важных». Эти индикаторы обычно стремятся «измерить» последствия

разрушения объектов инфраструктуры или функционального сбоя и включают выбор / комбинацию из следующего:

- Географический охват воздействия;
- Продолжительность воздействия;
- Тяжесть потенциальных последствий с точки зрения:
- экономических последствий (влияние на ВВП, прямые и косвенные экономические потери, численность занятого персонала, налоговые поступления);
- количества жертв и масштабы эвакуации населения;
- потери власти правительством / нарушение государственного управления;
- ущерба окружающей среде.

Изучение конкретной ситуации **8**
Системная критичность в сравнении с символической критичностью в Германии

В стратегии ЗКВОИ Германии проводится различие между критичностью системного и символического характера. Инфраструктура рассматривается как системная критичность всякий раз, когда - из-за ее структурного, функционального и технического положения в общей системе секторов инфраструктуры - она очень актуальна в отношении взаимозависимостей. Примерами являются электрическая, информационная и телекоммуникационная инфраструктура, которая из-за размера и плотности их соответствующих сетей имеет особое значение, и где большая площадь и длительное отключение могут привести к серьезным нарушениям общественной жизни и процессов, а также общественной безопасности. Инфраструктура может иметь символическую критичность, если ее утрата может происходить из-за ее культурного значения или ее важной роли в создании чувства идентичности с эмоциональной точки зрения.

Источник: Германия 2009

Можно использовать разнообразные методологии. Консорциум во главе с TNO, голландской исследовательской организацией, попытался схематически сгруппировать их по трем основным типам: i) подход, основанный на услугах (например, Швейцария), где правительство идентифицирует критически важные активы на основе отраслевых критериев, определяющих пороговые значения / количественную выработку уровня обслуживания активов, например количество доставленных мегаватт; ii) подход, основанный на операторе (например, Франция), где задача определения того, какие активы или услуги являются критически важными, остается за отдельными операторами КВОИ; iii) подход, основанный на активах или гибридах (например, в Великобритании), в котором используются элементы подходов, ориентированные как на услуги, так на оператора (RECIPE 2011, стр. 23).

Изучение конкретной ситуации **9**
Методологии по идентификации КИ: ЕС, Франция, Великобритания

Евросоюз

Четырехэтапная методология идентификации КВОИ изложена в Директиве Совета ЕС 2008/114 / ЕС от 8 декабря 2008 года об идентификации и обозначении европейских критически важных инфраструктур и оценке необходимости улучшения их защиты. Хотя технически Директива касается только определения европейских критически важных объектов инфраструктур (ЕКВОИ) в транспортном и энергетическом секторах, она косвенно предполагает, что ее методология применима к идентификации национальных КВОИ также в других секторах, помимо энергетики и транспорта. Приложение III описывает соответствующую процедуру следующим образом:

Этап 1

Каждое государство-член должно применять отраслевые критерии, чтобы сделать первый выбор критически важных инфраструктур в секторе.
Этап 2
Каждое государство-член должно применять определение критически важной инфраструктуры в соответствии со статьей 2 (a) к потенциальным ЕКВОИ, определенному на этапе 1. Значимость воздействия будет определяться либо с использованием национальных методов определения критически важных объектов инфраструктур, либо со ссылкой на межсекторальные критерии [см. этап 4 ниже] на соответствующем национальном уровне. Для инфраструктуры, предоставляющей услуги систем жизнеобеспечения, будут приняты во внимание наличие альтернатив и продолжительность сбоев / восстановлений.
Этап 3
Каждое государство-член должно применять трансграничный элемент определения ЕКВОИ в соответствии со статьей 2 (b) к потенциальным ЕКВОИ, который прошел первые два этапа этой процедуры. Потенциальные ЕКВОИ, которые удовлетворяют определению, перейдут на следующий этап процедуры. Для инфраструктуры, предоставляющей услуги систем жизнеобеспечения, будут приняты во внимание наличие альтернатив и продолжительность сбоев / восстановлений.
Этап 4
Каждое государство-член должно применять межотраслевые критерии к остальным потенциальным ЕКВОИ. Межотраслевые критерии должны учитывать: степень воздействия; и для инфраструктуры, предоставляющей услуги систем жизнеобеспечения, наличие альтернатив; и продолжительность срыва / восстановления. Потенциальные ЕКВОИ, который не удовлетворяют межотраслевым критериям, не будут считаться ЕКВОИ.
Потенциальные ЕКВОИ, прошедшие эту процедуру, должны сообщаться только тем государствам-членам, на которых потенциальный ЕКВОИ могут оказать существенное влияние.

Франция
Во Франции правительство не идентифицирует отдельные активы КВОИ напрямую. Вместо этого назначены так называемые «жизненно важные операторы» (ЖВО), которые, в свою очередь, отвечают за выявление отдельных активов. В соответствии с Кодексом обороны, ответственный министр («координирующее министерство») данного сектора деятельности назначает «жизненно важного оператора» (ЖВО) в консультации с другими соответствующими министерствами. Министр-координатор уведомляет оператора о своем намерении назначить его ЖВО. Этот шаг также является поводом для первоначальной консультации между правительством и оператором. Для обозначения ЖВО операторы должны выполнить два условия:
- их деятельность осуществляется полностью или частично в сфере деятельности, имеющей жизненно важное значение;- они управляют или используют, по крайней мере, одно учреждение, структуру или объект, чей ущерб, недоступность или разрушение в результате злонамеренных действий, диверсии или терроризма могут иметь серьезные последствия для способности нации к выживанию или здоровья и жизни населения.
В целом, статус в качестве ЖВО могут получить:
-ассоциации, фонды или международные организации; - государственные службы, местные органы власти, группа местных органов власти, государственное учреждение, независимый административный орган власти.
В случае корпорации, ЖВО может быть материнской компанией или дочерней компанией. Выбор делается после консультации с соответствующим оператором.
Несколько дочерних компаний одной и той же группы могут потенциально быть назначены. Когда назначение оператора выполняется одновременно несколькими министрами, консультативный процесс позволяет определить, какой министр будет выполнять функции координирующего. По мере возможности координирующее министерство должно отвечать за сектор жизненной важности, в котором ЖВО осуществляет свою основную деятельность.
В рамках своей обычной деятельности ЖВО может иметь субподрядную или аутсорсинговую, одну или несколько, функций, способствующих достижению жизненно важной деятельности. В этом случае OIV должен принять необходимые меры в отношении своего субподрядчика или поставщика, чтобы последний способствовал достижению безопасности и защиты ЗКИ.
Следуя своему назначению, ЖВО разрабатывает свои «планы безопасности оператора» (ПБО). Анализ рисков, проведенный во время разработки ПБО, позволяет им предоставлять, в качестве дополнения к

своему плану, список установок, предприятий или систем, которые они считают уместными для обозначения как «жизненно важные объекты» (ЖВО).
Источник: Франция 2014
Великобритания
Великобритания признает девять критически важных секторов и двадцать подчиненных критически важных служб. Эти службы в свою очередь состоят из активов, которые необходимо идентифицировать. Министерство, ответственное за сектор, проводит первоначальный отбор активов и операторов (операторы выбираются на основе их относительной доли рынка). Центр по защите национальной инфраструктуры проводит собственную оценку параллельно. На основе совокупных исходных данных операторов, ответственных министерств и Центра по защите национальной инфраструктуры, актив (который также может быть процессом) сопоставляется с последствиями потенциального сбоя в обслуживании. Шесть уровней критичности (от CAT0 до CAT5) были определены и сопоставлены с тремя конкретными межотраслевыми критериями, а именно: воздействие на жизнь, экономическое воздействие и влияние на жизненно важные услуги.
На общедоступном уровне эти критерии носят только описательный и субъективный характер. На классифицированном уровне каждому из восемнадцати возможных критериев присвоены количественные и объективные значения (метрики). Эта сегментация выполняется в сочетании с критериями, специфичными для каждого сектора, которые являются уникальными для каждого из девяти критически важных секторов. В результате получается очень небольшой набор активов с самыми высокими уровнями критичности. Только активы категории 3 и выше считаются действительно «критически важными». Комбинация уровня CAT и вероятности атаки, которая представляет собой комбинацию уязвимости (например, легкость доступа к активу) и угрозы (например, тип атаки и вероятность атаки, или, для угроз, вероятность неудачи), определяет приоритет актива. Масштаб вероятности может быть очень динамичным и может меняться много раз в год, в отношении угроз безопасности.
Источник: RECIPE 2011, с.23

2.4.2 Критически важные информационные объекты инфраструктуры (КВИОИ)

В современной экономике цепочки промышленного производства и поставки товаров и услуг как правительством, так и частным сектором в значительной степени управляются компьютеризированными системами, известными как системы промышленного контроля (СПК). За последние несколько десятилетий СПК постепенно получили подключение к Интернету и частным корпоративным сетям. Это изменение упростило производство и предоставление услуг. Кроме того, «создание систем управления промышленными сетями в более широком масштабе привело к увеличению синергии и эффективности, и из-за отмены регулирования коммунальных предприятий, информация в реальном времени становится все более важной для маркетинговых целей» (Shea 2003, стр.3).

В то же время тот факт, что СПК все чаще связаны с компьютерными системами компаний через Интернет, делает их гораздо более уязвимыми для кибератак. Конкретные проблемы безопасности связаны с устаревшими системами, то есть с теми СПК, которые были установлены в эпоху, предшествующую Интернету, и которые изначально не предназначались для целей подключения.

Важно отметить, что СПК используются практически во всех секторах КВОИ, поскольку они часто управляют бесперебойной работой на электростанциях, плотинах, мостах, телекоммуникационных вышках и т. д. Таким образом, СПК являются ключевыми компонентами, так называемых критически важных информационных инфраструктур (КИИ). Существует несколько национальных определений этой концепции. ОЭСР определяет КИИ как «такие взаимосвязанные информационные системы и сети, нарушение или разрушение которых может оказать серьезное влияние на здоровье, безопасность или экономическое благосостояние граждан или на эффективное функционирование правительства или экономики» (ОЭСР 2008).

Крайне важно, чтобы стратегии по ЗКВОИ признавали и обеспечивали защиту КИИ наравне с физическими объектами инфраструктуры, тем более что «мы можем приблизиться к точке, в которой различия между «объектами инфраструктуры» и «информационной инфраструктурой» не имеют значения, поскольку они сливаются в один постоянно расширяющийся круг критически важных «предметов». По мере увеличения зависимости от объектов инфраструктуры с поддержкой кибер операций, растет и распространение критически важных «узлов» (т. е. точек в системе, где сбой может значительно ухудшить работу сети) (Clemente 2013).

Важно отметить, что при идентификации КИИ, киберпространство необходимо принять во внимание. В результате может возникнуть необходимость включить объекты инфраструктуры, которые сами по себе не являются критически важными (например, небольшая электростанция), в той степени, в которой они внутренне связаны с критически важными объектами инфраструктуры (например, плотиной).

2.4.3 Взаимосвязи и взаимозависимости

Поставка основных товаров и услуг обществу все чаще становится результатом взаимодействия между несколькими поставщиками. Эти провайдеры охватывают все сектора и подсекторы КВОИ, образуя сложные взаимосвязи. Хотя взаимосвязь активов, систем и процессов основана на более эффективном управлении ресурсами, она увеличивает зависимости. Их можно широко определить как «взаимосвязь между двумя продуктами или услугами, в которой один продукт или услуга требуется для создания другого продукта или услуги».[17] Например, поставки продуктов питания зависят от транспорта, банковский / финансовый сектор использует телекоммуникации для аутентификации транзакций, а телекоммуникации зависят от прерванного распределения электроэнергии. Большинство основных услуг зависят от одновременного предоставления услуг из нескольких секторов. Например, здравоохранение не может быть предоставлено при отсутствии электричества, воды и аварийных служб одновременно.

Зависимости могут вызывать эффекты различной интенсивности и состоять из разных типов. В частности, после террористического нападения, КВОИ могут пострадать от:

- Физических зависимых объектов: функционирование одних объектов инфраструктуры зависят от поставок материальных продуктов из других объектов инфраструктуры;
- Кибер-зависимости: функционирование одних объектов инфраструктуры зависят от информации, передаваемой через информационную инфраструктуру.

Изучение конкретной ситуации **10**
Взаимозависимости и «жизненно важные зоны» Франции

Стратегия по ЗКВОИ во Франции вводит в действие понятие зависимостей, вводя понятие «жизненно важная зона» («zone d'importance vitale», ЖВЗ). ЖВЗ - это область, в которую внедрили несколько «жизненно важных точек» (ЖВТ), принадлежащих разным «жизненно важным операторам» (ЖВО), и для которых совместная оценка и управление безопасностью представляет дополнительную ценность. С точки зрения безопасности существует взаимозависимость между ЖВТ, когда:

- осуществление угрозы одной из них будет иметь последствия для неприкосновенности или деятельности других; или же
- меры безопасности, применяемые для одной ЖВТ или общей части, влияют на безопасность одной или нескольких других ЖВТ.

Существуют три типа географических областей:

[17] Проект CIPRNet, https://www.ciprnet.eu/home.html

- Случай 1: область, состоящая из соседних ЖВТ. ЖВТ являются смежными или расположены на сравнительно небольшом расстоянии друг от друга;
- Случай 2: область, состоящая из закрытых ЖВТ. ЖВТ "2" находится внутри ЖВТ "1";
- Случай 3: зона, объединяющая характеристики первых двух случаев.

В любом случае, создание области жизненной важности должно удовлетворить оперативную потребность и способствовать улучшению защиты ЖВТ путем объединения и оптимизации ресурсов. Под соответствующей областью следует понимать зону с однородными характеристиками, например, в определенных промышленных зонах, аэропортах, морских или речных портах.

Источник: Франция 2014

Важно отметить, что зависимости повышают уровень уязвимости. Угроза становится все более острой из-за широкой зависимости правительственных учреждений и частного сектора от информационных и коммуникационных технологий, которые усугубляют влияние межсекторальных и транснациональных зависимостей. В связи с этим было отмечено, что «сценарий, который вызывает наибольшую обеспокоенность у экспертов, заключается в комбинированном использовании кибератаки на КВОИ в сочетании с физической атакой. Такое использование кибертерроризма может привести к усилению эффектов физической атаки. Примером этого может быть обычная бомбовая атака на здание в сочетании с временным отказом в электроснабжении или телефонной связи. Итоговое ухудшение аварийного реагирования, пока резервные электрические или коммуникационные системы не будут задействованы и использованы, может увеличить число жертв и общественную панику» (Shea 2003, стр.9).

Когда уязвимости ведут к сбоям в результате террористической атаки, зависимости могут вызывать «каскадные эффекты». Например, распространение токсичных веществ в цепочке водоснабжения приводит к сбоям в системе здравоохранения.

Для стратегий ЗКВОИ крайне важно использовать причинно-следственную связь, которая существует между взаимосвязями КВОИ, зависимостями и уязвимостями, как способ:

- Достигнуть адекватного уровня понимания (со стороны всех заинтересованных сторон, будь то из частного или государственного сектора) точек системной уязвимости, что должно быть отражено в более точном управлении рисками и кризисами. Задача интеграции концепции зависимостей в процессы управления рисками и кризисами усложняется тем фактом, что зависимости могут меняться в зависимости от режима работы данного КВОИ. Например, хотя обычно больница не зависит от дизельного топлива, после сбоя в электрической системе она может внезапно стать зависимой от подачи дизельного топлива для работы аварийного генератора. Стратегии ЗКВОИ должны формировать зависимости как нестатические, а скорее динамичные и быстро меняющиеся отношения;

- Повышение осведомленности о взаимозависимости через межсекторальные сети (основанные, например, на обсуждении сценариев риска), чтобы стимулировать дальнейшее сотрудничество между различными игроками.

Изучение конкретной ситуации **11**
Нидерланды: межсекторальные семинары и обмен знаниями о зависимостях

В соответствии со своей стратегией по ЗКВОИ Нидерланды провели серию межсекторальных семинаров, позволяющих секторам КВОИ получить представление о последствиях вторичных зависимостей. Заинтересованные стороны определили технические и организационные сети, в которых работают критически важные сектора. Это позволило объединить публичные и частные

стороны для планирования и обсуждения сценариев угроз. Никакие конкретные модели не использовались для изучения анализа зависимостей, основная идея заключалась в том, что обмен знаниями через сетевое взаимодействие и обмен опытом позволил бы секторам лучше понимать зависимости и способы устранения уязвимостей. Кроме того, участвующие стороны будут лучше знакомы друг с другом и своими соответствующими возможностями, что увеличивает потенциал для эффективного сотрудничества в случае аварии. Для обсуждения использовались сценарии:

- Последствия нарушений КВОИ, например, прямой / косвенный, цепочка поставок, доступ / дефицит / целостность, период времени сбоя, характеристика сектора и человеческие факторы;
- Зависимости, резервирование и восстановление;
- Меры по снижению уязвимости.

Источник: RECIPE 2011, стр.32

Взаимосвязи и зависимости часто пересекают границы, что влечет за собой необходимость того, чтобы стратегии по ЗКВОИ также учитывали их международный размах. Этот аспект более подробно рассматривается в главе 6.

2.5 Проектирование архитектуры ЗКВОИ

Не существует единой, заранее определенной институциональной модели, определяющей, как страны должны защищать свои КВОИ. Таким образом, ожидается, что правительства выберут структуру, которая наилучшим образом соответствует их характеристикам с точки зрения возникающих угроз, размера и структуры их экономики и, в более общем плане, их культуры общественной политики и сложившейся институциональной практики. Примечательно, что архитектуры управления ЗКВОИ должны учитывать основную конституционную структуру страны, то есть унитарные / централизованные и федеративные / децентрализованные государства. Это особенно важно при распределении ролей и обязанностей между различными уровнями правительства.

2.5.1 Основные модели «управления»

Архитектура ЗКВОИ колеблется между двумя основными моделями. На одном конце спектра управление КВОИ основано на принципах саморегуляции, стимулах и добровольном соблюдении стандартов. Так называемый «добровольный подход» подчеркивает политику, сосредоточенную на необязательном руководстве. В соответствии с этой моделью всем заинтересованным сторонам (будь то из государственного или частного сектора) рекомендуется вносить вклад в определение и реализацию политики ЗКВОИ путем предоставления рекомендаций, убеждений и создания общего восприятия для достижения общей цели. Обязывающая сила законодательства и схем регулирования используется слабо и только в качестве дополнительного инструмента, за исключением определенных секторов (таких как атомный сектор), где они могут играть доминирующую роль.

На другом конце спектра лежит так называемый «обязательный подход», основанный на идее, что сотрудничество в области ЗКВОИ наилучшим образом достигается через создание обязательных

правовых рамок, сопровождаемых мерами наказаний для операторов КВОИ, которые не соблюдают требуемые стандарты в рамках установленных сроков.

На практике страны не следуют ни одному из подходов в их «чистых» формах. Скорее они принимают элементы обеих. Их системы могут быть определены только как преимущественно «добровольные» или «обязательные» по своей природе. Примерами первых являются США, Великобритания, Канада и Швейцария. Примерами последних являются Франция, Испания, Бельгия и Эстония.

Странам может быть трудно определить, какая модель лучше всего соответствует их потребностям. В частности, когда они впервые устанавливают политику ЗКВОИ, они могут принять структуры и процессы, которые в конечном итоге окажутся неадекватными. По этой причине страны часто создают механизмы для обеспечения того, чтобы стратегии периодически подвергались пересмотру. США предлагают пример страны, которая начала с чистой концепции добровольного участия операторов КВОИ в этом процессе. Несмотря на то, что он все еще основан на этом принципе, с течением времени он все чаще сталкивается с необходимостью укрепления своей правовой базы для защиты КВОИ. Урок здесь заключается в том, что страны должны учиться на своем опыте.

Институциональные рамки ЗКВОИ должны, как минимум, охватывать следующие аспекты:

- Определить правительственное агентство, которое играет общую координирующую роль в определении и реализации национальной стратегии по ЗКВОИ;

- Распределение обязанностей по конкретным секторам, как правило, отдельным министерствам на основе установленного опыта и предметной компетенции (например, продовольственная безопасность министерству сельского хозяйства, здравоохранение министерству здравоохранения и т. д.);

- Определить объем и формы взаимодействия между заинтересованными правительственными учреждениями и операторами КВОИ. В разделе 4.5.2 более подробно рассматривается динамика цены вопроса с точки зрения государственно-частного партнерства.

Таблица 4: Архитектура ЗКВОИ в отдельных странах

Австралия	В федеральной системе Австралии разные правительства несут прямую ответственность за КВОИ в зависимости от типа объектов инфраструктуры или характера угрозы. Межправительственная работа происходит на кооперативной основе. Правительства штатов и территорий несут ответственность за управление угрозами жизни и имуществу в пределах своей юрисдикции. Они готовятся к чрезвычайным ситуациям и реагируют на них, а также обеспечивают правопорядок. Они также часто предоставляют такие услуги, как здравоохранение и водоснабжение. Все правительства штатов и территорий Австралии имеют свои собственные программы КВОИ в соответствии с операционной средой и договоренностями для каждой юрисдикции. Стратегия призвана дополнять эти программы и поддерживать их цели, где это возможно. Правительства штатов и территорий также являются ключевыми участниками сети доверительного обмена информацией (TISN), основного механизма взаимодействия страны с инициативами по обмену информацией между бизнесом и правительством и повышением устойчивости. Австралийское правительство несет ответственность за национальную оборону и безопасность, а также за оказание помощи государствам и территориям в реагировании на крупномасштабные чрезвычайные ситуации по запросу. Правительство Австралии также осуществляет прямой обязательный надзор за рядом важнейших инфраструктурных секторов, таких как

	авиация, связь, морские нефтегазовые и банковские операции. В ряде случаев эти регулирующие органы участвуют в TISN (в рекомендательном качестве) с целью содействия устойчивости соответствующего сектора.
США	Министр национальной безопасности обеспечивает стратегическое руководство и координирует общие федеральные усилия. Федеральные агентства по конкретным секторам США (SSA) ведут совместные процессы для обеспечения безопасности КИ в каждом из 16 секторов КВОИ. Каждый SSA отвечает за разработку и реализацию отраслевого плана (SSP) на основе уникальных характеристик каждого сектора. Государственные, местные, племенные и территориальные (SLTT) правительства обеспечивают безопасность и устойчивость КВОИ, находящегося под их контролем, а также тех, которые принадлежат и управляются другими сторонами в пределах своих юрисдикций. Механизмы сотрудничества между владельцами и операторами частного сектора и правительственными учреждениями сформулированы вокруг нескольких отраслевых и межотраслевых координационных структур.
Великобритания	Секретариат по гражданским чрезвычайным ситуациям (CCS), являющийся частью Секретариата национальной безопасности, поддерживает премьер-министра и кабинет министров и возглавляет более широкие усилия правительства по гражданскому чрезвычайному планированию и реагированию. Специфические политические обязанности CCS следующие: - Национальная оценка рисков и национальный реестр рисков (выявление и оценка рисков для национальной безопасности и обороны, возникающих в результате терроризма, крупных промышленных аварий и стихийных бедствий, в течение 5 лет); - Оценка рисков национальной безопасности (определение глобальных рисков для интересов безопасности Великобритании, в течение 5-20 лет). Работая с владельцами и регуляторами КВОИ, правительственные департаменты, ответственные за 13 критически важных секторов, должны ежегодно составлять планы обеспечения безопасности и устойчивости секторов. В этих планах, основанных на рисках, определенных в Национальной оценке рисков, изложено понимание каждым департаментом рисков для своих секторов и основных видов деятельности, которые они предпримут для устранения этих рисков в предстоящем году. Несколько агентств предоставляют центральному правительству, регулирующим органам, а также владельцам и операторам инфраструктуры консультации по вопросам рисков и смягчения последствий для инфраструктуры, в частности Центр по защите национальной инфраструктуры и Национальный центр кибербезопасности. Никакие явные меры наказания или другие последствия не устанавливаются в случае, если оператор КВОИ не взаимодействует с правительством.
Канада	Архитектура ЗКВОИ имеет сильный добровольный компонент. Обязанности распределяются между федеральными, провинциальными и территориальными правительствами, местными властями и владельцами, и операторами критически важной инфраструктуры. Все эти участники представлены в национальных сетях сектора (для каждого из десяти определенных критически важных секторов инфраструктуры), чьи цели: - выявлять проблемы национального, регионального или отраслевого значения; - использовать предметную экспертизу из важнейших секторов инфраструктуры для обеспечения руководства текущими и будущими проблемами; а также

	- разработать механизмы и лучшие практики для повышения устойчивости критически важной инфраструктуры по всему спектру мер по предотвращению, смягчению, готовности, реагированию и восстановлению. Участие в этих сетях добровольное. Их члены также руководят отраслевыми планами работы. Чтобы поддерживать комплексный и совместный подход к повышению устойчивости критически важных объектов инфраструктуры, национальный межсекторный форум способствует обмену информацией между отраслевыми сетями и решению межведомственных и межотраслевых взаимозависимостей.
Франция	Координацию по ЗКВОИ обеспечивает генеральный секретариат по обороне и национальной безопасности (SDGSN) от имени премьер-министра Франции. SDGSN утверждает директивы национальной безопасности (DNS), разработанные координирующими министерствами в каждом критически важном секторе. Эти министерства также являются контактами операторов. Префекты зон и департаментов (т.е. представители государства в департаменте или регионе) действуют под общим руководством Министерства внутренних дел в качестве территориальных координаторов стратегии ЗКВОИ. После назначения операторы должны предпринять несколько шагов: назначение делегата по обороне и безопасности (привилегированное контактное лицо с административным органом), разработка плана безопасности оператора, в котором излагается политика безопасности оператора, и разработка проекта конкретных планов защиты для каждой из определенных «жизненно важных точек». Задача по контролю, соответствуют ли уровни безопасности в жизненно важных точках минимальным требованиям, ожидаемым на местах, возложена на CIDS и CZDS, поддерживаемые префектами департаментов. Контрольные отчеты направлены на выявление уязвимостей в отношении выявленных угроз и рекомендуют меры, которые необходимо предпринять для повышения устойчивости. В крайних случаях несоблюдения, политика контроля может привести к передаче в судебный орган для судебного преследования и применения уголовных мер наказаний в случае нарушения правил.
Испания	Госсекретарь по безопасности через национальный центр защиты КВОИ является высшим органом министерства внутренних дел, ответственным за систему ЗКВОИ. Для каждого стратегического сектора, назначается, по крайней мере, один субъект от общей государственной администрации с правами продвигать в пределах своей компетенции политику правительства в области безопасности и обеспечивать ее применение. С точки зрения привлечения операторов КВОИ, Испания является типичным примером "обязательного подхода". Система основана на подробных нормативных положениях, требующих принятия различных уровней стратегических планов и планов безопасности, разработка и утверждение которых осуществляется различными участниками в конкретные сроки. В частности: a) Национальный план защиты КВОИ: устанавливает критерии и руководящие принципы для мобилизации оперативных возможностей государственных администраций в координации с операторами; b) Секторальные стратегические планы: позволяют определить объем основных услуг в каждом из выявленных секторов, уязвимости системы, потенциальные последствия бездействия и стратегические меры, необходимые для обеспечения устойчивости системы. c) Планы безопасности оператора: определение общих политик операторов для обеспечения безопасности объектов или систем, которыми они владеют или управляют; они должны быть представлены в течение шести месяцев после

	уведомления министерства внутренних дел о назначении оператора; d) Конкретные планы защиты: определить конкретные меры, которые уже приняты, и те, которые должны быть приняты операторами для обеспечения безопасности (физической и логической) своих КВОИ; они должны быть представлены в течение четырех месяцев после утверждения плана безопасности оператора министерством внутренних дел; e) Планы оперативной поддержки: определить конкретные меры, которые должны быть реализованы государственными администрациями в поддержку критически важных операторов.
Нидерланды	Основную ответственность за непрерывность и устойчивость критически важных процессов несут их действительные операторы. Это включает в себя понимание угроз, уязвимостей и рисков, а также развитие и поддержание потенциала, который увеличивает и защищает устойчивость критически важных процессов. Ответственное министерство устанавливает общие рамки для секторов, подпадающих под его ответственность (в политике или в законах и нормативных актах). Министерства, в сотрудничестве с операторами критически важных процессов, несут ответственность за защиту и проверку возможностей, связанных с КВОИ. Охрана и безопасность регионов предоставляет поддержку операторам критически важных процессов в случае (неизбежного) сбоя или отказа, если возможности недостаточны, а общественный порядок и безопасность находятся под угрозой. Это происходит в координации с операторами критически важных процессов и министерств. Тот факт, что существует множество различных заинтересованных сторон, требует координации и управления. Национальный координатор по вопросам безопасности и борьбы с терроризмом (NCTV) министерства юстиции и безопасности отвечает за общую координацию и управление задачами.
Германия	Архитектура ЗКВОИ страны основана на определении 6 рабочих пакетов, соответствующих различным этапам цикла управления рисками. Государственный сектор (под координацией федерального министерства внутренних дел) играет ведущую роль в реализации первых четырех пакетов при участии частного сектора / операторов. Взамен этого, при реализации пакетов 5 и 6, роли меняются местами, а компании и операторы выступают в роли «ведущих организаций». Рабочие пакеты: 1. определение общих целей защиты; 2. анализ угроз, уязвимостей и возможностей управления; 3. оценка угроз; 4. уточнение целей защиты с учетом существующих защитных мер; анализ существующих правил и, где это применимо, определение дополнительных мер, способствующих достижению цели; если и где требуется, законодательство. 5. Внедрение мер по достижению цели в первую очередь посредством: i) решений для конкретных ассоциаций и правил внутреннего распорядка; ii) соглашения о самообязательстве между бизнесом и промышленностью; iii) разработка концепций защиты компаниями. 6. Непрерывный, интенсивный процесс информирования о рисках (диалог по результатам анализа, оценкам, целям защиты и вариантам действий). Система предусматривает ряд институционализированных платформ с участием государственных органов, компаний и ассоциаций. Эти партнерские платформы безопасности могут быть организованы как: - Круглые столы по ЗКВОИ (федеральный уровень); - Круглые столы по ЗКВОИ (Länder); - Круглые столы по ЗКВОИ (уровень местного самоуправления);

	- Совместные круглые столы Федерации / Länder или Länder / местных органов власти.

2.5.2 Государственно-частные партнерства для ЗКВОИ

В большинстве стран подавляющее большинство активов КВОИ находятся в частной собственности. Кроме того, частные операторы находятся в авангарде инвестиций и главных усилий по разработке новых технологий производства и защиты. Эти обстоятельства в сочетании с тем фактом, что главная ответственность за защиту активов / систем КВОИ лежит на их владельцах / операторах, подчеркивают важность установления эффективного государственно-частного партнерства (ГЧП) для достижения адекватных уровней устойчивости.

При работе с ГЧП составители стратегий ЗКВОИ должны быть нацелены на создание условий для их эффективности путем: i) оценки факторов успеха и сдерживающих факторов; ii) определение объемов; iii) определение форм; iv) рассмотрение проблем и вызовов.

i) Оценка факторов успеха и ограничения ГЧП

«Меридианский процесс», открытый форум для обмена идеями по ЗКВОИ и сотрудничества между высокопоставленными правительственными политиками, определил следующие факторы, лежащие в основе эффективных ГЧП (GFCE-Меридиан 2016, стр.55):

Доверие: поскольку ГЧП часто касается проблемных субъектов (коммерчески, с точки зрения репутации, безопасности, перераспределения обязанностей), важно создать атмосферу доверия, в которой все организации будут осознавать потребность друг друга в осмотрительности и последовательно действовать соответственно. Четкие руководящие принципы членства в оперативных правилах могут способствовать укреплению доверия;

Ценность: участие в ГЧП должно приносить пользу, иначе энтузиазм к участию быстро угаснет;

Уважение: все организации должны признавать и уважать добавленную стоимость, которую другие организации вносят в сотрудничество. Это может быть достигнуто путем «продажи» Вашей собственной добавленной стоимости (в терминологии Вашего партнера) при активном поиске добавленной стоимости Ваших партнеров;

Кодекс поведения: необходимо иметь четкие, конкретные и предсказуемые правила, которые не предоставляют возможности для разобщения и предотвращают любой конфликт интересов;

Осведомленность о возможностях и ограничениях друг друга: это предотвращает конфликт через неправильное суждение о причине отрицательного ответа и позволяет оптимально окупить усилия альянса. Это означает, что обе организации должны быть осведомлены о деятельности друг друга. Хороший способ добиться этого - работать вместе долгое время, предпочтительно годы;

Реалистичные ожидания: все организации должны учитывать доступность ресурсов, бюджет развития и т. д., чтобы иметь возможность формировать реалистичные ожидания ГЧП.

ii) Определить сферу применения ГЧП

ГЧП не должны фокусироваться на одном конкретном этапе цикла ЗКВОИ, но должны охватывать все из них, от разработки и реализации мер до этапов управления рисками и кризисами. Преимущества объединения ресурсов, взаимной поддержки и совместного принятия решений между государственным сектором и частными операторами КВОИ распространяются на такие области, как

оценки безопасности, обзор мер безопасности, определение критически важных активов и процессов, разработка планов действий в чрезвычайных ситуациях, обучение реагированию на инциденты, и т.п.

Обмен информацией является ключевым (хотя и не исключительным) аспектом ГЧП и ставит конкретные задачи, например, в области защиты данных. Вопросы, связанные с обменом информацией, рассматриваются в главе 4.

iii) Определение формы ГЧП:

Наиболее подходящая форма данного партнерства зависит от множества факторов, таких как преследуемые цели, число заинтересованных сторон, которые будут вовлечены, и от того, ожидается ли, что партнерство решит стратегические или операционные вопросы. ГЧП могут принимать самые разные формы, от очень неформальных форм сотрудничества до более формальных условий. Степень формальности часто связана с уровнем контроля, который государственные органы стремятся осуществлять. С другой стороны, утверждается, что «проектно-ориентированные» ГЧП, как правило, более эффективны, чем «процессо-ориентированные», поскольку первый обычно включает более четко определенные миссии, сроки и бюджеты (Колесникова, 2017, с.13.15).

Изучение конкретной ситуации **12**
Государственно-частное партнерство для обеспечения устойчивости критически важных объектов инфраструктуры в Финляндии

Национальное агентство по чрезвычайным ситуациям (NESA), созданное в 1993 году, отвечает за планирование, разработку и поддержание безопасности поставок в Финляндию. В то время как его историческая роль сохранения резервных запасов для защиты средств к существованию населения и функционирования экономики остается частью его стратегических задач, NESA все активнее участвует в обеспечении непрерывности и устойчивости бизнеса в различных секторах экономики через государственно-частное партнерство. NESA создало сеть тематических кластеров, где ключевые заинтересованные стороны критически важных секторов развивают партнерские отношения для оценки уязвимости и производительности, и планирования устойчивости. NESA также предлагает специальные инструменты, такие как информационные системы, хранилища и транспортные средства для обеспечения непрерывности бизнеса в этих областях. NESA также финансирует конкретные мероприятия, связанные с непрерывностью бизнеса и защитой критически важной инфраструктуры. Агентство готовит ежегодные отчеты, в которых оцениваются результаты деятельности компаний в критически важных секторах, включая рейтинги и конкретные рекомендации. Среди своих результатов, NESA может похвастаться расширением партнерских отношений между государственным и частным секторами с компаниями в критически важных секторах (в настоящее время их насчитывается более 1000), что привело к разработке плана обеспечения непрерывности бизнеса, соответствующего их деятельности и секторам.

Источник: Инструментарий ОЭСР по управлению рисками, по адресу: www.oecd.org/governance/toolkit-on-risk-governance/home/

iv) Предвидение проблем ГЧП

ГЧП, которые не совсем точно продуманы, подвержены риску стать «пустыми коробками», принося ограниченную или нулевую добавленную стоимость для ЗКВОИ. Чтобы гарантировать, что государственно-частные договоренности о сотрудничестве рождаются и продолжают оставаться актуальными и продуктивными усилиями, странам необходимо помнить о наиболее частых причинах неудач. Недостатки могут быть связаны с разрывом ожиданий между частным и государственным секторами, неустойчивыми моделями финансирования, нечетким разделением труда и т. д. Можно утверждать, что «предпочтения и восприятие затрат и выгод участвующих сторон в конечном итоге определят успех или провал партнерства. Чувство безотлагательности помогает создать связь между государственным и частным секторами, способствуя готовности к сотрудничеству и достижению общего видения, что в конечном итоге позволяет партнерству развиваться и продолжаться. Долговечность партнерства зависит от взаимодействия этих факторов и представляет собой динамический процесс с периодами как слабых, так и сильных показателей» (Колесникова, 2017, с. 13-15).

Другие проблемы могут быть связаны с отсутствием мотивации у бизнеса инвестировать финансовые ресурсы в защиту своих собственных КВОИ. В разделе 2.10.1 обсуждается необходимость стратегий ЗКВОИ для определения соответствующих типов стимулов в этом отношении.

ОБСЕ разработала базовое 8-ступенчатое руководство о том, как страны должны максимизировать выгоды, которые могут быть получены от ГЧП, используя общие интересы всех заинтересованных сторон. Несмотря на то, что руководящие принципы были разработаны в рамках передовой практики для критически важной энергетической инфраструктуры, они, как представляется, в целом применимы во всех секторах (ОБСЕ 2013, стр.69):

- Шаг 1: Проанализируйте и определите мотивацию каждого партнера, который будет включен в партнерства по ЗКИ, чтобы уточнить взаимные ожидания и вклады;

- Шаг 2: Определите амбиции и цели партнерства по ЗКВОИ на основе общих национальных целей ЗКВОИ; уточнить цели партнерства по ЗКВОИ и задачи, которые необходимо выполнить (см. также шаг 5);
- Шаг 3: Проверка существующей нормативной базы, относящейся к каждому критически важному сектору инфраструктуры; определить обязательные и самообязывающие нормы, правила и принципы; оценить адекватность существующей нормативной базы с учетом ожидаемых рисков и существующих уровней готовности; обсудить, как закрыть возможные пробелы;
- Шаг 4: Обеспечить механизмы, защиту и правовую определенность для обмена информацией, связанной с ЗКВОИ, между всеми заинтересованными сторонами. И обеспечить механизмы для добровольных усилий, включая разработку и обмен передовым опытом, консультации и диалог для обеспечения постоянного и эффективного партнерства;
- Шаг 5: Создать институциональную структуру, которая способствует межорганизационному сотрудничеству и обмену информацией; уточнить роли и вклад каждого партнера (например, правительственных учреждений, владельцев и операторов критически важной инфраструктуры, поставщиков продукции, ассоциаций); определить отдельные точки контакта для каждого партнера; установить руководящие принципы для сотрудничества;
- Шаг 6: Начать с малого, сосредоточившись на одном или двух критически важных секторах инфраструктуры; неуклонно расти, опираясь на готовность всех заинтересованных сторон к сотрудничеству и рассмотрению уровней угрозы;
- Шаг 7: Определить критически важные этапы, чтобы рассмотреть, что было достигнуто, и определить потенциальные следующие шаги;
- Шаг 8: Обеспечить постоянный процесс проверки для пересмотра и обновления партнерских отношений, чтобы гарантировать постоянный прогресс, соразмерный с общей картиной риска и мерами безопасности, которые необходимы для обеспечения оптимального уровня защиты.

Изучение конкретной ситуации **13**
UP Kritis: платформа Германии для государственно-частного партнерства по ЗКВОИ

Организованный в 2007 году и скорректированный в 2013 году, UP KRITIS является государственной / частной платформой Германии по ЗКВОИ для секторального и межотраслевого сотрудничества. Взаимное доверие лежит в основе его работы. Участники обмениваются ноу-хау и опытом и учатся друг у друга в отношении ЗКВОИ. В рамках UP KRITIS разрабатываются концепции, устанавливаются контакты, проводятся учения и создается, и запускается совместный подход к управлению кризисом в сфере ИТ. В то же время UP KRITIS занимается вопросами, которые выходят за пределы области ИТ, основываясь на признании того, что отдельного исследования физической безопасности и безопасности ИТ недостаточно для достижения общей цели защиты критически важных объектов инфраструктуры.

В рамках UP KRITIS имеют место две формы сотрудничества: оперативно-техническое сотрудничество (между всеми участниками) и стратегически-концептуальное сотрудничество (в установленных органах). Важно отметить, что бизнес вовлекается постепенно и может стать более или менее интенсивным в зависимости от готовности компаний к активному участию, цель состоит в том, чтобы система оставалась управляемой при одновременном обращении к как можно большему числу компаний из всех секторов КВОИ. В частности, организация сначала интегрируется в UP KRITIS в качестве «участника». Все немецкие операторы КВОИ, национальные профессиональные и отраслевые ассоциации из секторов КВОИ, а также компетентные государственные органы могут подать заявку на участие в UP KRITIS. Участники назначают представителей своей организации, которым предоставляется доступ к продуктам UP KRITIS, включая конфиденциальную информацию. Если организация желает сотрудничать более активно, она может стать «партнером» и подать заявку на интеграцию своих представителей в отраслевые рабочие группы и тематические рабочие группы. Каждая рабочая группа представляет собственную информационную сеть, в которой информацией можно обмениваться на конфиденциальной основе.

Другими ключевыми компонентами организационной структуры являются Пленум и Совет. Пленум является комитетом сотрудничества системы. Он действует во всех секторах, устанавливая ключевые стратегические направления деятельности UP KRITIS, принимая решение о создании или роспуске рабочих групп, планируя будущие совместные действия и т. д. Пленум состоит из представителей операторов КВОИ, их профессиональных и отраслевых ассоциаций, а также представителей государственного сектора. Совет укрепляет партнерские отношения и сотрудничество в рамках UP KRITIS и дает импульс для достижения стратегических целей и проектов. Он также гарантирует, что платформа может выполнять свои задачи, используя адекватные ресурсы и необходимую поддержку со стороны государственного и частного секторов. Совет состоит из высокопоставленных политиков операторов КВОИ и государственного сектора.

Источник: UP KRITIS 2014

2.5.3 Роль гражданского общества и общественности

Общественность в целом должна сыграть важную роль как в предотвращении атак на КВОИ, так и в снижении ущерба после того, как атака произошла (антикризисное управление). В некоторых странах четко и активно предусматривается роль отдельных лиц в стратегиях по ЗКВОИ. Например, французский план Vigipirate[18] инструктирует граждан о том, как вести себя в случае нападений в определенных контекстах, которые имеют отношение к защите информации, например, в метро, поездах, самолетах и на кораблях, или в случае нападений с использованием токсичного продукта. Швеция применяет подход «всего общества» после признания того, что «отдельные лица и семьи часто наиболее подвержены кризису или присутствуют на месте раньше, чем сотрудники аварийно-спасательных служб или другие социальные представители. Люди должны рассматриваться как активы» (Линдберг и Сунделиус 2013, стр.1304)

Методы и каналы для достижения совместных отношений со стороны общественности существенно отличаются от тех, которые требуются для привлечения операторов КВОИ. В качестве отправной точки, участие сообщества и отдельных лиц в общих усилиях по обеспечению устойчивости КВОИ влечет за собой принятие широких образовательных программ и кампаний по повышению осведомленности. Коммуникационные стратегии должны быть разными в зависимости от целевой группы. Эти стратегии могут поддерживаться на местном уровне и в зависимости от контекста такими мерами, как установление выделенных номеров экстренных служб, повторение сообщений через громкоговорители, напоминая пользователям общественного транспорта об обязанностях сообщать, и т. д. После волн террористических нападений за последние двадцать лет в транспортной системе крупных столиц, государственные администрации ряда стран приняли меры, чтобы побудить граждан быть бдительными и сообщать о подозрительных ситуациях властям.

Широкое использование технологической продукции населением также означает, что социальные сети могут способствовать повышению осведомленности общественности о ситуации, информировать людей о действиях, предпринимаемых правительством, и своевременно предоставлять инструкции по безопасности. Все это представляется особенно важным в быстро меняющихся сценариях.

Изучение конкретной ситуации **14**
Национальная система оповещения и информации народов Франции (SAIP)

SAIP, разработанный генеральным директоратом по гражданской безопасности и урегулированию кризисов (DGSCGC) министерства внутренних дел, в сотрудничестве с правительственной информационной службой (GIS), позволяет гражданам получать оповещения посредством уведомлений на смартфоны в случае подозрения на атаку или исключительное событие, которое

[18] http://www.gouvernement.fr/vigipirate

может произойти в результате нападения. Инструкции по безопасности, отправленные через прямых пользователей SAIP, предпринимают конкретные действия, такие как нахождение убежища в здании или эвакуация из опасной зоны, избежание вызова по телефону (за исключением неотложной медицинской помощи), не забирать детей в школе и т. д. Решение о том, отправлять ли сообщение и связанный с ним контент оставлены за органом, отвечающим за общую защиту населения, общественный порядок и гражданскую оборону. На местном уровне эта компетенция принадлежит мэру и префекту департамента. Это приложение дополняет существующую систему оповещения и информирования населения (SAIP) и является частью глобального подхода по повышению осведомленности населения о рисках.

Источник: www.gouvernement.fr/risques/l-application-d-alerte-mobile-saip

2.6 Разработка стратегий ЗКВОИ вокруг концепций управления рисками и кризисами

Эффективная национальная стратегия должна поставить процессы управления рисками и антикризисного управления в центр усилий ЗКВОИ. Независимо от того, какая институциональная модель выбрана, заинтересованные стороны, вовлеченные в ЗКВОИ (будь то владельцы / операторы КИ частного сектора или государственные органы), должны быть знакомы с этими концепциями и последовательно применять их в своем соответствующем секторе и областях компетенции.

2.6.1 Управление рисками

Бюро ООН по снижению риска бедствий (БСРБ ООН) определяет управление рисками как «системный подход и практику управления неопределенностью для минимизации потенциального ущерба и потерь. Управление рисками включает оценку и анализ рисков, а также реализацию стратегий и конкретных действий по контролю, снижению и переносу рисков» (БСРБ ООН 2009).

В контексте процессов управления рисками применительно к ЗКВОИ важно иметь четкое понимание ключевых концепций, которые часто (и по ошибке) взаимозаменяемы, а именно:

- *Угроза*: все, что использует уязвимость КВОИ
- *Уязвимость*: слабость КВОИ, которая может быть использована угрозой;
- *Риск*: вероятность ущерба, повреждения, разрушения или вмешательства в способность КВОИ предоставлять свои услуги в результате уязвимости, используемой угрозой.

Не существует уникального или универсального стандарта для управления рисками. Использование разных «полномочий» различными заинтересованными сторонами, отвечающими за эту задачу, может привести к несовместимым результатам. На государственном уровне использование различных методологий может затруднить, если не сделать невозможным, сравнение результатов внутри секторов и между ними, что потенциально может повлиять на надежность работы в целом. Поэтому странам важно поддерживать создание процессов управления рисками, охватывающих, как минимум, следующие элементы:

- Установление контекста - объем и параметры оценки риска;

- Оценка риска (определение, анализ, оценка) - преобразование данных риска в информацию для принятия решений;
- Снижение риска - преобразование информации о риске в решения и действия по снижению риска;
- На протяжении всего процесса:
- Коммуникация и консультации - определение методов коммуникации, используемых всеми заинтересованными сторонами, вовлеченными в процесс; а также
- Мониторинг и проверка - проведение регулярной проверки или надзора для улучшения управления рисками, выявления изменений в контексте существующих рисков и выявления новых рисков.

Для обеспечения выявления надлежащих превентивных мер безопасности система управления рисками должна детализировать механизмы получения достоверной информации об угрозах и проведения оценок рисков с учетом международных, национальных и региональных ситуаций и условий. Меры и процедуры безопасности должны быть гибкими и соизмеримыми с оценкой риска, которая может колебаться в зависимости от различных изменяющихся факторов. Эта система должна быть внедрена своевременно и эффективно, чтобы итоговая оценка рисков всегда была актуальной, точной и полной.

На международном уровне ISO создала общепризнанную парадигму в этой области, выпустив стандарт ISO 31000. Это относится к семейству стандартов, которые ISO определяет как «набор компонентов, которые обеспечивают основы и организационные механизмы для разработки, внедрения и мониторинга, анализа и постоянного совершенствования управления рисками во всей организации»[19]. Важно отметить, что стандарт ISO 31000 не относится к какой-либо отрасли или сектору.

Изучение конкретной ситуации **15**
Методика оценки рисков авиационной безопасности ИКАО

Методика оценки рисков авиационной безопасности ИКАО была разработана для формирования понимания и относительного классификации текущего остаточного риска с целью информирования лиц, принимающих решения. Несмотря на то, что методология была разработана с учетом угроз против гражданской авиации, большинство ее элементов можно рассматривать как общеприменимые. Этот процесс оценки риска включает следующие элементы:

- выявление и анализ вероятных сценариев угроз, их вероятностей и последствий;
- оценка текущих мер по смягчению и оставшихся уязвимостей;
- оценка остаточного риска с учетом вероятности, последствий и уязвимости конкретного сценария угрозы; а также
- рекомендации для дальнейшей работы, основанной на риске, и возможные меры

Ключевые компоненты завершения оценки риска:

Сценарий угрозы: идентификация и описание заслуживающего доверия акта незаконного вмешательства, включающего цель (например, терминал аэропорта, связанную инфраструктуру или самолет или другие КВОИ), метод работы (включая перевозку и сокрытие) и методы атаки (такие как самодельное взрывное устройство) и злоумышленник (исходя из роли) и роли злоумышленника в авиационной системе - пассажир, провожающий и / или инсайдер). Это должно быть достаточно подробным, чтобы обеспечить точную оценку и анализ; «нападение на воздушное судно» не является достаточно хорошим сценарием, тогда как «пассажира, атакующего терминал аэропорта с использованием самодельного взрывного устройства (СВУ) в ручной клади», будет достаточно;

[19] ISO 31000:2009(en):www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en
Применяя тот же подход к управлению рисками, что и ISO 31000, серия ISO 27000 обеспечивает эталонный стандарт в области систем защиты информации. Таким образом, ISO 27000 предлагает полезную руководящую структуру для защиты критически важных информационных инфраструктур.

Вероятность атаки (угрозы): вероятность или возможность того, что атака (сценарий угрозы) предпринимается, исходя из намерений и возможностей террористов, но НЕ принимая во внимание текущие меры безопасности. Вероятность используется в качестве индикатора угрозы, учитывая как намерение, так и способность преступника реализовать сценарий угрозы;

Последствия: характер и масштаб последствий конкретного нападения в человеческом, экономическом, политическом и репутационном отношении при разумном наихудшем сценарии;

Текущие меры по смягчению: соответствующие практики стандартов и рекомендаций (которые могут не все присутствовать в Приложении 17 ИКАО и которые, как обычно предполагается, эффективно применяются там, где это явно не так, риск будет выше) или другие соответствующие национальные и / или местные программы и положения, направленные на снижение вероятности нападения стать успешным и / или уменьшить последствия, если атака должна произойти. Предполагается, что никакой угрозы нельзя полностью устранить.

Уязвимость: степень остающихся уязвимостей после того, как текущие смягчающие меры были приняты во внимание;

Риск: общий риск успешного нападения, который сохраняется при условии принятия текущих мер по смягчению последствий с учетом вероятности и последствий угрозы; а также

Возможные дополнительные меры по смягчению: определены меры, которые государства-члены или ИКАО могли бы принять для дальнейшего снижения остаточных рисков, где это необходимо.

Важно, чтобы при оценке риска были тщательно и достаточно подробно определены вероятные сценарии, конкретно и тщательно при рассмотрении каждой формы угрозы. Угрозы могут быть направлены на конкретные аэропорты, терминалы или другую инфраструктуру, такую как склады ГСМ, средства управления воздушным движением или навигационное оборудование, а также воздушные суда, включая различные виды авиации, такие как авиация общего назначения, пассажирские воздушные суда и грузовые воздушные суда. Средства и методы, с помощью которых может быть осуществлена угроза, также должны быть оценены. Это будет включать то, как оружие или взрывное устройство может быть сконструировано, каким образом оно может быть передано (например, перевозится ли оно человеком или транспортным средством) и кем (например, сотрудником, пассажиром или представителем общественности), как оно может быть скрыто, и как оно может быть активировано или использовано для совершения акта незаконного вмешательства. Однако это не охватывает полный список возможных сценариев, а государствам или другим организациям, проводящим оценку рисков, рекомендуется разрабатывать свои собственные версии, отражающие местные обстоятельства.

В некоторых странах, в частности в США и Канаде, созданы государственные программы, специально призванные стимулировать операторов КВОИ к принятию общей системы оценки. Эти программы также предназначены для оказания технической помощи в проведении оценок в соответствии с «мягким подходом», основанным на стимулах и добровольных планах.

Изучение конкретной ситуации **16**
Региональная программа оценки устойчивости Канады (RRAP)

RRAP - это комплексная программа оценки рисков для владельцев и операторов канадской критически важной инфраструктуры (КВОИ). Эта программа включает оценку площадок, чтобы помочь организациям оценить и улучшить свою устойчивость ко всем опасностям в Канаде, таким как киберугрозы, случайные или преднамеренные антропогенные события и природные катастрофы. Эти оценки на местах являются добровольными, не регламентирующими, бесплатными и конфиденциальными.

Для повышения устойчивости критически важных объектов инфраструктуры RRAP использует три основных инструмента:

- Инструмент обеспечения устойчивости критически важной инфраструктуры (CIRT): инструмент для обследования на объекте, который измеряет устойчивость и защитные меры объекта;

- Мультимедийный инструмент для критически важных объектов инфраструктуры (CIMT): мультиплатформенный программный инструмент, который генерирует интерактивное визуальное руководство по объекту критически важной инфраструктуры, показывая сферическую фотографию;

- Анализ киберустойчивости Канады (CCRR): инструмент для обследования на объекте, который измеряет уровень кибербезопасности в организации.

Программа может включать в себя семинары, встречи, геопространственные продукты и тематические интервью экспертов. Результаты оценок RRAP предназначены для того, чтобы помочь владельцам и операторам определить зависимости и уязвимости в своих организациях. Оценки на местах также определяют ряд необязательных экономически эффективных мер, чтобы помочь владельцам и операторам снизить риски и улучшить их способность реагировать и восстанавливаться после сбоев. В частности, RRAP предусматривает:

- Улучшенное управление рисками - повышает понимание организацией своих уязвимостей на основе использования надежных инструментов оценки.

- Укрепление связей с правительством. Укрепление отношений с несколькими правительственными ведомствами, включая службы реагирования.

- Повышение осведомленности о кибербезопасности - лучшее понимание, насколько хорошо организация подготовлена к кибератакам и другим киберугрозам.

Другие ключевые факторы для владельцев и операторов критически важных объектов инфраструктуры:

- Минимальные затраты времени и ресурсов - услуга RRAP быстрая и предоставляется бесплатно.

- Безопасность - Общественная безопасность Канады будет защищать конфиденциальность документов и информации, предоставленной на доверительной основе владельцами и операторами критически важных объектов инфраструктуры департаменту.
Источник: Общественная безопасность Канады, по адресу:
www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx.

2.6.2 Антикризисное управление

Антикризисное управление определяет процессы, которые необходимо активировать, когда угрозы все же материализуются. Этапы антикризисного управления включают в себя:

- выявление кризиса;
- планирование соответствующих ответных мер на кризис;
- противостояние и устранение кризиса.

Когда речь идет о терминологии, связанной с антикризисным регулированием, страны иногда называют «планы действий на случай внештатных ситуаций» и «планы действий на случай чрезвычайных ситуаций» синонимичными. Строго говоря, однако, планы действий в чрезвычайных ситуациях носят реактивный характер, в то время как планы действий во внештатных ситуациях более превентивный. В то время как планы действий в чрезвычайных ситуациях предназначены для ограничения последствий или воздействия инцидента, планы действий во внештатных ситуациях

предназначены для прогнозирования событий и подготовки всех заинтересованных сторон к чрезвычайной ситуации, а также для обеспечения скорейшего возвращения к нормальной работе.

Одному субъекту, назначенному государством, должна быть передана основная ответственность и полномочия для определения порядка действий, которые должны быть предприняты в случае возникновения кризиса. Этот субъект должен координировать все действия со всеми участвующими и затрагиваемыми субъектами. В рамках плана антикризисного управления должен быть разработан эффективный план реагирования на чрезвычайные ситуации, включая обеспечение взаимодействия систем связи и адекватного времени реагирования, а также планы эвакуации для ограничения воздействия. Реакция аварийно-спасательной бригады должна планироваться, тестироваться и оцениваться заранее, чтобы смягчить последствия атаки.

2.7 Обозначение угроз, последствий и уязвимостей

Разрабатывая свои стратегии ЗКВОИ вокруг подхода к управлению рисками, страны должны учитывать ряд руководящих принципов. Эти принципы выделены ниже.

2.7.1 Многоуровневое учение

Определение характера и уровней угроз для КВОИ и связанных с ними уязвимостей обязательно является совместным и согласованным продуктом оценок, проводимых на разных уровнях. Подобно увеличительным линзам, которые могут захватывать широкую картину и двигаться дальше, чтобы захватить мельчайшие детали, стратегия по ЗКВОИ должна быть в состоянии интегрировать многоуровневые оценки угроз, последствий и уязвимости. Схематически эти уровни представлены следующим образом: i) национальный уровень; ii) отраслевой уровень; iii) уровень инфраструктуры / компании.

i) Оценки на национальном уровне

Целью национальной оценки риска является получение обзора угрозы, с которой сталкиваются КВОИ страны в целом, ее уязвимости и последствия успешной атаки. Важным вкладом общенациональных оценок является то, что они показывают, как несколько секторов взаимодействуют друг с другом. При разработке документов такого типа на основе разведывательных данных, которые поддерживали разработку стратегий национальной безопасности и борьбы с терроризмом, могут быть предложены соответствующие рекомендации и выводы.

Изучение конкретной ситуации **17**
Национальная оценка риска Швеции

Согласно национальному законодательству, все государственные органы обязаны разработать и представить анализ рисков и уязвимости в Национальное агентство по чрезвычайным ситуациям (MSB). Основываясь на таких отчетах, с 2011 года MSB проводит национальные оценки рисков. Эти документы (последний из которых был выпущен в 2016 году) призваны обеспечить стратегическую основу для направления и дальнейшего развития гражданских непредвиденных обстоятельств.

Оценка 2016 года определяет пять областей развития, которые MSB считает особенно важными для повышения готовности к стихийным бедствиям (и, таким образом, имеют непосредственное отношение к ЗКВОИ):

- Усилия в области обеспечения готовности к стихийным бедствиям и гражданской обороны должны стать более приоритетными для ответственных заинтересованных сторон в Швеции;
- Необходимо повышать знания и осведомленность о ролях и обязанностях, связанных с подготовкой к стихийным бедствиям, в частности, когда речь идет об ответственности за географические районы;
- Анализ рисков и уязвимости, проводимый на местном, региональном и национальном уровнях, требует улучшений, чтобы их можно было использовать в качестве основы для планирования готовности к стихийным бедствиям и гражданской обороны;
- Сценарии, предоставленные MSB, могут стать вспомогательным инструментом для планирования и развития стихийных бедствий.
- Необходимо установить более четкие требования к защитным мерам для критически важных инфраструктур.

MSB подчеркивает необходимость дальнейшего развития возможностей в следующих областях:

- Способность реагировать на перебои с подачей электроэнергии;
- Способность предотвращать и реагировать на перебои с подачей питьевой воды;
- Область информации и кибербезопасности;
- Способность предотвращать и реагировать на перебои с поставками лекарств;
- Способность предотвращать и реагировать на радиологические и ядерные события.

Источник: Швеция 2016

ii) Отраслевая оценка

Очень важно разработать профили риска для конкретных секторов КВОИ. Эти профили имеют решающее значение для оценки существующих практик смягчения последствий, результатов и уязвимостей. В зависимости от рассматриваемого сектора оценки риска могут проводиться для конкретных подсекторов и впоследствии возвращаться в более широкие профили отраслевых рисков. Например, стратегия устойчивости критически важной инфраструктуры Австралии разбивает транспортный сектор на следующие подсекторы: авиация, наземные пассажирские перевозки (включая мосты и туннели), наземные перевозки и морские перевозки (судоходство и порты). В соответствии с той же стратегией энергетический сектор состоит из систем электроснабжения, морских нефтегазовых месторождений, наземных нефтегазовых и угольных поставок.

iii) Оценка на уровне инфраструктуры

Операторы КВОИ часто являются теми, кто лучше всех знает, как их объекты инфраструктуры функционируют с точки зрения систем и процессов. Следовательно, они имеют конкретное понимание своих внутренних факторов уязвимости. Кроме того, компании часто проводят циклы управления рисками независимо от институциональной роли, которую они призваны играть в ЗКВОИ. Корпорации в основном занимаются управлением рисками для минимизации ущерба, который может повлиять на цели компании с целью обеспечения непрерывности бизнеса или ограничения последствий угрозы. Не концентрируясь на ЗКВОИ, этот тип управления рисками направлен на выявление рисков для непрерывности производства и принятие мер по смягчению. В результате это может принести непосредственную пользу инфраструктурам компаний и повысить их устойчивость. Таким образом, странам следует внимательно рассмотреть роль, которую должны играть процессы управления рисками, управляемые компанией, в контексте стратегий ЗКВОИ, включая способы интеграции оценок на корпоративном уровне в процессы принятия решений ЗКВОИ.

2.7.2 Многосторонний процесс

Эффективная оценка рисков является результатом процесса консультаций, который опирается на точки зрения и выводы различных правительственных учреждений, аварийных служб и организаций частного сектора. В то время как обычно правительственные агентства играют ведущую роль в разработке национальных и отраслевых оценок угроз, а операторы КВОИ играют ведущую роль в планах, связанных с КВОИ, вклад и участие всех заинтересованных сторон во всех случаях желательны. Хотя участие широкого круга заинтересованных сторон может замедлить весь процесс, опыт стран показывает, что ценности инклюзивности (всеобщего охвата) и прозрачного принятия решений играют важную роль в достижении приемлемости. Это является ключевым предварительным условием, учитывая, что несколько участников несут ответственность за реализацию стратегий ЗКВОИ.

Всеобщий охват процесса также позволяет учитывать риски с разных точек зрения. Достигается совместное понимание взаимодействия различных инфраструктур и секторов. Однако обеспечение широкой коллективной природы процесса и его общей согласованности сопряжено с трудностями. В целом, разные заинтересованные стороны воспринимают риски по-разному. Как уже отмечалось, «критически важные партнеры по инфраструктуре управляют рисками на основе разнообразных обязательств перед сообществом, сосредоточения внимания на благосостоянии клиентов и структурах корпоративного управления. Допуски на риск будут варьироваться от организации к организации, а также от сектора к сектору, в зависимости от бизнес-планов, ресурсов, операционной структуры и нормативно-правовой среды. Они также различаются между частным сектором и правительством в зависимости от лежащих в их основе ограничений. Разные субъекты, вероятно, будут иметь разные приоритеты в отношении инвестиций в обеспечение безопасности, а также потенциально разные суждения относительно того, что может быть подходящим допуском риска» NIPP 2013, стр.5).

Важно не только признать наличие различных установок и подходов заинтересованных сторон, но и понять, как они могут повлиять на общий процесс установления совместных приоритетов. С этой точки зрения достижение «критически важные объекты инфраструктуры безопасности и устойчивости зависит от применения практики управления рисками как отрасли, так и правительства в сочетании с доступными ресурсами и стимулами для руководства и поддержки усилий» (NIPP 2013, с.15).

2.7.3 Обозначение террористических угроз в отношении КВОИ

По сравнению с оценками угроз по отношению к другим опасностям, выявление и оценка террористических угроз по КВОИ ставит конкретные вопросы. Часть проблем проистекает из высокой неопределенности, связанной с этим типом определения объема работ. Как уже отмечалось, «фундаментальная проблема в этом контексте заключается в том, что террористы адаптируют свое поведение к изменениям в ландшафте безопасности» (ИДКТК 2017). С этой точки зрения террористическую угрозу следует рассматривать как динамическую, приспосабливающуюся, например, к изменениям в ресурсах, доступных террористической группе, и к изменениям в функциях безопасности потенциальной цели.

С точки зрения источников, из которых можно извлечь элементы для оценки угроз, связанных с терроризмом, стратегии по ЗКВОИ должны признавать основную роль разведывательного сообщества. Спецслужбы отвечают за защиту национальной безопасности. При выполнении своих миссий они часто используют конфиденциальную информацию как средство защиты источников и методов, чтобы не предупреждать цели текущих мероприятий по слежению и т. д. Следовательно, стратегии по ЗКВОИ должны иметь механизмы для работы с информацией, распространение которой ограничено. Как показано в разделе 4.2, основная задача заключается в обеспечении того, чтобы как можно больше

информации распространялось среди всех заинтересованных сторон при защите ее конфиденциального характера. Это может быть как конфиденциальная деловая информация, которой владеют компании, так и секретная информация, хранящаяся в государственных органах.

Изучение конкретной ситуации **18**

Подход Австралии, основанный на разведывательных данных по защите КВОИ от террористических атак

Австралия опирается на сильный режим разведки, предотвращения и обеспечения готовности для поддержки контртеррористических мероприятий. Этот подход включает в себя целенаправленные меры по предотвращению и обеспечению готовности, основанные на принципах управления рисками и сохранении возможностей для управления различными видами террористических угроз, нападений и их последствий. Контртеррористическая разведка и уголовные расследования проводятся австралийской разведывательной организацией (ASIO) и правоохранительными органами. Быстрая и надлежащая передача информации о террористической угрозе владельцам / операторам КВОИ позволяет владельцам и операторам принимать более обоснованные решения по управлению рисками и принимать эффективные меры по снижению риска в ответ на среду угроз.

В частности, оценки угроз ASIO указывают на уровни угрозы и вероятного характера терроризма, политически мотивированного насилия, шпионажа, иностранного вмешательства, насильственного протеста и диверсии. Оценка угроз может быть произведена для конкретных событий, объектов, людей или секторов и отделена от национального уровня угрозы терроризма. ASIO распространяет оценки угроз среди соответствующих правительственных учреждений Австралии, правительств штатов и территорий, федеральной полиции Австралии и полиции штатов и территорий. Владельцам / операторам КВОИ также предоставляется копия оценки национальной угрозы терроризма, и ожидается, что она будет использоваться в процессе их подготовки и планирования. ASIO предоставляет консультации по угрозам частному сектору и правительственным учреждениям через отдел связи с бизнесом. В случае особой срочности ASIO свяжется с полицией штата и территории и другими соответствующими организациями, включая владельцев / операторов КВОИ, как можно скорее и до отправки письменного уведомления. Хотя оценки угроз ASIO учитывают намерения и возможности террористов, они не оценивают уязвимость или адекватность существующей безопасности КВОИ. Впоследствии, оценки угроз должны использоваться при анализе рисков безопасности, чтобы определить требования и тип мер по смягчению для любого объекта КВОИ.

Источник: Австралия-Новая Зеландия 2015

Стратегии по ЗКВОИ должны также учитывать, что оценка угроз, связанных с терроризмом, против КВОИ основывается на способности обрабатывать несколько наборов показателей, а также контекстуализировать имеющуюся информацию. Изменения в геополитических реалиях, экономической ситуации, динамике власти между преступными организациями и т. д. должны быть взвешены и стимулировать повторение учений через регулярные промежутки времени.

Одним из полезных индикаторов являются данные о предыдущих атаках или угрозах в отношении КВОИ, особенно если они неоднократно происходили с течением времени или последовательно нацеливались на определенные сектора или КВОИ в конкретных регионах. Оценки могут также извлечь пользу из данных, доступных из других стран, особенно когда можно провести аналогии. Например, если террористическая группа уже напала на ядерные объекты в стране X, а страна Y находится в союзе со страной X, можно предположить более высокий уровень угрозы ядерным объектам в стране Y.

Изучение конкретной ситуации **19**
Анализ угроз кибербезопасности Германии

В рамках своего анализа кибербезопасности федеральное управление информационной безопасности Германии (BSI) составило список наиболее критических угроз, с которыми в настоящее время сталкиваются промышленные системы управления (ICS). Угрозы классифицируются с учетом таких факторов, как группы преступников, распределение и простота использования уязвимостей, а также возможные технические и экономические последствия атаки. Для получения информации анализируются базы данных фактических событий. **Источник:** ОБСЕ 2013, с.35.

Радиолокаторы также должны быть в состоянии обнаружить признаки "низкой интенсивности" потенциальных текущих террористических планов. Зарегистрированные акты нарушений в отношении КВОИ, такие как простое проникновение, могут указывать на интерес террористов к тому, как структурируется КВОИ, или попытки осуществлять тщательное наблюдение за определенными местами. В то же время зачастую невозможно сделать выводы на основе единичных и спорадических действий. Здесь опять-таки, спецслужбы играют ключевую роль в выявлении закономерностей событий, которые кажутся незначительными, если рассматривать их изолированно.

Хотя ожидается, что стратегии по ЗКВОИ не будут содержать полных списков индикаторов и источников, они должны быть составлены таким образом, чтобы наделять правами (или уполномочивать, в зависимости от выбранных моделей управления ЗКВОИ) соответствующие органы власти для формирования процесса оценки риска специфически изменчивого и нестабильного характера террористической угрозы.

2.8 Минимизация уязвимости КВОИ для террористических атак

В предыдущих разделах подчеркивалась важность комплексного процесса управления рисками и проведения оценки рисков на разных уровнях в качестве условия минимизации уязвимости КВОИ для террористических атак. Управление рисками должно в конечном итоге привести к конкретным превентивным планам и мерам. В этом разделе рассматривается место профилактических мер в контексте стратегий по КВОИ с точки зрения физической, кадровой и киберзащиты.

При рассмотрении таких мер странам всегда рекомендуется изучать степень их потенциального воздействия на соблюдение прав человека (например, влияние на свободу передвижения, создаваемое ограничениями безопасности на местах, вмешательство в частную жизнь, вызванное технологиями видеонаблюдения и т. д.). Во всех таких случаях цель защиты КВОИ от террористических актов должна быть сбалансирована с необходимостью соблюдения основных прав человека, закрепленных в международных договорах, таких как международный пакт о гражданских и политических правах. При этом должны быть сохранены только те меры, которые считаются необходимыми для достижения ЗКВОИ. Запланированные меры также должны оцениваться с точки зрения их соразмерности поставленным целям.

2.8.1 Предотвращение

Предотвращение террористических нападений на КВОИ является частью общенациональной задачи противодействия угрозам и нарушениям планов, заговоров и других приготовлений к совершению террористических актов в целом. В конечном итоге защита КВОИ зависит от скоординированных действий разведывательных служб, правоохранительных органов в целом и т. д. Степень, в которой

уголовные законы используют превентивный подход, а также способность следственных органов проявлять инициативу (в отличие от простого реагирования на совершение террористических актов) играют основополагающую роль в профилактических усилиях. Стратегии по ЗКВОИ должны опираться на существующие рамки, концентрируясь на тех политиках и мерах, которые имеют непосредственное отношение к активизации деятельности по предотвращению террористических атак, направленных конкретно против КВОИ. Они могут, в частности:

- Определять основные роли и обязанности в области профилактики, в том числе на уровне операторов КВОИ (т. е. общую роль руководителей высшего звена, сотрудников службы безопасности и, в более общем плане, установить концепцию, согласно которой реализация профилактических мер является задачей для всей компании и требует поддержки на всех уровнях);

- Описать рабочую площадку и методик для разработки пособий и практических руководств для использования операторами КВОИ в области профилактики;

- Непосредственно определить методы и подходы, которые должны широко применяться или рассматриваться заинтересованными сторонами. Например, страны все чаще пропагандируют «концептуальную безопасность» как инструмент для достижения превентивных целей. Другим примером является требование к владельцам / операторам КВОИ поддерживать эффективные меры безопасности, чтобы максимизировать вероятность того, что подготовительная деятельность для террористов, такая как разведка на месте, будет быстро выявлена. Например, в рамках своей стратегии по ЗКВОИ правительство Австралии требует, чтобы о любых таких подозрительных действиях сообщалось в полицию, и создало специальную горячую линию национальной безопасности;

- Поощрять или поручать (в зависимости от выбранной модели управления) принятие конкретных наборов превентивных мер операторами КВОИ, как межсекторальные, так и по конкретным отраслям.

Изучение конкретной ситуации **20**
Изначально предусмотренная безопасность

Все больше стран включают концепции обеспечения безопасности в свои стратегии, направленные на повышение устойчивости КВОИ к террористическим атакам и другим опасностям. Безопасность по замыслу направлена на предотвращение с точки зрения долгосрочной перспективы. По данным британского центра защиты национальных объектов инфраструктуры, «рассмотрение требований физической безопасности с самого начала, как части проекта здания или объекта, часто приводит к более эффективной и более дешевой безопасности. Для новых зданий требования безопасности высокого уровня должны быть включены в первоначальное резюме. Требования физической безопасности также должны учитываться на этапе строительства новых зданий или модификации существующих объектов, так как они, вероятно, будут подвержены различным рискам и проблемам.

Внимание нужно уделить:

- Выявлению и оценке существующих и новых угроз безопасности

- Определению требований безопасности как для строительных работ, так и для любых изменений в безопасности самого объекта (это будет зависеть от того, находятся ли строительные работы рядом или внутри объекта).
- Определение перехода мер безопасности из «фазы строительства» в обычную эксплуатацию.

Концепция изначально предусмотренной безопасности может применяться не только к физическим активам, но и к КИИ. Стратегия кибербезопасности Сингапура на 2016 год специально ставит перед

собой цель упреждения кибер-уязвимостей, «переходя на более высокий уровень и продвигая методы обеспечения изначально предусмотренной безопасности. Кибербезопасность больше не будет второстепенным вопросом, а будет сознательно реализовываться на протяжении всего жизненного цикла технологических систем. Соответственно, Правительство обязалось принять следующие шаги:

- Постепенно институционализировать изначально предусмотренную безопасность в структуру управления по защите КИИ;
- Содействовать практике тестирования на проникновение для выявления уязвимостей на ранних этапах исправления на этапе проектирования;
- Создать сильное сообщество заинтересованных сторон по тестированию продуктов и систем на основе установленных международных стандартов, таких как сертификация обеспечения качества продуктов по общим критериям;
- Продолжать совершенствовать методологии и разрабатывать новые инструменты проверки безопасности для повышения эффективности изначально предусмотренной безопасности.

2.8.2 Процессы, физическая безопасность (включая технологии), безопасность персонала и меры кибербезопасности

Стратегии по ЗКВОИ и связанные с ними действия по реализации должны основываться на идее, что эффективные меры защиты на уровне КВОИ требуют интеграции элементов физической, кадровой и кибербезопасности. В таблице [число] приводится перечень практически ориентированных инструментов, разработанных рядом правительств с целью предоставления руководящих указаний операторам КВОИ. Хотя эти инструменты имеют национальную направленность, большинство содержащихся в них руководств применимо к международным границам и может стать источником вдохновения для органов власти и операторов КВОИ из других стран.

i) Процессы

Стратегии по ЗКВОИ должны отражать нормативные требования для профилактики безопасности в отношении КВОИ и должны быть направлены на установление целевых показателей эффективности, которые должны быть достигнуты, с помощью профилактических мер, а не описанием специальных процедур или мер. Должна быть создана комплексная организационно-правовая структура с четко определенными обязанностями и методами реализации. Стратегии должны включать политику, лежащую в основе правил, практик и процедур, применяемых к «нормальным» условиям работы, и дополнительные меры, необходимые в случае повышения уровня угрозы.

ii) Меры физической безопасности (в том числе технологии)

Это эффективно достигается за счет реализации так называемой концепции «глубокоэшелонированной защиты», в соответствии с которой защита требует многоуровневых различных мер. Основной принцип заключается в том, что безопасность инфраструктуры существенно не ухудшается при потере какого-либо одного слоя.

Для обнаружения любого несанкционированного доступа и обеспечения возможности задержания любых злоумышленников, прежде чем они смогут добраться до основных объектов, многоуровневый подход может включать в себя следующее:

- разграничение границ зоны и защиты КВОИ физическими барьерами;
- патрулирование и достаточное видеонаблюдение;
- контроль доступа с дополнительными функциями безопасности, используемыми для повышения его функционирования или эффективности (например, покрытие колючей проволокой, система обнаружения вторжения по периметру, освещение или система замкнутого телевидения; использование таких технологий, как методы и / или техники проверки (например, обнаружение взрывчатых веществ собаками, ручной поиск, ручные

металлоискатели, обнаружение следов взрывчатых веществ и мобильные поисковые устройства).

Меры физической безопасности должны поддерживаться должным образом обученным персоналом, продуманным и всесторонним планированием на случай непредвиденных обстоятельств и краткими, хорошо написанными планами и приказами по безопасности.

Изучение конкретной ситуации **21**
Национальный центр Великобритании по защите национальных объектов инфраструктуры

Центр приводит следующие примеры мер физической безопасности:

- Меры по оказанию помощи в обнаружении оружия, представляющего угрозу, в том числе, например, взрывчатых веществ, ножей, огнестрельного оружия, химических / биологических / радиологических материалов и т. д.;
- Меры по оказанию помощи в обнаружении, отслеживании и мониторинге злоумышленников и других угроз, таких как беспилотные летательные аппараты;
- Системы контроля доступа и блокировки;
- Физические и активные барьеры, препятствующие или задерживающие продвижение злоумышленников;
- Меры по защите людей или имущества от воздействия взрыва или баллистической атаки;
- Меры по защите или ограничению распространения химических, биологических или радиологических материалов;
- Меры по защите засекреченных (например, конфиденциальных) материалов или активов.

Источник: Национальный центр по защите национальных объектов инфраструктуры, по адресу: www.cpni.gov.uk

iii) Безопасность персонала

Под безопасностью персонала понимаются политика и процедуры, необходимые для снижения риска, связанного с внутренними угрозами (например, сотрудников компании), использующими их законный доступ к помещениям, системам или процессам инфраструктуры для осуществления несанкционированных / злонамеренных действий. Эффективная безопасность персонала включает в себя различные меры, начиная от проверок биографических данных, процедур отбора, тренинга по повышению осведомленности в вопросах безопасности, повышая бдительность и общую культуру безопасности, обучения персонала, систем охраны периметра и контроля доступа, видеонаблюдения и контроля качества.

Таблица 5: Практические инструменты для операторов КВОИ

Название/тема и страна	Описание
Защита критически важных объектов инфраструктуры - базовая концепция защиты, рекомендации для компаний Германия, федеральное министерство внутренних дел	Этот инструмент был разработан Федеральным министерством внутренних дел, Федеральным управлением гражданской защиты и реагирования на стихийные бедствия и Федеральным управлением уголовной полиции. Деловое сообщество предоставило свой опыт с самого начала. Концепция базовой защиты предоставляет компаниям в Германии рекомендации с точки зрения внутренней безопасности. Имеется вопросник и контрольный список. https://www.preventionweb.net/files/9266_2967ProtectionofCriticalInfrastruct.pdf
Безопасность персонала и людей **Физическая охрана**	Советы, инструментарий и руководства CPNI касаются следующих тем и подтем: **Безопасность персонала и людей** (Снижение риска появления

Великобритания, Центр по защите национальных объектов инфраструктуры (CPNI)	инсайдеров; оптимизация безопасности людей; разрушение вражеской разведки) Физическая безопасность (поиск и проверка с целью ослабления конкретных угроз; физические средства защиты; контроль доступа и блокировки; обнаружение и мониторинг злоумышленников; задержка активного доступа; строительные конструкции; окна и фасады; двери; служебные помещения и пространства; комнаты управления; конфиденциальная информация и активы) https://www.cpni.gov.uk/advice
Кибер-стратегия **ИТ-инфраструктура** **Устройство конечного пользователя** **Операционная технология** Великобритания, Национальный центр кибербезопасности www.ncsc.gov.uk/guidance	Доступное руководство организовано по темам в следующих категориях и подкатегориях: **Кибер-стратегия** (Гибкая работа - Управление инцидентами - Оперативная безопасность - Безопасность персонала - Физическая безопасность - Управление рисками - Навыки и обучение - Социально-техническая безопасность) **ИТ-инфраструктура** (Криптография - Передача данных - Проектирование и настройка - Уничтожение и утилизация - Защита от вредоносных программ - Мониторинг - Безопасность сети - Безопасное хранение - Технология конечного пользователя - BYOD) **Устройство конечного пользователя** (Идентификационные данные и пароли - Безопасные коммуникации - Цифровые услуги - Гражданские услуги - Облачная безопасность - Предложения SaaS (облачная услуга по программному обеспечению) - Мониторинг транзакций) **Операционные технологии** (Киберугрозы - Кибератаки - Уязвимости)
Инструментарий для защиты и устойчивости критически важной инфраструктуры США, Министерство национальной безопасности	Инструментарий призван стать отправной точкой для малого и среднего бизнеса для интеграции защиты инфраструктуры и ее устойчивости в готовность, управление рисками, непрерывность бизнеса, управление в чрезвычайных ситуациях, безопасность и другие, связанные с этим проблемы. Для дополнительной информации: IP_Education@hq.dhs.gov.

iv) Кибербезопасность

Меры кибербезопасности представляют собой третью группу мер, для разработки которых стратегии по ЗКВОИ должны установить адекватную основу. Это включает в себя комплекс мер, предназначенных для защиты КВОИ от кибератак. Являясь не только технологическими по своей природе, они помогают сохранить целостность, устойчивость и нормальное функционирование КВОИ. Они могут, например, включать процедуры безопасности, политики, организационные меры, осведомленность и обучение, конкретные руководящие принципы и процессы разработки или регулярные оценки безопасности.

Изучение конкретной ситуации **22**
Руководство Швеции по повышению безопасности в промышленных информационных и управляющих системах

Агентство по чрезвычайным ситуациям в Швеции разработало 17 основных рекомендаций на основе руководств, практик и методов работы, признанных на международном уровне. Некоторые рекомендации носят технический характер, а другие делают упор на методологию.

1. Обеспечить обязательство и ответственность руководства за безопасность в промышленных информационных и управляющих системах.
2. Уточнить роли и обязанности по обеспечению безопасности в промышленных информационных и управляющих системах.
3. Поддерживать процессы для системных обследований и управления рисками в промышленных информационных и управляющих системах.
4. Обеспечить систематическое управление изменениями в промышленных информационных и управляющих системах.
5. Обеспечить систематическое планирование действий в чрезвычайных ситуациях и управление инцидентами в промышленных информационных и управляющих системах.
6. Внедрить требования безопасности в промышленных информационных и управляющих системах с самого начала при планировании и закупках.
7. Создать хорошую культуру безопасности и повысить осведомленность о необходимости обеспечения безопасности в промышленных информационных и управляющих системах.
8. Работать с архитектурой безопасности в промышленных информационных и управляющих системах.
9. Непрерывный мониторинг подключений и систем с целью обнаружения попыток вторжения в промышленные информационные и управляющие системы.
10. Проводить регулярный анализ рисков промышленных информационных и управляющих систем.
11. Проводить периодические технические проверки безопасности промышленных информационных и управляющих систем.
12. Постоянно оценивать физическую безопасность промышленных информационных и управляющих систем.
13. Регулярно проверять надежность и актуальность всех без исключения подключений к промышленным информационным и управляющим системам.
14. Укрепление и модернизация промышленных информационных и управляющих систем в сотрудничестве с поставщиками систем.
15. Проводить обучение и практику по вопросам ИТ-инцидентов в промышленных информационных и управляющих системах.
16. Отслеживать инциденты в промышленных информационных и управляющих системах и отслеживать внешние проблемы безопасности.
17. Участвовать в ассоциациях пользователей, органах стандартизации и других сетях по безопасности в промышленных информационных и управляющих системах.

Полный текст руководства (https://www.msb.se/RibData/Filer/pdf/27473.pdf) содержит пояснения по каждой рекомендации, текст дополнительных рекомендаций и примеры рисков и проблем, которые могут возникнуть.

Источник: Швеция 2014

2.9. Реагирование и восстановление после террористической атаки на КВОИ

Раздел 2.6 ввел понятие «антикризисное управление» по отношению к КВОИ. В контексте борьбы с терроризмом «реагирование» относится к действиям, предпринятым в ходе и сразу после совершения террористического акта или угрозы совершения террористического акта. Ответные действия обычно направлены на: предотвращение или минимизацию последствий атаки, таких как гибель людей, травмы, повреждение имущества и ущерб или нарушение инфраструктуры; проведение уголовных расследований; оказание немедленной помощи и поддержки пострадавшему населению.

По сравнению с реагированием «восстановление» обычно определяет действия, которые в долгосрочной перспективе необходимы для поддержки усилий по восстановлению, включая физическую инфраструктуру и восстановление статус-кво с точки зрения физического, социального и

экономического благосостояния сообществ. Расширенное психологические воздействие террористических актов за пределами конкретного места инцидента позволяют предположить, что в некоторых случаях восстановление можно понимать, как процесс, требующий комплексного и устойчивого сотрудничества между правительственными учреждениями, частным сектором и организациями гражданского общества.

Стратегии по ЗКВОИ должны учитывать, как существующие структуры антикризисного управления должны быть интегрированы в их компетенцию, и какие изменения в общей системе, если таковые имеются, необходимо сделать, чтобы лучше соответствовать кризису, особенно влияющему на КВОИ. Необходимо создать четкие правовые и операционные рамки, совместимые с правами человека, отметив, что антикризисное управление важно не только в случае особо разрушительных террористических атак, но и в случае незначительных инцидентов, чтобы избежать или уменьшить последствия эскалации кризиса.

Определение подходящей основы антикризисного управления требует рассмотрения двух основных вопросов. Первый из них заключается в том, будет ли управление в чрезвычайных ситуациях основываться на подходе, основанном на всех опасностях, или на конкретных рисках. Новая Зеландия предлагает пример последнее (см. Изучение конкретной ситуации ниже). Оба подхода имеют свои преимущества и недостатки. Когда структуры антикризисного управления созданы для конкретных типов угроз, могут быть созданы индивидуальные процессы. Тем не менее, выбор подхода, специфичного для опасности, может оказаться проблематичным, когда характер инцидента неясен, поскольку это может вызвать неопределенность в отношении применимых рамок для вмешательства.

Второй вопрос, который следует рассмотреть, должен ли охват структур и процедур антикризисного управления КВОИ быть отраслевым или межсекторальным. Если выбран первый подход, правовая основа часто принимается министерством, ответственным за рассматриваемый сектор, или регулятором сектора. Вместо этого межотраслевой подход часто видит принятие общего законодательства.

Нормативные рамки КВОИ для особой отрасли часто встречаются в секторе телекоммуникаций. Например, в Нидерландах национальный телекоммуникационный форум по вопросам стабильности (NCO-T) стремится обеспечить, чтобы оператор мог использовать критически важные телекоммуникационные услуги в условиях исключительных обстоятельств. Участниками NCO-T являются назначенные операторы и генеральный директорат по энергетике, телекоммуникациям и рынкам министерства экономики. Во Франции план PIRANET запускается премьер-министром в конкретном случае крупного кризиса в сфере ИКТ.

Другие сектора КВОИ могут устанавливать эквивалентные механизмы, основанные на правовых рамках, принятых регулирующими органами по конкретным секторам. Например, после атак 11 сентября 2001 года «Нью-Йоркская фондовая биржа - постоянная потенциальная цель террористических атак - смогла продолжить свои торговые операции, так как уже создала альтернативную торговую площадку за пределами Нью-Йорка, как и другие финансовые учреждения с тех пор, чтобы копировать свои бизнес-операции за пределами своих муниципальных зон в случае катастроф, вызванных терроризмом» (Синай, 2016).

Примером межотраслевых нормативных рамок является эстонский закон о кризисах, глава IV которого посвящена «Организации непрерывной работы служб жизнеобеспечения». Закон устанавливает роли и обязанности министерств, местных и национальных агентств по урегулированию кризисов, а также операторов КВОИ, чтобы гарантировать продолжение оказания 41 критически важной услуги.

Изучение конкретной ситуации **23**
Структура управления кризисными ситуациями в Новой Зеландии

В Новой Зеландии основным документом, в котором излагается комплексная структура управления, основанная на всех опасностях, для управления потенциальными, развивающимися или фактическими

кризисами (включая, помимо прочего, те, которые влияют на КВОИ), является справочник по системе национальной безопасности. Критерии запуска системы национальной безопасности делятся на две широкие категории. Они относятся либо к характеристикам рисков, либо к способам управления ими.

Характеристики риска

- Необычные особенности масштаба, характера, интенсивности или возможных последствий;
- Вызовы суверенитету или общенациональному правопорядку;
- Множественные или взаимосвязанные проблемы, которые в совокупности представляют собой национальный или системный риск;
- Высокая степень неопределенности или сложности, когда только центральное правительство может справиться с ними;
- Взаимозависимые проблемы с потенциалом для каскадных эффектов или эскалации.

Требования к управлению

- Требования по реагированию необычно требовательны к ресурсам;
- Существует двусмысленность в отношении того, кто играет ведущую роль в управлении риском, или существуют противоречивые взгляды на решения;
- Первоначальное реагирование неуместно или недостаточно с национальной точки зрения;
- Существуют межведомственные сложности;
- У правительства есть возможность внести свой вклад в создание условий, которые повысят общую безопасность страны.

Для любого риска национальной безопасности (или основного элемента такого риска) определяется ведущее агентство. Эти агентства уполномочены (либо прямо через законодательство, либо из-за своего особого опыта) управлять чрезвычайной ситуацией, возникающей из списка конкретных опасностей.

Антикризисное управление в Новой Зеландии использует функции нескольких различных органов, включая:

Дежурные группы

Они призваны обеспечить ситуационную ясность в том, что часто является хаотичной средой, и несут ответственность за обеспечение наличия систем, обеспечивающих эффективное управление сложными проблемами. Дежурные группы обычно состоят из высокопоставленных чиновников, способных выделять ресурсы и согласовывать действия от имени своей организации. Точный состав групп наблюдения зависит от характера мероприятия и включает агентства, которые должны сыграть свою роль в реагировании на данную проблему. Иногда это могут быть агентства, которые обычно не считают себя агентствами «национальной безопасности» и не имеют большого опыта работы в структурах системы национальной безопасности.

Комитет должностных лиц по координации внутренней и внешней безопасности (ODESC)

Обеспечивает стратегическое руководство, поддерживает ведущее агентство и связывает с политическим уровнем, включая консультирование комитета национальной безопасности кабинета министров.

Рабочие группы или группы специалистов

Они формируются, когда желательно, чтобы профессия или специализация определяли и представляли консолидированный взгляд или конкретный совет дежурной группе или ODESC. (примеры: правительственная правовая сеть, экономическая консультативная группа, научная сеть и спецслужбы).

Национальный центр антикризисного управления

Обеспечивает безопасный, централизованный объект для различных координирующих задач, таких как управление операциями реагирования, планирование и поддержка; сбор, управление и обмен информацией; связь между оперативным реагированием и национальным стратегическим реагированием;

«Дежурная команда»

«*Дежурная* команда» включает в себя строгий анализ и проверку плана, идей или предположений, чтобы повысить обоснованность и качество окончательного плана. Многоучрежденческие «*дежурные* команды» могут создаваться на всех этапах кризиса (и, действительно, в проекте) и могут действовать параллельно с реагированием. В рамках национального кризиса «красная команда» помогает по-новому взглянуть на подход, используемый для управления угрозой.

Источник: Департамент премьер-министра и кабинета министров Новой Зеландии по адресу: www.dpmc.govt.nz/our-programmes/national-security-and-intelligence/national-security

После определения основных структур и процессов антикризисного управления стратегии по ЗКВОИ должны обеспечить бесперебойную работу в случае необходимости. Основные предпосылки для достижения гибкого и быстрого принятия решений рассматриваются в главе 5 (Обеспечение координации между национальными учреждениями). В той же главе также рассматриваются совместные государственно-частные учения как ключевые инструменты кризисного управления.

Еще одно соображение заключается в том, что в случае нападения на химический, биологический, радиологический или ядерный объект потребуется специальное реагирование для защиты населения и аварийно-спасательных групп, осуществляющих первые меры реагирования, от загрязнения и уменьшения потенциального выброса опасных материалов. Специализированное реагирование повлечет за собой конкретное планирование действий в чрезвычайных ситуациях и на случай непредвиденных обстоятельств, а также специальное оборудование для обнаружения, личной защиты и дезактивации.

2.10 Обеспечение актуальности и устойчивости стратегий

Стратегии по ЗКВОИ должны заложить основу для их практической реализации путем: i) обеспечения финансовой жизнеспособности общих усилий по ЗКВОИ; ii) создания механизмов анализа и мониторинга как части процессов управления рисками для существующих списков КВОИ и самих стратегий.

2.10.1 Финансовая устойчивость

В то время как операторы КВОИ несут основную ответственность за обеспечение устойчивости своих критически важных активов и процессов, усиление мер физической защиты и защиты ИТ часто требует выделения значительных ресурсов. Достижение устойчивости КВОИ может быть дорогостоящим делом. В этом контексте стратегии по ЗКВОИ должны обеспечивать финансовую устойчивость инвестиций в направлении достижения оптимального уровня КВОИ. На практике странам необходимо найти баланс с точки зрения соглашений о распределении затрат между владельцами / операторами КВОИ, правительственными учреждениями и поставщиками страховых услуг.

Важным инструментом для стимулирования участия бизнеса является создание стимулов. Они варьируются от нормативно-правового регулирования до субсидий, налоговых льгот и займов.

Стимулы становятся тем более важными в периоды экономического кризиса, когда операторы могут естественным образом склоняться к расходованию ресурсов на краткосрочные цели роста, а не на цели долгосрочной защиты.

Изучение конкретной ситуации **24**
Стимулы и механизмы финансирования для обеспечения устойчивости КВОИ в Швеции, Японии и США.

Швеция:

В шведской стратегии по ЗКВОИ признается, что для ее реализации требуется повышенная потребность в ресурсах, как людских, так и финансовых. В соответствии с Указом о готовности к чрезвычайным ситуациям 2006 года и усиленным оповещением власти могут подать заявку на получение средств из распределения средств по обеспечению готовности к чрезвычайным ситуациям. Другие организации могут получить косвенную выгоду от этого механизма финансирования путем сотрудничества в проектах с властями, указанными в указе.

Источник: План действий по защите жизненно важных социальных функций и критически важных объектов инфраструктуры, 2014, по адресу: www.msb.se/RibData/Filer/pdf/27412.pdf

Япония:

Япония наращивает усилия, чтобы убедить бизнес в том, что частные действия, направленные на укрепление кибербезопасности, должны рассматриваться не как затраты, а как инвестиции в продвижение продуктов и услуг компаний, а также в повышение конкурентоспособности. В этом контексте правительство создает механизм вознаграждения компаний (посредством финансовых выгод), которые отдают приоритет кибер-проблемам. Кроме того, оно спонсирует программы для поощрения профессионального развития сотрудников в навыках по промышленной кибербезопасности.

Источник: Arie H.2017

США:

В рамках задачи NIPP по обеспечению безопасности и устойчивости министерство национальной безопасности - в сотрудничестве с национальным институтом безопасности родного города (NIHS) - финансирует инновационные идеи, которые могут предоставить технологии и инструменты для сообщества критически важных объектов инфраструктуры. Проекты, финансируемые в рамках «NIPP Challenge», предназначены не только для получения ощутимых, краткосрочных результатов, чтобы их можно было быстро разрабатывать и реализовывать, но также для обеспечения финансовой, практической и логистической устойчивости в долгосрочной перспективе, с тем чтобы они могли повысить безопасность и устойчивость критически важных объектов инфраструктуры в нескольких секторах на долгие годы. Проекты оцениваются независимой комиссией NIHS в соответствии с рядом критериев, которые также принимают во внимание их жизнестойкость и ожидаемое воздействие.

Источник: Министерство национальной безопасности, по адресу: www.dhs.gov/nipp-challenge

Финансовая устойчивость стратегий по ЗКВОИ также основывается на разработке эффективных механизмов страхования, особенно в случае действий по «восстановлению», необходимых для восстановления серьезно поврежденных активов и восстановления прерванных услуг. Обсуждение схем страхования для КВОИ началось только после событий 11 сентября 2001 года. До этого риск терроризма обычно включался в стандартные страховые полисы без уплаты каких-либо более высоких премий. После событий 11 сентября 2001 года и других чрезвычайно разрушительных террористических атак, например, произошедших в Мадриде 11 марта 2004 года, восприятие радикально изменилось из-за беспрецедентных сумм компенсации, которые пришлось выплачивать страховой отрасли. Как уже отмечалось, «анализ терроризма как части проблемы по защите критически важных объектов инфраструктуры» показывает, что терроризм в настоящее время является признанным источником острых рисков, тех, которые наиболее близки к внешнему пределу страхования» (Мишель-Керджан, 2018 г., стр. 12). Поскольку чистая зависимость от рыночных механизмов была неудовлетворительной, правительства должны были определить характер и степень своего финансового участия в действиях по восстановлению КВОИ. В настоящее время «создание и внедрение адекватного финансового покрытия для таких мероприятий все больше и больше становится предметом рассмотрения на национальном уровне, выходящим далеко за рамки одной только страховой отрасли» (Мишель Кержан 2018, стр.12).

Изучение конкретной ситуации **25**

Схемы страхования устойчивости КВОИ от террористических актов во Франции, Испании, США и Великобритании

Франция:

Действуя с 2002 года, Управление по страхованию и перестрахованию рисков нападений и террористических актов («Gestion de l'Assurance et de la Réassurance des Risques d'Attentats et Actes de Terrorisme», GAREAT) является некоммерческой структурой, состоящей из страховых компаний. GAREAT управляет перестрахованием рисков "атак" и террористических актов, которые наносят ущерб Франции (независимо от страны, в которой совершается террористический акт). GAREAT состоит из двух разделов: раздел «Большие риски», который включает риски, страховые суммы которых составляют 20 миллионов евро и более, и раздел «Малые и средние риски», который управляет рисками со страховыми суммами ниже 20 миллионов евро. GAREAT полагается на принцип «взаимности», при котором все участники несут солидарную ответственность с остальными в одном разделе. Государство обеспечивает неограниченное покрытие программы GAREAT через Caisse Centrale de Réassurance (центральная сберкасса перестрахования).

Источник: GAREAT, www.gareat.com

Испания

«Consortio de Compensacion de Seguros» компенсирует ущерб людям и имуществу, вызванный «чрезвычайными рисками». Чтобы получить право на компенсацию от Консорциума, необходимо подписать страховой полис в определенных специальных филиалах. Специальное возмещение Консорциума является автоматическим, если ущерб является результатом террористического акта. Консорциум является общественной организацией при министерстве экономики, промышленности и конкурентоспособности.

Источник: Министерство экономики, промышленности и конкурентоспособности, по адресу: www.consorseguros.es/web/inicio

США

В США система вращается вокруг соглашения о распределении рисков между федеральным правительством, страхователем и страховщиком. В соответствии с Законом о страховании от террористических рисков 2002 года (TRIA) страховщики обязаны предлагать страхование от терроризма своим клиентам (хотя они вправе устанавливать цену страхового покрытия). В свою очередь, клиенты не обязаны брать страховое покрытие. Крайне важно, что согласно TRIA, атака должна быть засвидетельствована как «террористический акт» министром финансов. Определение требует, чтобы атака была совершена иностранными силами.

Великобритания

В Великобритании система представляет собой государственно-частное партнерство под названием «Pool Re». Большинство страховщиков, предоставляющих страхование коммерческой недвижимости и страхование от возможных убытков в Великобритании, являются членами «Pool Re» и согласны предложить своим клиентам защиту от терроризма. Предполагается, что любой страхователь, который получил такое покрытие и понесет убытки в результате ущерба от террористического акта, должен связаться со своим страховщиком, который организует рассмотрение претензии в соответствии с обычными процедурами. «Pool Re» имеет договоренности со всеми своими членами о возмещении им стоимости претензий, которые они платят в рамках предоставляемого ими покрытия терроризма. С этой целью страховщики платят премию «Pool Re». Правительство обязуется поддерживать «Pool Re», если когда-либо у него будет недостаточно средств для оплаты законных требований.

Источник: «Pool Re», www.poolre.co.uk/

2.10.2 Механизмы анализа и мониторинга

Экономика динамична. Объекты инфраструктуры, которые использовались для предоставления критически важных услуг обществу и экономике, могут быть по какой-либо причине закрыты или настроены на выполнение функций, которые больше не считаются критически важными. Например, угледобывающие шахты могут уступить место различным типам источников энергии. Кроме того, проще говоря, некоторые активы могут больше не выполнять функции, для которых они предназначены, поскольку они устаревают, или по другим экономическим причинам они стали нерентабельными.

Более того, характер и интенсивность угроз для КВОИ могут измениться. Результаты даже точных оценок риска, проведенных в определенный момент времени, могут более не соответствовать реалиям. Некоторые террористические группы могут просто представлять меньшую угрозу в определенных географических районах, продолжая оказывать давление в других местах. Например, в конце 2017 года ИГИЛ утратило контроль над примерно 95% территории, которую оно контролировало в 2014 году. КВОИ, расположенные на этих территориях, вероятно, больше не подвержены такому же типу и интенсивности угрозы со стороны ИГИЛ, хотя опасность может исходить от новых групп / игроков. В других случаях угроза могла измениться не так сильно, как уязвимость определенных объектов инфраструктуры, например, из-за устаревания или отсутствия обслуживания.

Учитывая все это, стратегии по ЗКВОИ должны предусматривать механизмы, направленные на регулярные промежутки времени:

- Обновить то, что часто является обширными «списками» национальных КВОИ;
- Переоценить риски;
- Пересмотреть стратегический документ, лежащий в основе ЗКВОИ, для улучшения управления рисками, выявления изменений в контексте существующих рисков и выявления новых рисков.

При выполнении трех вышеупомянутых функций правительственные учреждения должны, естественно, привлекать операторов КВОИ, следуя той же логике государственно-частного партнерства, которая была подчеркнута в предыдущих разделах.

Изучение конкретной ситуации **26**
Обновление Испанией «каталога» КВОИ

В соответствии с Королевским указом 704/2011, в котором содержатся положения о защите критически важных объектов инфраструктур, «в случае значительных изменений, затрагивающих инфраструктуры, перечисленные [в Национальном каталоге], когда эти изменения актуальны для целей, предусмотренных в настоящих правилах, компетентные операторы будут предоставлять, с помощью средств, предоставленных им в распоряжение министерством внутренних дел, новую информацию национальному центру по защите инфраструктуры и кибербезопасности (CNPIC), который будет проверять их перед внесением в каталог. В этом случае обновление имеющейся информации должно проводиться на ежегодной основе» (ст. 5 (5).

3. УСТАНОВЛЕНИЕ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ

Резолюция Совета Безопасности 2341 (2017)
Пункт 3 постановляющей части

Совет Безопасности (...)

Ссылается на свое решение, содержащееся в резолюции 1373 (2001), о том, что все государства должны квалифицировать террористические акты как серьезные уголовные правонарушения во внутригосударственных законах и положениях, и призывает все государства-члены обеспечить, чтобы они установили уголовную ответственность за террористические акты, направленные на уничтожение или дезактивацию критически важных объектов инфраструктуры, а также за планирование, подготовку, финансирование и материально-техническую поддержку таких нападений;

3.1. Цели криминализации нападений на КВОИ

Требование криминализации действий, направленных на КВОИ, способствует достижению трех взаимосвязанных целей:

- Обеспечить адекватный уровень сдерживания путем применения серьезных мер наказания к лицам, совершившим террористические акты против КВОИ;
- Разрушать преступные / террористические планы, направленные на КВОИ, используя уголовное право в качестве профилактического инструмента. Профилактическая направленность резолюции 2341 (2017) четко вытекает из требования о том, что страны должны криминализировать, среди прочего, «планирование, подготовку, финансирование и материально-техническое обеспечение» террористических атак;
- Установить правовые основы и предпосылки для беспрепятственного международного сотрудничества в области уголовного правосудия по вопросам, связанным с КВОИ.

В разделе 3.2 обсуждается, в какой степени универсальные правовые рамки борьбы с терроризмом касаются преступного поведения в отношении КВОИ. В разделах 3.3, 3.4 и 3.5 представлен обзор того, как в уголовных законах стран решаются вопросы ответственности, связанные с КВОИ, и как установление уголовных преступлений связано с международным сотрудничеством в уголовных делах. Кроме того, в этих разделах рассматриваются основные варианты уголовного права с точки зрения разработки законодательства с учетом международных стандартов и требований, в том числе с точки зрения прав человека.

3.2 Криминализация действий против КВОИ: резолюции Совета Безопасности и международные конвенции

Уникальная особенность резолюции 2341 (2017) заключается в том, что она является первым документом Совета Безопасности, в котором содержится специфичный призыв к государствам криминализировать действия против КВОИ. При этом резолюция 2341 (2017) основывается на ряде ранее принятых резолюций, устанавливающих общие требования для установления уголовной ответственности лиц, совершивших террористические акты. Важнейшим инструментом в этой области (на который прямо ссылается резолюция 2334 (2017)) является резолюция 1373 (2001). Принятая вскоре после событий 11 сентября 2001 года, предусматривает, среди прочего, всеобъемлющий набор требований уголовного правосудия, таких как обязательства:

- Ввести уголовную ответственность за предоставление или сбор средств в связи с совершением террористических актов;

- Отказывать в убежище всем, кто планирует, поддерживает или совершает террористические акты и привлекать их к ответственности;
- Установить террористические акты в качестве серьезных уголовных преступлений в национальном законодательстве.

В дополнение к резолюциям Совета Безопасности в ряде договоров, касающихся предотвращения и пресечения международного терроризма, изложены требования в отношении криминализации в области КВОИ. В отсутствие согласованности в отношении сферы применения всеобъемлющей конвенции, охватывающей все аспекты и проявления международного терроризма, эти документы принимались в течение более пятидесяти лет с учетом секторального подхода. Последовательный и прагматичный подход международного сообщества привел к принятию конвенций и протоколов, ориентированных на такие области, как морская и авиационная безопасность, ядерное и террористическое финансирование и т. д.

Аналогичным образом, в резолюциях Совета Безопасности в этих конвенциях и протоколах не упоминается выражение «критически важные объекты инфраструктуры». Частично это можно объяснить тем фактом, что большинство этих инструментов были приняты в то время, когда само понятие термина «критически важный объект инфраструктуры» еще не утвердилось в глобальной политической дискуссии о борьбе с терроризмом. Однако, как показано в таблице [число], большинство из них содержат положения, ведущие к правонарушениям, непосредственно направленные на злоумышленные действия, направленные на разрушение или вмешательство в функционирование КВОИ. Такие правонарушения часто подробно описываются, поскольку они были предметом тщательных подготовительных работ в рамках длительных технических и дипломатических переговоров.

В той степени, в которой страны являются участниками таких документов, они обязаны внедрить свои положения, в числе прочего, установив поведение, изложенное в них какие уголовное преступление в национальном законодательстве. Странам, которые не являются участниками некоторых конвенций и протоколов о борьбе с терроризмом, предлагается ратифицировать их или присоединиться к ним, как это предусмотрено, в частности, резолюцией 1373 (2001).

Таблица 6: Преступления, связанные с КВОИ, в универсальных документах о борьбе с терроризмом

Сектор КВОИ	**Конвенция/протокол**	Основные преступления * *(Полный перечень требований криминализации и точной формулировки, используемой конвенциями, см. в официальных текстах договоров)
Воздушный	**Конвенция 1963 года о преступлениях и некоторых других актах, совершаемых на борту воздушных судов (и дополнительный протокол к ней от 2014 года)**	Требует, чтобы следующие государства-участники договора устанавливали юрисдикцию для наказания за преступления, совершенных на борту воздушного судна: - государство регистрации воздушного судна; - государство посадки, когда воздушное судно, на борту которого совершено преступление, приземляется на его территории, а предполагаемый преступник все еще находится на борту; - государство оператора, когда правонарушение совершено на борту воздушного судна, сданного в аренду без экипажа арендатору, чье основное место ведения бизнеса или, у арендатора не имеется

		такого основного места ведения бизнеса, чье постоянное место жительства, находится в этом государстве.
	Конвенция 1970 года о борьбе с незаконным захватом воздушных судов (и дополнительный протокол от 2010 года)	Захват или осуществление контроля над воздушным судном, находящимся в эксплуатации, силой или угрозой, или принуждением, или любой другой формой запугивания, или любыми техническими средствами.
	Конвенция о борьбе с незаконными актами, направленными против безопасности гражданской авиации 1971 года, **а также** **Протокол о борьбе с незаконными актами насилия в аэропортах, обслуживающих международную гражданскую авиацию 1988 года, дополненный** **Конвенцией о борьбе с незаконными актами, касающимися международной гражданской авиации 2010 года**	- Совершение акта насилия в отношении лица, находящегося на борту воздушного судна в полете, если этот акт может угрожать безопасности воздушного судна; - Уничтожение воздушного судна, находящегося в эксплуатации, или причинение ущерба такому воздушному судну, которое делает его неспособным к полету или которое может поставить под угрозу его безопасность в полете; - Помещение или размещение на воздушном судне, находящемся в эксплуатации, устройства или вещества, которое может разрушить это воздушное судно или причинить ему ущерб, который делает его неспособным к полету, или причинить ему повреждение, которое может угрожать его безопасности в полете; - Разрушение или повреждение аэронавигационных средств или вмешательство в их эксплуатацию, если любой такой акт может поставить под угрозу безопасность воздушного судна в полете; - Передача информации, которая, как известно, является ложной, что ставит под угрозу безопасность воздушного судна в полете; - Использование против или на борту воздушного судна, находящегося в эксплуатации, любого биологического, химического, ядерного оружия или взрывчатых, радиоактивных или аналогичных веществ таким образом, который вызывает или может привести к смерти, серьезным телесным повреждениям или серьезному повреждению имущества или окружающей среды; - Уничтожение или серьезное повреждение объектов аэропорта, обслуживающего международную гражданскую авиацию, или воздушных судов, не находящихся в эксплуатации, расположенных на нем или нарушение функционирования аэропорта, если такой акт ставит под угрозу или может поставить под угрозу безопасность в этом аэропорту

Морской	**Конвенция 1988 года о борьбе с незаконными актами, направленными против безопасности морского судоходства**	- Захват или осуществление контроля над судном с помощью силы или угрозы, или любой другой формы запугивания; - Совершение акта насилия против лица на борту судна, если этот акт может угрожать безопасному плаванию этого судна; - Уничтожение судна или причинение ущерба судну или его грузу, которые могут угрожать безопасному плаванию этого судна; - Размещение или создание на судне любыми средствами какого-либо устройства или вещества, которое может разрушить это судно или причинить ущерб этому судну или его грузу, что угрожает или может поставить под угрозу безопасное плавание этого судна; - Уничтожение или серьезное повреждение морских навигационных средств или серьезное вмешательство в их эксплуатацию, если любой такой акт может угрожать безопасному плаванию судна - передача информации, которая, как известно, является ложной, что ставит под угрозу безопасное плавание судна;
	Протокол 2005 года к Конвенции о борьбе с незаконными актами, направленными против безопасности морского судоходства	Когда целью акта является запугивание населения или принуждение правительства или международной организации к совершению или воздержанию от совершения какого-либо действия: использование против или на судне или взрыв на корабле любого взрывчатого, радиоактивного материала или биологического, химического, ядерного оружия таким образом, который вызывает или может привести к смерти или серьезной травме или повреждению.
	Протокол 1988 о борьбе с незаконными актами, направленными против безопасности стационарных платформ, расположенных на континентальном шельфе от 1988 года	Захват или контроль стационарной платформы силой или угрозой, или любой другой формой запугивания; Выполнение акта насилия против человека на борту платформы, если этот акт может угрожать ее безопасности; Уничтожение стационарной платформы или ее повреждение, которое может поставить под угрозу ее безопасность; Размещение на стационарной платформе устройства или вещества, которое может разрушить эту стационарную платформу или поставить под угрозу ее безопасность.
	Протокол 2005 года к Протоколу о борьбе с незаконными актами, направленными против	Когда целью акта является запугивание населения или принуждение правительства или международной организации к совершению или воздержанию от совершения какого-либо

	безопасности стационарных платформ расположенных на континентальном шельфе	действия: использование против или на стационарной платформе или взрыв на стационарной платформе любых взрывчатых, радиоактивных материалов или биологического, химического, ядерного оружия таким способом, который вызывает или может привести к смерти или серьезным травмам или повреждению;

Ядерный	**Международная конвенция о борьбе с актами ядерного терроризма 2005 года** **а также** **поправки 2005 года к Конвенции о физической защите ядерного материала**	Использование или повреждение ядерного объекта, вмешательство в его эксплуатацию или совершение любого другого действия, направленного против ядерного объекта таким образом, чтобы выпускать или подвергать риску выброс радиоактивного материала, - с целью причинения смерти или серьезных телесных повреждений; или существенного ущерба имуществу или окружающей среде; или же - со знанием того, что этот акт может привести к смерти или серьезным травмам любого лица или существенному ущербу для имущества или окружающей среды в результате воздействия радиации или выброса радиоактивных веществ, если только этот акт не осуществляется в соответствии с национальным законодательством государства-участника на территории расположения ядерного объекта; или же - принуждать физическое или юридическое лицо, международную организацию или государство совершать, или воздерживаться от совершения акта
Правительственный	**Конвенция о предотвращении и наказании преступлений против лиц под международной защитой от 1973 года**	Проведение насильственного нападения на официальные помещения, частное жилье или транспортные средства лица, находящегося под международной защитой, которое может поставить под угрозу его личность или свободу

Комплексный	**Международная конвенция о борьбе с бомбовым терроризмом от 1997 года** **Международная конвенция о борьбе с финансированием**	Доставка, размещение, взрывание или детонация взрывного или другого смертоносного устройства в месте общественного пользования, в государственном или правительственном учреждении, в системе общественного транспорта или на инфраструктурном объекте с целью вызвать обширное разрушение такого места, объекта или системы, в которой такое разрушение приводит или может привести к крупным экономическим потерям Размещение или предоставление средств для этой цели или при условии, что эти средства будут использованы для совершения террористического акта (как определено в самой Конвенции) или любого другого акта, изложенного в одном из

	терроризма от 1999 года	универсальных документов против терроризма.

Помимо универсальной нормативно-правовой базы по борьбе с терроризмом, ряд региональных контртеррористических документов устанавливают требования криминализации, связанные с КВОИ, особенно в области критически важной информационной инфраструктуры (КИИ). Новаторская конвенция в этой области - Совет Европы по киберпреступности 2001 года, которая впервые представила на международном уровне описания преступного поведения, связанного с нарушением безопасности сети (в дополнение к установлению полномочий и процедур, таких как поиск компьютерных сетей и перехват). Совсем недавно ЕС принял директиву, направленную, среди прочего, на гармонизацию уголовного законодательства государств-членов в области атак на информационные системы. Другим недавним примером является Конвенция Африканского союза 2014 года о кибербезопасности и защите данных (см. Изучение конкретной ситуации ниже).

Изучение конкретной ситуации **27**

Правовые рамки ЕС и Африканского союза по криминализации атак на информационные системы

Директива ЕС 2013 об атаках на информационные системы

Основной целью этого документа является установление минимальных правил для определения уголовных преступлений и соответствующих мер наказаний. Директива предусматривает уголовное наказание, по крайней мере, за дела, которые не являются малозначительными. Государства-члены могут определять, что является малозначительным делом, в соответствии со своим национальным законодательством и практикой. Директива касается, например, создания бот-сетей, т. е. установление удаленного управления значительным количеством компьютеров путем заражения их вредоносным программным обеспечением посредством целенаправленных кибератак. После создания, зараженная сеть компьютеров, составляющая бот-сеть, может быть активирована без ведома пользователей компьютера для запуска масштабной кибератаки.

Важно отметить, что в Директиве определены три «отягчающих» обстоятельства, при которых рассматриваемые правонарушения должны наказываться максимальным сроком тюремного заключения не менее пяти лет. В частности:

- Когда они совершены в рамках преступной организации;

- Когда они наносят серьезный ущерб;

- Когда они совершаются против критически важных объектов инфраструктуры информационной системы.

Конвенция Африканского союза 2014 года о кибербезопасности и защите данных

Принятая в 2014 году, Конвенция требует, чтобы «каждое государство-участник [...] принимало такие законодательные и / или нормативные меры, которые оно сочтет эффективными, рассматривая в качестве существенных деяний уголовные преступления, которые затрагивают конфиденциальность, целостность, доступность и выживание информационных и коммуникационных технологических систем, данных, которые они обрабатывают, и объекты инфраструктуры базовой сети (...) (ст. 25).

Среди положений, касающихся требований криминализации, те, которые непосредственно связаны с защитой КИИ, изложены в ст.29 (Преступления, характерные для информационных и коммуникационных технологий) под двумя подзаголовками «атаки на компьютерные системы» и «нарушения компьютеризированных данных».

Помимо установления правонарушений, связанных с прямыми атаками на компьютерные системы, Конвенция Африканского союза предусматривает явный профилактический подход к совершению кибер-преступлений. В соответствии со статьей 29 (1) (h), в частности, Стороны обязуются «[...] считать уголовным преступлением незаконное производство, продажу, импорт, хранение, распространение, предложение, передачу или предоставление компьютерного оборудования, программ, или любого устройства или данных, разработанных или специально предназначенных для совершения преступлений, или незаконно сгенерировать или произвести пароль, код доступа или аналогичные компьютеризированные данные, обеспечивающие доступ к части или ко всей компьютерной системе».

3.3 Разработка уголовного законодательства по ЗКВОИ

Национальные власти обязаны включать в национальное законодательство элементы преступлений, указанных в конвенциях о борьбе с терроризмом, участниками которых они являются. Кроме того, им необходимо определить, в какой степени они хотят криминализировать преступления, связанные с КВОИ, помимо договорных требований, которые, как видно из предыдущего раздела, охватывают только определенные аспекты этой темы. При планировании введения всеобъемлющего уголовного законодательства, связанного с КВОИ, национальные власти должны учитывать, что не существует международного определения «критически важных объектов инфраструктуры». В общих чертах, можно предусмотреть несколько вариантов оформления:

i) Криминализировать поведение, связанное с конкретными типами объектов инфраструктуры (отраслевой подход);
ii) Криминализировать поведение против КВОИ в целом (межотраслевой подход);
iii) Опираться на криминальное законодательство не специфичное для КВОИ (косвенный подход).

Стоит отметить, что вышеупомянутые подходы не являются взаимоисключающими, и на практике страны часто принимают комбинацию из трех. Какой бы подход (или сочетание подходов) ни был выбран, уголовные преступления должны быть сформулированы в соответствии с принципом законности. Это требует, чтобы уголовная ответственность и наказание основывались на предварительном введении в действие запрета, который выражен с достаточной точностью и ясностью.

i) Отраслевой подход

Преступления, связанные с КВОИ, могут быть нацелены на конкретные критически важные сектора, такие как ядерный, транспортный сектор и т. д. Соответствующее поведение может быть признано уголовным преступлением с или без указания конкретной террористической цели в качестве элемента преступления. Хотя резолюция 2341 (2017) призывает государства быть в состоянии установить уголовную ответственность за террористические акты, она, безусловно, не препятствует странам расширять сферу охвата рассматриваемых преступлений путем криминализации поведения, не связанного с террористической целью. Действительно, формулировка, используемая в большинстве универсальных конвенций о борьбе с терроризмом, подтверждает этот результат. Например, Конвенция 1970 года о борьбе с незаконным захватом воздушных судов требует, чтобы стороны устанавливали в качестве правонарушения акт установления контроля над воздушным судном (силой или угрозой или любой другой формой запугивания) независимо от конкретного намерения или лежащего в его основе мотивации преступника.

Несколько примеров отраслевого законодательства можно найти в странах « англосаксонского права», например: гражданская авиация Фиджи (Закон о безопасности), 1994 год, Закон Шри-Ланки о борьбе с бомбовым терроризмом 1999 года, и закон Великобритании о лицах, состоящих под международной защитой 1978 года. Часто когда выбран отраслевой подход, связанные с ним преступления являются частью более широкой нормативной базы, также направленной на детальное регулирование операций

в секторе, требований и процедур лицензирования и т. д. Примером является Закон Японии о регулировании материалов, являющихся источником ядерного топлива, материала ядерного топлива и реакторов.

Преимущество этого подхода заключается в том, что он позволяет странам точно адаптировать свои требования в отношении криминализации к особенностям определенных типов инфраструктуры и секторов. Это также позволяет идентифицировать штрафы, которые более точно отражают восприятие уровня «критичности» определенных активов и ожидаемого воздействия в случае сбоев. Основным недостатком этого подхода является то, что он ограничивает охват уголовного права закрытым списком секторов / активов, оставляя тем самым другие без внимания.

ii) Межотраслевой подход

Несколько стран криминализируют нападения на КВОИ непосредственно как террористические преступления. Хотя обычно сфера действия террористических преступлений, связанных с КВОИ, не ограничивается какими-либо конкретными секторами, ряд стран приводят неисчерпывающие примеры типов охватываемой инфраструктуры. Например, законодательство Кении определяет «террористический акт» как акт или угрозу действия, которые, в частности, «мешают работе электронной системы, что приводит к нарушению предоставления услуг связи, финансов, транспорта или других важных услуг [или] мешает или нарушает оказание основных или неотложных услуг [...]».

В Рамочном решении ЕС о борьбе с терроризмом[20], нападения на КВОИ занимают видное место среди материальных элементов террористических преступлений в форме, в частности: «обширного уничтожения правительственного или общественного объекта, транспортной системы, объекта инфраструктуры, включая информационную систему, стационарную платформу, расположенной на континентальном шельфе, общественное место или частную собственность, которые могут поставить под угрозу человеческую жизнь или привести к значительным экономическим потерям», или « захват воздушных судов, судов или других средств общественного или грузового транспорта», или «вмешиваться или нарушать подачу воды, электроэнергии или любой другой фундаментальный природный ресурс, воздействие которого должно поставить под угрозу человеческую жизнь».

С другой стороны, выражение «критически важный объект инфраструктуры», которое присутствует в большинстве документов и стратегий национальной политики, не фигурирует как таковое в национальных законах о борьбе с терроризмом. Чаще всего упоминаются понятия «общественная инфраструктура» или «основные услуги, средства или системы», часто когда их разрушение или вмешательство в их функционирование приводит к серьезным экономическим потерям, опасности для жизни людей и т. д.

Стоит отметить, что ряд законов, предусматривающих уголовную ответственность за нападения на КВОИ, как террористические акты, являются осторожными и предусматривают исключения для действий, предпринимаемых в контексте законного осуществления определенных гражданских, политических или социальных прав. Например, уголовный кодекс Канады исключает из понятия «террористическая деятельность» те акты, которые, хотя и вызывают «серьезное вмешательство или серьезное нарушение основных услуг, объектов или систем, будь то государственные или частные, совершаются» в результате защиты общественных интересов, протеста, инакомыслия или прекращения работы, которая не планировалась как результат такого поведения или вреда, упомянутого в [определении «террористическая деятельность»].[21]

Преимущество межсекторального подхода заключается в том, что он обеспечивает основу для обеспечения охвата всех секторов КВОИ, включая те, которые потенциально могут быть добавлены в качестве критически важных в будущем. Если существуют другие внутригосударственные уголовные законы, касающиеся конкретных секторов, эти законы обычно применяются как «lex specialis» (специальные законы, отменяющие действие общего закона). Одним из возможных недостатков является отсутствие точности в том, что законодатель может установить один диапазон мер наказаний,

[20] Рамочное решение ЕС от 13 июня 2002 года о борьбе с терроризмом (2002/475 / JHA), ст.1.
[21] Криминальный кодекс, 83.01(1).

который неразличимо применим во всех секторах. В этих случаях у судей может быть больше возможностей для адаптации уровней мер наказаний к обстоятельствам дела, чем при узком отраслевом подходе.

Изучение конкретной ситуации **28**

Закон ЮАР о защите конституциональной демократии от террористической деятельности № 33 от 2004 года

Определение терроризма / террористического акта в ЮАР содержит особенно обширную и подробную ссылку на КВОИ. Соответственно, «террористическая деятельность» означает, среди прочего:

«(a) любое действие, совершенное в Республике или за ее пределами, которое: [...]

(vi) спланировано или рассчитано для того, чтобы вызвать серьезные помехи или серьезное нарушение жизненно важных услуг, средств или систем или предоставление любой такой услуги, средств или систем, будь то государственных или частных, в том числе, но не ограничиваясь -

(aa) системы, используемой электронной системой, включая информационную систему;

(bb) телекоммуникационная услуга или система;

(cc) банковская или финансовая служба или финансовая система;

(dd) система, используемая для предоставления жизненно важных государственных услуг;

(ee) система, используемая жизненно важным поставщиком коммунальных услуг или транспорта;

(ff) жизненно важный объектов инфраструктуры; или же

(gg) любые жизненно важные экстренные службы, такие как полиция, медицинские службы или службы гражданской обороны;

(vii) приводит к серьезным экономическим потерям, значительной дестабилизации экономической системы или значительному разрушению национальной экономики страны; или же

(viii) создает серьезную общественную чрезвычайную ситуацию или общее восстание в Республике, независимо от того, причинен ли ущерб, предусмотренный в пунктах (a) (i) до (vii), в Республике или за ее пределами, и является ли деятельность, упомянутая в подпунктах (ii) до (viii) было совершено каким-либо способом или методом; а также

(b) то, что предполагает, по своему характеру и контексту может быть разумно рассмотрено как планирование, полностью или частично, угрожающее единству и территориальной целостности Республики через следующие поступки -

запугивать или вызывать чувство неуверенности среди общественности или части общества в отношении своей безопасности, включая экономическую безопасность, или вызывать, создать или распространять чувство страха, ужаса или паники среди гражданского населения; или же

ненадлежащим образом принуждать, запугивать, заставлять, добиваться или побуждать какое-либо лицо, правительство, широкую общественность или часть общественности, или национальную или международную организацию, или орган или межправительственную организацию или орган делать или воздерживаться совершать какие-либо действия, или принимать или отказываться от определенной точки зрения, или действовать в соответствии с определенными принципами,

находятся ли общественность или лицо, правительство, орган или организация, или учреждение, упомянутые в подпунктах (ii) или (iii), в зависимости от обстоятельств, внутри или за пределами Республики; а также

(c) совершенное, прямо или косвенно, полностью или частично, с целью продвижения индивидуального или коллективного политического, религиозного, идеологического или философского мотива, цели, причины или обязательства [...]

iii) Косвенный подход

Этот подход состоит в криминализации действий против КВОИ с использованием «стандартных» уголовных преступлений, таких как повреждение имущества, поджог, незаконное проникновение (например, несанкционированный доступ к собственности) и т. д.

Одним из преимуществ является то, что страны могут полагаться на базовый ряд устоявшихся правонарушений в ожидании принятия более целенаправленных правовых рамок или для того, чтобы заполнить пробелы, оставленные новым законодательством, касающимся КВОИ. Другим потенциальным преимуществом является то, что судьи во многих странах часто более знакомы и свободны в применении этих «классических» преступлений, чем новые режимы, связанные с КВОИ. Недостатки этого подхода включают отсутствие разграничения между критическими и некритическими активами. Кроме того, запрет на применение уголовных законов по аналогии вызывает, по крайней мере, серьезные сомнения в отношении возможности применения в кибер-области преступлений, которые были задуманы только для физического мира (например, использование традиционных преступлений с целью незаконного доступа к компьютерным системам).[22]

3.4 Сфера действия уголовного законодательства, связанного с КВОИ

При формулировании уголовных преступлений, связанных с КВОИ, необходимо учитывать важные аспекты их применения. Национальные власти должны обеспечить, чтобы их уголовное законодательство должным образом учитывало следующие сценарии:

- Нападение на инфраструктуру, расположенную на территории государства, оказывает существенное воздействие на другое государство. Подобный сценарий в основном происходит в случае действий с участием КИИ. Например, система промышленного контроля (ICS), расположенная в стране A, регулирует доставку газа в страну B. После манипуляции с ICS сбои ощущаются в стране B, но не в стране A;

- После нападения на КВОИ, находящегося в стране A, предполагаемый преступник находит убежище в стране B. Все универсальные договоры о борьбе с терроризмом обязывают страны устанавливать свою экстерриториальную юрисдикцию в отношении действий, совершенных за границей, по крайней мере, в двух случаях:

    - Преступление было совершено одним из их граждан (принцип активного гражданства);

    - предполагаемый преступник находится на территории государства и не выдается ни одному государству, запрашивающему выдачу за такое же поведение (так называемое «aut dedere aut judicare» (либо выдай, либо суди))

Некоторые конвенции о борьбе с терроризмом устанавливают особые юрисдикционные критерии. Например, в случае совершения преступления, связанного с воздушными судами, в соответствии с Конвенцией 1970 года о борьбе с незаконным захватом воздушных судов или Конвенцией 1971 года о борьбе с незаконными актами, направленными против безопасности гражданской авиации, национальные суды устанавливают юрисдикцию в отношении преступлений на борту воздушного судна, если воздушное судно приземляется на территории государства с предполагаемым

[22] С практической точки зрения, расследование киберпреступлений ставит особые проблемы с точки зрения присвоения соответствующих видов поведения.

преступником, все еще находящимся на борту, и никакое другое государство-участник не запрашивает его выдачу для целей судебного преследования.

В других случаях конвенции о борьбе с терроризмом предусматривают необязательные основания для юрисдикции, например, в случае преступлений, совершенных за границей против гражданина (принцип пассивного гражданства). Национальным органам власти следует рассмотреть вопрос о введении таких дополнительных оснований и определить для дел или секторов КВОИ, не охватываемых применимой международно-правовой базой, соответствующий охват преступлений, связанных с КВОИ.

3.5 Международное сотрудничество по уголовным делам

Как упоминалось в разделе 3.1, необходимость того, чтобы государства криминализировали поведение, закрепленное в универсальных правовых рамках борьбы с терроризмом, также способствует международному сотрудничеству в уголовных делах. В той мере, в которой соответствующие (связанные с КВОИ) правонарушения были бы включены в уголовное законодательство государств-участников, значительные правовые препятствия для беспрепятственного сотрудничества могут быть устранены. Например, классическое требование о том, что выдача (и, в меньшей степени, взаимная правовая помощь) может быть предоставлена только в том случае, если рассматриваемое преступление криминализировано как в запрашиваемом, так и в запрашивающем государстве-члене, будет автоматически выполнено, если оба государства добросовестно перенесут язык договора в свои соответствующие уголовные законы.

В то же время способность отдельных стран эффективно преследовать по суду правонарушителей часто будет зависеть от эффективности существующих международных каналов сотрудничества между правоохранительными органами, сдачи лиц, скрывающихся от правосудия, и обмена доказательствами. Важно отметить, что страны, намеревающиеся обеспечить максимальную защиту своих КВОИ с точки зрения уголовного правосудия, должны учитывать роль универсальных инструментов борьбы с терроризмом в обеспечении правовых основ для выдачи и взаимной правовой помощи, как в дополнение, так и в отсутствие двусторонних или региональных договоренностей на этот счет.

С точки зрения правоохранительной деятельности стратегическая структура Интерпола на 2017–2020 годы ставит первую стратегическую цель для Организации «служить всемирным информационным центром сотрудничества в правоохранительной сфере» путем управления безопасными каналами связи, которые соединяют национальные центральные бюро во всех 192 странах-членах Интерпола, наряду с другими уполномоченными правоохранительными органами и партнерами, которые предоставляют доступ к ряду криминальных баз данных.

Сеть Интерпола I-24/7 лежит в основе всей оперативной деятельности Интерпола в поддержку международного сотрудничества по уголовным делам между его странами-членами. I-24/7, от рутинных проверок на пограничных переходах до целенаправленных операций в различных районах преступления и от развертывания специализированных групп реагирования до поиска лиц, скрывающихся от правосудия, является основой для обмена информацией между полицией мира.

Что касается борьбы с терроризмом и КВОИ, то в глобальной контртстратегии Интерпола подчеркивается решающее значение международного сотрудничества между правоохранительными органами во всем мире. Оно определяет контртеррористический мандат Интерпола как оказание помощи и создание возможностей для правоохранительных органов в его странах-членах по предотвращению и пресечению террористической деятельности путем выявления членов

террористических сетей и их филиалов, путем устранения основных факторов, способствующих их деятельности: поездок и мобильности, присутствия в сети, оружия, материалов и финансов.

Независимо от того, какой канал сотрудничества используется, странам необходимо обеспечить полное соблюдение стандартов справедливого судебного разбирательства и надлежащей правовой процедуры. Это относится не только к внутренним судебным процессам, направленным на установление уголовной ответственности отдельных лиц, но и к судебным разбирательствам, возбужденным от имени других стран в связи с выдачей лиц, скрывающихся от правосудия, или передачей вещественных доказательств.

4. ОБМЕН ИНФОРМАЦИЕЙ И ОПЫТОМ

Резолюция Совета Безопасности 2341 (2017)

Совет Безопасности (...):

4. Призывает государства-члены изыскать возможности для обмена соответствующей информацией и активно сотрудничать в деле предотвращения террористических нападений, планируемых в отношении критически важных объектов инфраструктуры, и обеспечения защиты от них и готовности к ним, а также смягчения последствий уже совершенных нападений, их расследования, реагирования на них и восстановления после них;

5. Призывает далее государства установить или укрепить национальные, региональные и международные партнерские отношения с заинтересованными сторонами, как государственными, так и частными, сообразно обстоятельствам, в целях обмена информацией и опытом и тем самым предотвращения террористических нападений на критически важные объекты инфраструктуры, обеспечения защиты от них, смягчения их последствий, их расследования, реагирования на них и восстановления после причиненного ими вреда, в том числе путем проведения совместных учебных мероприятий и применения или создания соответствующих сетей связи или экстренного оповещения;

7. Рекомендует Организации Объединенных Наций, а также тем государствам-членам и соответствующим региональным и международным организациям, которые разработали надлежащие стратегии защиты критически важных объектов инфраструктуры, сотрудничать со всеми государствами и соответствующими международными, региональными и субрегиональными организациями и структурами в целях выявления и широкого применения передовой практики и мер по регулированию риска террористических нападений на критически важные объекты инфраструктуры;

4.1 Обмен информацией в контексте стратегий ЗКВОИ

Если архитектура управления для ЗКВОИ является основой любой взаимосвязанной стратегии, обмен информацией является ее жизненной силой. Правильный обмен информацией способствует достижению ЗКВОИ на всех уровнях и на всех этапах. Это ключевой фактор, на котором строятся государственно-частные партнерства (см. Раздел 4.5.2). Координация внутригосударственных агентств основана на обмене информацией (см. Главу 7). Наконец, масштабы и качество международного сотрудничества в области КВОИ определяются способностью и желанием государств обмениваться информацией через границы (см. Главу 8).

4.2 Аспекты обмена информацией для ЗКВОИ

При установлении операционных рамок для обмена информацией стратегии по ЗКВОИ и / или связанные с ними планы реализации должны учитывать три основных вопроса:

- какую информацию следует обменивать и почему;
- каким образом будет передаваться информация по любому заданию;
- среди кого информация будет передана.

Информацией можно обмениваться на стратегическом, техническом или тактическом уровне. С другой стороны, информация может быть связанной или несвязанной с инцидентом. Это может также принять форму обмена информацией в режиме реального времени в контексте неизбежного или продолжающегося кризиса, когда ожидается, что получающая сторона предпримет немедленные действия. Всякий раз, когда речь идет об этом последнем типе информации, платформы для обмена

информацией (и связанные с ней функции безопасности) будут сильно отличаться от тех, которые стремятся донести лучшие практики или стратегические рекомендации и т. д.

Обмен информацией может (и должен) происходить между различными типами заинтересованных сторон:

- Между общественными организациями и операторами КВОИ (как в данном секторе, так и между секторами);
- Между операторами КВОИ (как внутри данного сектора, так и между секторами);
- Между государственными структурами.

4.2.1 Государственные субъекты - операторы КВОИ

Процесс приватизации нескольких секторов КВОИ и подсекторов, таких как газовые, почтовые системы и телекоммуникационные услуги, который исторически происходил во многих странах, привел к тому, что несколько операций КВОИ перешли в частные руки. Это, в свою очередь, породило необходимость прочных партнерских отношений между государственным и частным секторами. Обмен информацией для целей ЗКВОИ является жизненно важной задачей, которая должна выполняться в рамках таких партнерств.

Обмен информацией между правительственными учреждениями и операторами КВОИ должен проходить в обоих направлениях и охватывать, в частности:

Угрозы: например, правоохранительные органы и разведывательные службы должны передавать информацию о новых типах угроз операторам КВОИ. Эта информация гарантирует, что операторы КВОИ проводят оценку рисков и принимают необходимые меры по смягчению. С другой стороны, операторы КВОИ должны сообщать о результатах оценки рисков и мерах по смягчению, принятых соответствующими государственными структурами, чтобы обеспечить лучшую модуляцию планов по смягчению. В этом контексте «фиолетовые и оранжевые уведомления» Интерпола имеют особое значение для распространения срочной информации среди мирового сообщества правоохранительных органов и общественности. В то время как фиолетовые уведомления помогают искать или предоставлять информацию о modus operandi (метод работы), объектах, устройствах и методах сокрытия, используемых преступниками, оранжевые уведомления используются для предупреждения о событии, человеке, объекте или процессе, представляющем серьезную и неизбежную угрозу для государственной безопасности;

Подозрительные действия: операторам КВОИ может быть рекомендовано сообщать о так называемых «слабых сигналах», то есть о необычных ситуациях, которые сами по себе недостаточны для срабатывания тревоги, но выявляют надвигающуюся угрозу при рассмотрении в контексте аналогичных событий или когда возникает простое подозрение посредством информации, поступающей из других источников;

Данные об инцидентах: уроки, извлеченные из прошлых инцидентов (включая то, что было сделано, а не сделано для их устранения), могут дать важную информацию о способах предотвращения повторения такой же ситуации; это, в свою очередь, обеспечивает основу для более эффективного управления рисками и действиями по восстановлению.

В таблице [число] обобщены основные типы информации, связанной с КВОИ, которой государственный сектор может обмениваться с частным сектором (и наоборот) для противодействия угрозам кибертерроризма.

Таблица 7: Типы обмена государственной / частной информацией об угрозах кибертерроризма

Информация государственного сектора[23]	**Информация частного сектора**
• Ценная информация о кибер-возможностях ключевых террористических организаций	• Информация об основных категориях активов в энергетическом секторе (например, данные о газе, нефти, электричестве, возобновляемых источниках энергии; показатели надежности; информация с бирж по торговле энергией).
• Информация о связях между различными террористическими и нетеррористическими группами.	• Информация о технической уязвимости для конкретных аппаратных и программных продуктов, используемых операторами энергетической инфраструктуры.
• Ценная информация о прошлых векторах атаки	• Анонимная информация о последствиях прошлых атак
• Ценная информация о возможных направлениях будущих атак, выведенная из анализа подпольных веб-сайтов киберпреступников.	• Ценная информация о восстановлении должна учитывать различные формы атак.
Источник: ОБСЕ 2013, стр 74	• Анализ моделей атак в других критически важных секторах инфраструктуры, которые могут служить индикаторами раннего предупреждения для энергетического сектора.

Государственно-частный обмен информацией часто рассматривается как инструмент, позволяющий сломать стену между двумя отдельными мирами и помочь создать подлинное чувство общности вокруг вопросов КВОИ. Достижение этой цели тем более важно, учитывая отношение взаимных подозрений и реальную тенденцию частного и государственного секторов не обмениваться информацией, особенно секретной. Интересный тип проблем в этой области можно найти в энергетическом секторе. По данным ОБСЕ, «с точки зрения осведомленности о безопасности все еще существует большое расхождение между реальной потенциальной угрозой целевых атак и тем, как они воспринимаются. Это в основном связано с тем, что большинство атак, происходящих в областях поставок энергии и энергической промышленности, не предаются гласности, поскольку операторы затронутых установок не хотят сообщать об этих инцидентах. Такой подход создает ситуацию (инциденты воспринимаются как отдельные события), которая усиливает эту тенденцию к сохранению секретности инцидентов. Промышленность в некоторых странах просят, стимулируют, а иногда и обязывают сообщать об этих инцидентах» (ОБСЕ 2013, стр.58).

В контексте киберугроз обмен ценной информацией может включать информацию относительно:

- Уязвимостей (например, недостаток программного обеспечения, который можно использовать);
- Инциденты кибербезопасности (например, успешная атака на системы компании);
- Защитные меры (например, информация о патче).

Обмен информацией в этом контексте имеет существенные преимущества повышения безопасности и улучшения киберзащиты. Может быть полезно рассмотреть шаги, способствующие обмену кибер-информацией и снизить эти риски. Например, в качестве одного из первых шагов по устранению юридического риска обмена кибер-информацией Соединенные Штаты ввели закон об обмене информацией о кибербезопасности[24], который предоставляет, при некоторых обстоятельствах, надежную защиту от гражданской ответственности за определенные действия по обмену информацией, «проводимые в соответствии» с положениями этого закона.

[23] Ссылка на «государственный сектор» в таблице понимается как «правительственные учреждения».

[24] Закон об общих ассигнованиях 2016 года, P.L. 114-113, Отдел N (Закон о кибербезопасности 2015 года), Раздел I (Закон об обмене информацией о кибербезопасности 2015 года), 129 Stat. 2936, 6 США §§ 1501-1510.

Изучение конкретной ситуации **29**
Стимулы для частного сектора по обмену информацией в стратегии кибербезопасности Японии

Стратегия Японии в области кибербезопасности направлена на преодоление колебаний бизнеса делиться информацией с государственными органами, опасаясь потери доверия или доли рынка. Согласно этой стратегии, «чтобы сделать обмен информацией более активным, важно облегчить психологическое бремя операторов КИИ, которое может привести к потере доверия или порче репутации своих предприятий, если они предоставляют информацию соответствующей стороне, и позволяют им узнавать преимущества в результате такого действия. Правительство будет поощрять операторов КИИ к достижению общего понимания относительно внесения соответствующих изменений в предоставляемую информацию, таких как сокрытие личности информаторов и определение объема и предела информации, подлежащей обмену, и создаст среду, в которой информаторы не понесут никакой необоснованной потери или ущерба от предоставления информации».

Источник: Япония 2015, с.27

4.2.2 Операторы КВОИ - операторы КВОИ

Предоставление наиболее важных услуг является результатом сложных цепочек поставок, требующих участия различных компаний, работающих в нескольких секторах инфраструктуры и отраслевых сегментах. Зависимости цепочки поставок показывают важность наличия надлежащих частных-частных каналов для потоков информации между секторами. Обмен информацией в этой области может носить технический или организационный характер.

Необходимость создания адекватных механизмов обмена информацией также касается операторов КВОИ, производящих или поставляющих товары или услуги одного и того же типа в одном и том же секторе промышленности. По-видимому, это особенно актуально для обмена передовым опытом, информацией о методологиях оценки рисков, применяемых защитных мерах, уроках, извлеченных после инцидентов, и т. д. Опытные компании с многолетней практикой в области защиты КВОИ могут с пользой передать свои знания компаниям, которые менее знакомы с применимой нормативно-правовой базой и стратегиями соответствия КВОИ. В то же время необходимо осознавать внутреннюю сложность обеспечения бесперебойного обмена информацией между компаниями, которые часто являются конкурентами. По этой причине они могут опасаться сотрудничества друг с другом, особенно в обмене конфиденциальной информацией, из-за боязни потерять долю рынка.

4.2.3 Государственные субъекты - государственные субъекты

Создание механизмов обмена информацией между государственными учреждениями жизненно важно в той мере, в которой государственные учреждения уполномочены координировать и осуществлять действия, связанные с ЗКВОИ, как по горизонтали, так и по вертикали. Примером «горизонтального» обмена информацией является случай, когда несколько министерств отвечают за конкретные сектора и должны объединиться для решения межсекторальных вопросов. Другой случай связан с необходимостью предоставления разведывательными органами информации соответствующим органам, отвечающим за ЗКВОИ, с целью разработки национальных оценок рисков. Примерами соглашений вертикального типа являются те, которые необходимы для поддержки разделения труда между муниципальными, региональными и национальными органами власти, особенно (но не исключительно) в федеральных штатах.

Обмен информацией между государственными предприятиями является одним из аспектов более широких межучережденческих усилий по координации, которые более подробно рассматриваются в главе 5.

Изучение конкретной ситуации **30**
Обеспечение безопасности потока информации: спутниковая система связи Великобритании (HITS)

Технологии могут оказать существенную поддержку агентствам в обеспечении передачи критически важной информации во время чрезвычайных ситуаций. В Великобритании эту цель преследуют HITS. Разработанная правительством Великобритании, HITS - это независимая система, которая будет продолжать функционировать, когда обычная стационарная и мобильная связь недоступна или повреждена. Основанная на военной спутниковой сети Скайнет 5, она доступна для сотрудников полиции и других аварийных служб на стационарных объектах, расположенных по всей территории Великобритании, с дополнительными переносными блоками, позволяющими развертывать HITS в любом месте и в любое время, когда возникнет такая необходимость. Обеспечивая как передачу голоса и данных, так и доступ к Интернету, HITS играет важнейшую роль в обеспечении бесперебойной связи между региональным и национальным уровнями координации кризисов во время любого разрушительного события.

Источник: Кабинет министров Великобритании, по адресу: https://www.gov.uk/guidance/resilient-communications

4.3 Предпосылки для эффективного обмена информацией

Опыт показывает, что эффективность обмена информацией о ЗКВОИ зависит от двух основных факторов:

- Способности ведущих агентств создавать доверие среди заинтересованных сторон;
- Обеспечение адекватных уровней защиты конфиденциальной информации, обмен которой поощряется или разрешается в соответствии с соглашениями ЗКВОИ.

Разработчикам стратегий ЗКВОИ (и тем, кто призван их реализовывать) важно понять, как эти два фактора влияют друг на друга. В то время как уровни доверия будут снижаться, если информация не защищена надлежащим образом, жесткие уровни защиты информации сами по себе не будут вызывать более высокое доверие среди участников.

4.3.1 Доверительное управление

Создание подлинного доверия между участниками по определенному соглашению об обмене информацией может занять много времени и требует активной приверженности всех заинтересованных сторон. Однако после установления доверия потоки информации значительно возрастут как в качественном, так и в количественном отношении.

Основываясь на обзоре методологий ЗКВОИ, в которых основное внимание уделяется европейским странам, RECIPE составил список «основных факторов успеха» в обмене информацией. В частности, «опыт показал, что доверие лучше всего строить на небольших встречах с глазу на глаз. В общем, есть некоторые основные правила. Как правило, обмен информацией лучше всего начинать на уровне не слишком детализированном. Не всегда необходимо обмениваться слишком специфичной информацией, например, информацией о критически важных объектах и их местонахождении, или

конкретной информацией об уязвимостях или инцидентах. Некоторые успешные случаи по обмену информацией подчеркивают, что начинание с малого поможет установить требуемый уровень доверия. Для установления доверия необходимо иметь преемственность в людях, посещающих встречи по обмену информацией. Участники должны быть назначены на личном уровне с достаточным мандатом и ответственностью в своей собственной среде. Как правило, никакие замены не допускаются. Встречи по обмену информацией сконцентрированы на обмене информацией: все участвующие организации должны (в принципе) предоставлять информацию. Убедитесь, что предоставленная информация имеет правильный уровень содержания и фона. Основываясь на информации, получатели информации должны иметь возможность предпринять соответствующие действия в своих соответствующих организациях или быть предупреждены о новой угрозе. Прежде всего, поставщик информации остается владельцем общей информации и ее категории секретности. Большинство примеров успешного обмена информацией основаны на доверии. Однако есть также некоторые обязательные примеры, в которых необходимо делиться информацией об оценках риска и инцидентах, например, сообщение о значительных помехах в сетях связи общего пользования в соответствии со статьей 13a телекоммуникационного пакета ЕС. При обязательном подходе зачастую трудно гарантировать качество передаваемой информации. Поэтому даже утвержденные подходы подчеркивают, что ключом к успеху их схемы по-прежнему является укрепление доверия и дух добровольного сотрудничества. Опыт показывает, что инструменты для электронного обмена информацией лучше всего использовать в качестве дополнительного инструмента для существующих доверенных сообществ по обмену информацией. Если уровень доверия отсутствует, то очень сложно создать высокий уровень доверия в электронной среде» (RECIPE 2011, стр.52).

4.3.2 Защита конфиденциальной информации

Создание доверительной среды для обмена информацией зависит от установления четких правовых и операционных рамок для защиты конфиденциальной природы совместно используемых данных. При разработке таких рамок главная цель, заключающаяся в содействии распространению информации для целей ЗКВОИ, должна всегда учитывать необходимость соблюдения применимых документов, касающихся прав на неприкосновенность частной жизни и защиту данных. Например, в соответствии с Хартией основных прав ЕС, персональные данные «должны обрабатываться справедливо для определенных целей и на основе согласия соответствующего лица или какой-либо другой законной основы, установленной законом. Каждый имеет право на доступ к данным, которые были собраны в отношении него, а также иметь право на ее исправление».[25]

Определение «конфиденциальной информации, относящейся к ЗКВОИ», приводится в Директиве Совета ЕС 2008/114 / ЕС следующим образом: «Факты о критически важной инфраструктуре, которая в случае ее раскрытия может быть использована для планирования и действий с целью вызвать нарушение или разрушение объектов критически важной инфраструктуры»[26].

В той же Директиве излагается «особый принцип», согласно которому «государства-члены, Комиссия и соответствующие надзорные органы должны обеспечивать, чтобы конфиденциальная информация, связанная с защитой европейской критически важной инфраструктуры, представляемая государствам-членам или Комиссии, не использовалась для каких-либо целей, кроме защиты критически важных инфраструктур. [Это] также применимо к неписьменной информации, которой обмениваются во время встреч, на которых обсуждаются важные вопросы».[27]

[25] Ст.8.
[26] Статья 2(d).
[27] Статья 9.

Изучение конкретной ситуации **31**
Защита конфиденциальной информации авиационной безопасности

ИКАО разработала общие руководящие принципы защиты информации о безопасности полетов, связанной с авиацией. Это должно ограничиваться теми лицами, которые нуждаются в такой информации при исполнении своих обязанностей и, следовательно, имеют право на доступ к ней (так называемый принцип «необходимости знать»). Защитные меры должны применяться к конфиденциальной информации об авиационной безопасности, а степень защиты должна быть указана либо государством, либо соответствующими субъектами, принимая во внимание национальные требования по защите конфиденциальной информации, установленные соответствующими органами. Защитные меры могут также потребоваться при идентификации, классификации, получении, сохранении, раскрытии, распространение или утилизации конфиденциальной информации по авиационной безопасности.

Конфиденциальная информация по авиационной безопасности должна храниться, когда она не используется, для предотвращения несанкционированного доступа. Например, использование шкафов безопасности, запираемых комнат или сейфов можно считать способом обеспечения большей защиты, если это необходимо. Электронные копии конфиденциальных документов по авиационной безопасности должны быть равнозначно защищены. Государствам и соответствующим субъектам следует принять меры для обеспечения того, чтобы уполномоченные лица, имеющие доступ к конфиденциальной информации по авиационной безопасности, не раскрывали такую информацию посторонним лицам. Например, следует рассмотреть вопрос о том, чтобы уполномоченные лица подписали «соглашение о неразглашении», прежде чем им будет разрешен доступ к такой информации.

Всякий раз, когда необходимо обмениваться информацией между государствами, последние должны четко определять информацию как конфиденциальную информацию по авиационной безопасности и сообщать о любых конкретных требованиях к защитным мерам, которые должны применяться до передачи такой информации другим государствам. Государства, получающие конфиденциальную информацию об авиационной безопасности, должны применять необходимые защитные меры для предотвращения несанкционированного использования или разглашения.

Источник: Руководство по безопасности ИКАО, документ 8973, ограничен.

Что касается операторов КВОИ частного сектора, они, вероятно, будут обмениваться данными об инцидентах или факторах уязвимости только в том случае, если они получат соответствующие заверения в том, что раскрытие конфиденциальной информации не окажет на них негативного влияния (например, это не даст конкурентам конкурентного преимущества или не будет использовано против них государственными органами в целях, отличных от защиты КВОИ).

Не вся информация, связанная с КВОИ, должна рассматриваться конфиденциально. Точно так же не вся информация, считающаяся «конфиденциальной», заслуживает одинаковой степени защиты. Ограничения на распространение информации, связанной с КВОИ, могут принимать различные формы и быть более или менее строгими в зависимости от конкретных обстоятельств и целей определенного типа обмена информацией. Например, в Новой Зеландии установлен базовый принцип, согласно которому инциденты должны рассматриваться на самом низком уровне конфиденциальности в качестве способа раннего и эффективного распространения критически важной информации среди всех респондентов, отвечающих за снижение воздействия.

Защита информации, связанной с КВОИ, может начаться с принятия законодательства на основе принципа, согласно которому ненадлежащий выпуск конфиденциальных данных может представлять угрозу для национальной безопасности или общественной безопасности. В Канаде Закон об управлении чрезвычайными ситуациями 2007 года включает поправку к закону о доступе к

информации 1985 года для обеспечения защиты конфиденциальной информации, предоставляемой критически важными секторами инфраструктуры.

Изучение конкретной ситуации **32**
Национальные подходы по защите конфиденциальной информации, относящейся к КВОИ: Австралия и Франция

Австралия:

Созданная Правительством Австралии в 2003 году, доверенная сеть обмена информацией (TISN) является основным механизмом взаимодействия в стране с инициативами по обмену информацией между бизнесом и правительством и повышением устойчивости. TISN обеспечивает безопасную среду, в которой владельцы и операторы КВОИ в семи отраслевых группах регулярно встречаются для обмена информацией и сотрудничества внутри и между секторами для решения проблем безопасности и непрерывности бизнеса. Отраслевые группы TISN включают банковское дело и финансы, связь, энергетику, продукты питания и продовольствие, здравоохранение, транспорт и водоснабжение. Кроме того, существуют специализированные форумы (межсекторальные группы по интересам), которые помогают во временном изучении комплексных вопросов, и экспертно-консультативная группа по устойчивости, которая уделяет большое внимание организационной устойчивости. Координационное и стратегическое руководство для TISN обеспечивает Консультативный совет по критически важной инфраструктуре (CIAC). CIAC состоит из председателей каждой из групп TISN, старших представителей правительства Австралии из соответствующих учреждений, а также высокопоставленных представителей правительства штатов и территорий.

Источник: Доверенная сеть обмена информацией, по адресу: https://tisn.gov.au/

Франция:

Директивы и планы, принятые в рамках национальной системы обеспечения безопасности жизнедеятельности (SAIV), классифицируются на уровне конфиденциальной защиты. Являясь эмитентом или получателем, оператор КВОИ обеспечивает уничтожение секретных документов, которые ему больше не нужны, особенно когда:
- засекреченный документ пересмотрен или отменен;
- «жизненно важная точка» (ЖВТ) отменяется;
- «жизненно важная зона» (ЖВЗ) отменяется;
- оператор теряет свой статус «жизненно важного оператора» (ЖВО).

ЖВО, возможно, не пожелает раскрыть некоторую очень конфиденциальную информацию, связанную с управлением рисками и кризисами. В этом случае он должен ссылаться на особые процедуры или положения, ссылаясь на свои внутренние документы, которые их предусматривают. Компетентные административные органы, контролирующие планы безопасности оператора, могут обсудить этот вопрос с оператором, если это необходимо для выполнения его роли. Такие органы могут принять к сведению информацию, которую оператор желает скрыть, без необходимости ее удаления.

Источник: Франция 2014

На практике существует ряд методов и решений для защиты распространения конфиденциальной информации. Как правило, они сосредоточены вокруг: i) процедур допуска и благонадежности; ii) системы цветового кодирования; iii) электронных инструментов. Все три часто дополняют друг друга.

i) Допуск и проверка благонадежности

Правительства могут предоставить допуски к секретной информации для ключевых заинтересованных сторон, которым необходим доступ к конфиденциальной информации, связанной с КВОИ. Согласно Директиве Совета ЕС 2008/114 / ЕС, «любое лицо, обрабатывающее секретную информацию в соответствии с настоящей Директивой от имени государства-члена или Комиссии, должно иметь соответствующий уровень проверки благонадежности[28]

Платформы для обмена информацией могут также принять специальные критерии отбора для приема новых членов, например, на основе необходимости согласия существующих участников или в форме фоновой проверки, собеседования с государственными органами, отвечающими за платформу по обмену информацией и т.д.

В некоторых случаях может возникнуть нежелание привлекать членов правоохранительных органов из-за опасений, что раскрытие определенных типов информации приведет к действиям их стороны, которые могут нанести ущерб готовности участников делиться информацией вообще. Для стратегий по ЗКВОИ важно учитывать эти потенциальные трудности и находить способы их преодоления.

ii) Системы цветового кодирования

Эти системы основаны на принципе, согласно которому тот, кто предоставляет информацию, определяет степень ее распространения. Протокол светофора (TLP) применяет эту концепцию в том смысле, что отправитель информации помечает ее одним из четырех цветов:

- *Красный:* только для именованных получателей;
- *Янтарный:* ограниченный тираж, ожидается, что отправитель определит пределы и условия обмена информацией;
- *Зеленый:* информация может распространяться внутри определенного сообщества, но не может быть общедоступной (например, в Интернете) или распространяться за пределами сообщества;
- *Белый:* неограниченная циркуляция.

Преимущество TLP заключается в его удобстве для пользователя и в установлении четких границ между обязанностями отправителя и получателя.

iii) Электронные инструменты

Чтобы обеспечить обмен информацией, некоторые платформы используют электронные инструменты, такие как экстранет, для обмена документами. Экстранет - это телекоммуникационная сеть, использующая интернет-технологии, цель которой заключается в содействии обмену между основным субъектом и двумя или более партнерами, находящимися на географическом удалении. Партнеры должны пройти аутентификацию, чтобы иметь возможность просматривать сетевую информацию.

[28] (ст. 9)

Изучение конкретной ситуации **33**
Информационный портал критически важных обьектов инфраструктуры (CI Gateway) Канады

Одной из целей национальной стратегии и плана действий по критически важной инфраструктуре (Стратегия) является своевременное улучшение обмена информацией и защиты между партнерами по КВОИ. Для достижения этой цели Стратегия призывает к созданию CI Gateway, веб-портала обмена информацией о критически важной инфраструктуре, который будет размещаться в домене общественной безопасности Канады.

В Плане действий по критически важной инфраструктуре на 2014–2017 годы признается, что в рамках первоначального Плана действий было разработано несколько механизмов обмена информацией, и мы стремимся опираться на эти достижения путем дальнейшего расширения возможностей обмена информацией с помощью различных средств, включая официальные соглашения, виртуальные и физические механизмы, создание и распространение информационных продуктов.

В соответствии с планом действий на 2014–2014 годы основными задачами в этой области являются:

Расширение членства и участия заинтересованных сторон в информационном шлюзе критически важной инфраструктуры Канады и использование возможностей шлюза КВОИ для улучшения обмена информацией и совместной работы по конкретным проектам:

Государственная безопасность Канады стремится к успешному запуску CI Gateway, гарантируя, что его членство охватывает десять секторов и других ключевых заинтересованных сторон, поощряя активное участие в членстве и способствуя его использованию отраслевыми сетями и сообществами практиков для обмена информацией и передовым опытом, а также для совместной работы над специфичными проектами;

Продвижение допусков к секретной информации среди заинтересованных сторон из частного сектора с целью обеспечения более широкого обмена конфиденциальной информацией: Часть информации, собранной канадским сообществом по безопасности и разведке, является конфиденциальной и может передаваться только лицам с соответствующим допуском. Государственная безопасность Канады стремится сотрудничать с ведущими федеральными департаментами и агентствами, чтобы увеличить число заинтересованных сторон в частном секторе.

Источники: Информационный шлюз критически важной инфраструктуры, по адресу:

https://cigatewav.ps.gc.ca/lavouts/pscbranding /trms- eng.pdf: План действий по созданию критически важной инфраструктуры на 2014–2017 годы по адресу:
www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtci-nfrstrctr-2014-17/pln-crtci-nfrstrctr-2014-17-eng.pdf

5. ОБЕСПЕЧЕНИЕ КООРДИНАЦИИ ВНУТРЕННИХ ОРГАНОВ

Резолюция Совета Безопасности 2341 (2017)
Пункт 6 постановляющей части

Совет Безопасности (...) *Настоятельно призывает все государства обеспечить, чтобы все их соответствующие национальные ведомства, агентства и другие учреждения тесно и эффективно взаимодействовали в вопросах защиты критически важных объектов инфраструктуры от террористических нападений*

5.1 Необходимость межведомственного подхода к ЗКВОИ

Различные государственные органы (законодательные органы, регулирующие органы и т. д.) устанавливают множество норм, правил и стандартов по вопросам безопасности в различных секторах КВОИ. Связанные с терроризмом сведения, которые необходимы для оценки текущих типов и уровней угрозы для КВОИ, часто собираются несколькими ведомствами, подотчетными различным министерствам. Эффективные меры по управлению кризисами и реагированию на них требуют способности нескольких государственных структур (на местном, муниципальном, региональном и национальном уровнях) исполнять свою роль быстро и без проблем. Кроме того, во многих случаях ряд объектов может быть вовлечен в данную функцию безопасности. Так обстоит дело в авиационном секторе, где компетентный орган, администрация аэропорта и правоохранительные органы могут разделить ответственность за защиту аэропортов, аэронавигационных средств и служб.

Таким образом, широкая межведомственная координация является ключевой предпосылкой для реализации адекватных уровней ЗКВОИ. Связанные стратегии должны «связать точки» между различными национальными агентствами, ответственными за действия, связанными с ЗКВОИ. Координация должна быть достигнута с заинтересованными сторонами, такими как министерства (например, связи, экономики, безопасности, кабинета министров, юстиции, внутренних дел и обороны), региональными органами и регуляторами, сотрудничающими на стратегическом, тактическом и оперативном уровнях. Однако достижение этой всеобъемлющей цели не всегда под рукой. Использование различной терминологии и профессионального языка различными субъектами, участвующими в действиях по предотвращению / защите / реагированию, а также отсутствие унифицированных процедур и каналов связи могут серьезно повлиять на качество всей работы ЗКВОИ. Также было отмечено, что «в некоторых случаях государственные органы имеют тенденцию следовать разным повесткам дня, когда речь идет о ЗКВОИ. Некоторые из них придерживаются власти рыночных сил, тогда как другие твердо верят в законодательную роль правительства. Эти различия, однако, может стать серьезным камнем преткновения для сотрудничества при взаимодействии с частным сектором». (ОБСЕ 2013, стр.68)

Изучение конкретной ситуации **34**

Федерально-провинциально-территориальная рабочая группа по критически важным объектам инфраструктуры Канады

Наряду с отраслевыми сетями и межсекторальным форумом, Национальная стратегия и план действий Канады создали рабочую группу федерально-провинциально-территориальной и критически важных объектов инфраструктуры. Этот орган предлагает пример "вертикальной" координации между властями в федеральной системе управления. Его заявленные цели:

- Поддерживать реализацию Стратегии в рамках федеральной, провинциальной и территориальной юрисдикций;
- Обеспечивать руководство и участвовать в разработке и реализации плана действий;
- Действовать в качестве центра обмена информацией для правительств по важнейшим вопросам, связанным с объектами инфраструктуры, для высокопоставленных должностных лиц федерального, провинциального и территориального уровней, отвечающих за управление в чрезвычайных ситуациях;
- Содействие федеральным / провинциальным / территориальным сетям для поддержки обмена информацией критически важных объектов инфраструктуры, управления рисками, планирования критически важной инфраструктуры и учения;
- Выявить критические проблемные моменты инфраструктуры регионального или юрисдикционного значения;
- Продвигать общее понимание критически важных объектов инфраструктурных рисков и взаимозависимостей;
- Поощрять участие в учениях для проверки планов работы по конкретным секторам и выявления новых рисков;
- Предоставить руководство по текущим и будущим проблемам, связанным с критически важными объектами инфраструктуры;
- Выявление связей между федеральными, провинциальными и территориальными программами и инициативами и содействие обмену информацией и передовым опытом.

Членство в Рабочей группе открыто для всех правительств в соответствии с их потребностями и, насколько позволяют их ресурсы. Решение принимается только после обмена информацией и предоставления всем участникам возможности комментировать. Рабочей группой сопредседательствует представитель сектора управления чрезвычайными ситуациями и национальной безопасности Канады и представитель провинции / территории, определяемый консенсусом группы.

В следующем разделе рассматриваются основные концептуальные и институциональные строительные блоки для достижения координации агентства в сценариях кризиса. В последующих разделах представлен обзор основных проблем межведомственной координации в целом и основных инструментов для их преодоления, в частности, совместных учений / обучения и решений по взаимодействию.

5.2 Координация действий органов в кризисных ситуациях

Важным аспектом межведомственной координации является способность всех заинтересованных сторон оперативно и эффективно действовать в кризисных ситуациях. Концепция антикризисного управления была введена в разделе 2.6.2. После определения основных структур и процессов антикризисного управления, стратегии по ЗКВОИ должны обеспечить бесперебойную работу в случае необходимости. Некоторые основные предпосылки для достижения гибкого и быстрого принятия решений:

- Четкое распределение ролей и обязанностей, следствием чего является то, что решения должны приниматься на самом низком соответствующем уровне, а координация - на самом высоком необходимом уровне. Можно утверждать, что «тесная интеграция операторов КВОИ в антикризисное управление требует выполнения большого набора требований. Взаимное понимание ролей, обязанностей, способностей и возможностей - это длительный процесс, требующий инвестиций с точки зрения времени, человеческого сотрудничества, обучения сленгу друг друга» (RECIPE 2011, стр.82);

- Полное понимание последствий разрушения КВОИ, включая его каскадные эффекты. В связи с этим было отмечено, что «нынешний упор на антикризисное управление в большинстве стран гораздо более сфокусирован на единичном нарушении КВОИ и его потенциальных последствиях, например, при планировании перебоя в питьевом водоснабжении, чем на каскадных сбоях и отказу по общей причине, такому как сильный шторм, вызывающий одновременное нарушение нескольких КВОИ. Рекомендуется подготовиться к отказам по общей причине и каскадным воздействиям, влияющим на несколько КВОИ одновременно» (RECIPE 2011, стр.81);

- Назначение координаторов во всех участвующих учреждениях с круглосуточной доступностью;

- Создание адекватных систем управления информацией для поддержки эффективного сбора, анализа и распространения данных в поддержку принятия единых и межведомственных решений, а также для предоставления информации населению. Организация взаимодействия должна быть разработана таким образом, чтобы минимизировать ситуации, когда принимаются противоречивые инструкции. Кроме того, в идеале системы управления информацией поддерживаются безопасными линиями связи (см. Раздел 4.3 по вопросам безопасности и защиты данных в контексте обмена информацией).

Изучение конкретной ситуации **35**
Антикризисное управление после взрыва в Лондоне в 2005 году

7 июля 2005 года в результате взрыва четырех бомб на лондонской транспортной системе были убиты пятьдесят два человека. Обстоятельства происшествия особенно усложнили координацию действий в чрезвычайных ситуациях. Как подчеркивалось в отчете судебного следователя после расследования событий, «расположение трех взрывов в туннелях означало ограниченное количество свидетелей того, что произошло. Во-вторых, связь в туннелях была ограничена. В-третьих, повсеместное нарушение, вызванное взрывами, привело к лавине входящих звонков, что вызвало перегрузку операторов радиосвязи и привело к перегрузке всей радиосвязи и телефонной связи. Потребовалось время, чтобы выявить и извлечь наиболее значимую и важную информацию из множества полученных сообщений (в дополнение к обычным ежедневным требованиям служб экстренной помощи и лондонскому метро), чтобы агентства могли реагировать соответствующим образом».

Судебный следователь обнаружил ряд недостатков в реагировании на чрезвычайные ситуации и дал несколько рекомендаций. В частности, по словам следователя, «свидетельства выявили не просто сбои в системах связи, которые имелись на местах, но и некоторые основные недоразумения между аварийными службами в отношении их соответствующих ролей и операций, например, неспособность некоторых сотрудников аварийных служб оценить и понимать обязанность со стороны персонала LAS [Служба скорой помощи Лондона] выступать в качестве сотрудников скорой помощи вместо того, чтобы принимать участие в обработке пострадавших. [...] Отдельные спасатели столкнулись с задержкой и трудностями при попытке выяснить, каков был характер инцидентов или какие ресурсы были необходимы, и имелись значительные различия в способах, которыми каждый спасатель пытался решать общие проблемы, такие как использование радиостанций там, где имелся возможный риск взрыва вторичных

устройств [...] Фактические данные свидетельствуют о необходимости пересмотра степени и масштабов межведомственной подготовки. Такая подготовка имеет жизненно важное значение для уменьшения путаницы и лучшего понимания соответствующих функций аварийных служб».

Примечательно, что в отчете отмечалось, что, хотя обучение (в форме командно-штабных или «реальных» учений) уже было широко предоставлено высшим руководящим уровням», факты также указывают на то, что межведомственной подготовки было значительно меньше для этих «передовых» сотрудников аварийных служб, которым поручено реагировать на первоначальный хаос, бойню и путаницу в крупном инциденте».

Другие рекомендации касались: межведомственной подготовки по крупным инцидентам для персонала по работе с клиентами; протоколов по обмену информацией о чрезвычайных ситуациях между TfL [Транспорт для Лондона] и службами экстренной помощи; создания и укомплектование пунктов сбора персонала; процедур подтверждения и передачи информации о том, что тяговый ток отключен на лондонском метро; предоставлению оборудования для оказания первой помощи и носилок на подземных поездах и станциях; процедур для сортировки множества пострадавших; и неотложная медицинская помощь, предоставляемая Лондонской аэрослужбой скорой помощи и бригадами неотложной медицинской помощи.

В своем докладе следователь также упомянула такие вопросы, как регулирование поставок перекиси водорода; эффективную межведомственную связь; хорошее взаимодействие и обмен информацией; базовые радиостанции AIRWAVE и их пропускная способность в случае крупного инцидента; и прозрачность между различными аварийными службами.

Источник: «Дознание судебного следователя по взрывам в Лондоне» от 7 июля 2005 года, 6 мая 2011 года, по адресу: http://image.guardian.co.uk/sys-files/Guardian/documents/2011/05/06 /rule43-report.pdf

5.3 Совместные учения / тренинги

В контексте ЗКВОИ межучрежденческие учения / тренинги повсеместно признаны в качестве важного инструмента для проведения как минимум следующих целей:

- Достичь общего понимания применимых процессов и методологий;
- Выяснить роль и ответственность в циклах защиты КВОИ;
- Укрепить уверенность персонала в выполнении инструкций и политик по защите, связанных с КВОИ (важно во время стрессовых фаз реального кризиса);
- Выявить слабые стороны и внести любые изменения, необходимые для безопасного исхода реальной аварийной ситуации;
- Гарантировать, что эксплуатационная надежность и совместимость всего оборудования связи предназначены для использования во время инцидента.

Изучение конкретной ситуации **36**
«Кибер Европа»

Под руководством ENISA, «Кибер Европа» представляет собой серию учений по управлению кибер-инцидентами и кризисами для государственного и частного секторов из стран-членов ЕС и ЕАСТ. Учения представляют собой модели крупномасштабных инцидентов в области кибербезопасности, которые перерастают в кибернетические кризисы. Они предлагают группам ИТ-безопасности, непрерывности бизнеса и управления кризисами возможности для анализа сложных случаев технической кибербезопасности и для решения сложных ситуаций непрерывности бизнеса и антикризисного управления.

Учения «Кибер Европа» начались в 2010 году и проходили каждые два года. В издании 2016 года приняли участие более 1000 участников. Следующий запланирован на 2018 год.

Источник: Агентство Европейского Союза по Сетевой и Информационной Безопасности (ENISA), по адресу: www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-program

Межведомственное может происходить на обязательной или добровольной основе в зависимости от обстоятельств. Страны применяют различные формы учений в зависимости от поставленных целей, числа участвующих субъектов и участников, наличия ресурсов и т. д.

Изучение конкретной ситуации **37**
Обучение, подготовка и тренировка в соответствии с кодексом ISPC

Международный кодекс по охране судов и портовых средств (Кодекс ISPS) предусматривает обязательное обучение и учения в рамках мер, необходимых для углубления понимания заинтересованными сторонами своих соответствующих обязанностей и обязательств, связанных с безопасностью (разделы 13 и 18 Кодекса).

В частности, учения должны предусматриваться через соответствующие промежутки времени. Что касается безопасности судна, учения должны учитывать «тип судна, смены персонала судна, посещаемые портовые сооружения и другие соответствующие обстоятельства» (Раздел 13.3.) В отношении безопасности портовых объектов учения должны принимать во внимание «типы работы портового объекта, смену персонала портового объекта, тип судна, которое обслуживает портовый объект, и другие соответствующие обстоятельства» (раздел 18.3).

Во всех случаях учения и тренировки должны учитывать инструкции, приведенные в части В самого Кодекса ISPS.

Украинский институт стратегических исследований составил перечень наиболее распространенных видов учений и их основных применений (Украина, 2017, стр. 110). Среди них можно отметить следующие:

- *Семинары:* дать общее руководство по существующим стратегиям, планам, политике, процедурам, протоколам, ресурсам и концепциям;
- *Командно-штабные учения (ТТХ):* для обсуждения гипотетической, смоделированной чрезвычайной ситуации. ТТХ полезны для облегчения концептуального понимания, определения сильных сторон и областей для улучшения и достижения изменений в восприятии;
- *Симуляторы (Игры):* для изучения последствий решений и действий игрока. Этот тип учений часто основан на создании конкурентной среды, в которой две или более команды сталкиваются друг с другом в реальных ситуациях;
- *Тренировочные учения:* проводить обучение на новом оборудовании, проверять процедуры или практику и поддерживать текущие способности. Тренировочные учения основаны на понятии обучения и совершенствования навыков посредством повторения задач;

- *Полномасштабный (в реальном времени):* для предоставления участникам сценариев, предназначенных для отражения реальных ситуаций, требующих от них действий и реагирования в реальном времени.

Важно отметить, что некоторые из учений, упомянутых ниже, особенно те, в которых задействовано большое количество участников и которые основаны на сложных имитациях в реальном времени, требуют тщательного планирования и зачастую месяцев, если не лет, подготовки.

Изучение конкретной ситуации **38**
«Прочная устойчивость 2017» Украины

«Прочная устойчивость 2017» - это командно-штабное учение, спонсируемое НАТО, призванное повысить устойчивость критически важной энергетической инфраструктуры Украины.

Учение направлено на:

- проверку существующих процедур по предотвращению, защите и реагированию на инциденты, связанные с энергетическим сектором;
- содействие межведомственному сотрудничеству в повышении устойчивости национальной энергетической системы, включая международные усилия по решению возникающих проблем безопасности.
- в «Прочной устойчивости 2017» приняли участие двадцать правительственных организаций, в том числе более ста человек, которые занимались планированием и выполнением учений в четырех рабочих направлениях: кибер / терроризм, антикризисное управление, стратегические коммуникации и реагирование международных организаций. Среди участников были, среди прочего, сотрудники правительственных учреждений и министерств в области энергетики, аварийных служб и национальной безопасности, а также военный персонал, национальная полиция и другие учреждения, и органы, отвечающие за защиту и повышение устойчивости в критически важном секторе электроснабжения.

Различные сценарии были разработаны, чтобы побудить участников:

- анализировать уязвимости критической энергетической инфраструктуры на основе выявленных рисков и угроз;
- определить последствия отказа, атаки и / или повреждения критически важной энергетической инфраструктуры и воздействия на другие связанные показатели общества;
- определить сотрудничество и координацию между учреждениями, агентствами и организациями, создающими аварийные службы, и оценить их планы;
- использовать процессы управления кризисами, включая военное и гражданское чрезвычайное планирование, в качестве реакции на условия, спровоцированные гибридными средствами в предконфликтных, конфликтных и постконфликтных ситуациях.

Источник: Украина 2017

5.4 Продвижение взаимодействующих процессов и решений

Ключевой концепцией межведомственной координации является «функциональная совместимость». Она может быть операционной / функциональной или технической. Канадская стратегия по химической, биологической, радиологической, ядерной и взрывчатой устойчивости определяет оба аспекта следующим образом:

«(1) *Операционная / функциональная возможность взаимодействия* - это способность эффективно работать вместе. В частности, это способность различных юрисдикций или направлений предоставлять услуги и принимать услуги из других юрисдикций или направлений скоординированным образом, а также использовать эти услуги для более эффективной совместной работы в чрезвычайной ситуации. С практической точки зрения эксплуатационная совместимость означает, что персонал из разных юрисдикций или служб выступает в качестве команды под общей структурой командования и управления.

(2) *Техническая возможность взаимодействия* - это способность общаться и обмениваться информацией, а также интегрировать оборудование и технические возможности. Это способность систем обеспечивать динамический интерактивный обмен информацией и данными между элементами командования, управления и связи для планирования, координации, интеграции и выполнения операций реагирования» (Канада 2005).

В контексте межведомственной координации возможность полагаться на совместимые процессы представляется особенно важной для связи в чрезвычайных ситуациях. В связи с этим было отмечено, что «этот вопрос [...] вызывал обеспокоенность почти все время, пока службы первой помощи и другие должностные лица в сфере общественной безопасности пользовались радио. Однако это было не так до 11 сентября 2001 года, когда произошла террористическая атака всемирного торгового центра, в результате которой совместимость была повышена с продолжительной озабоченности до критически важного национального приоритета. Одна из величайших трагедий 11 сентября 2001 года произошла из-за невозможности эффективно передавать предупреждения пожарному персоналу о возможном обрушении башен, и что им нужно было немедленно эвакуироваться. Многие эксперты сходятся во мнении, что неспособность радиосистемы пожарной охраны эффективно взаимодействовать с другими учреждениями или даже между новыми и более старыми моделями радиосвязи, стала главным образом причиной гибели 343 пожарных (Federal Signal 2013).

Использование систем возможного взаимодействия является ключевым не только для того, чтобы позволить полиции и другим службам реагирования (полиции, пожарно-спасательным службам, службам скорой помощи и т. д.) общаться друг с другом для координации действий, но также и для того, чтобы они могли оптимизировать ресурсы при составлении бюджета и планировании меры по ликвидации последствий стихийных бедствий и восстановлению.

5.5 Преодоление культурных барьеров

В то время как принятие совместимых решений и отлаженных / единообразных процессов может иметь большое значение для преодоления обособленности и содействия межведомственной координации, факт остается фактом, что защита КВОИ зависит от повседневной работы людей с самыми разнообразными техническими и профессиональными составляющими. Разные виды мировоззрения могут основываться на разных терминологиях, методологических подходах и способах организации работы.

Степень, в которой культурные различия между участниками КВОИ могут препятствовать достижению оптимальных уровней сотрудничества, была рассмотрена с особым вниманием в Швеции в рамках подхода всей страны к устойчивости КВОИ и, в большей степени, в целом, социальной безопасности. Соответственно, исследование, посвященное устойчивости к стихийным бедствиям, выделило ряд профессиональных отношений, связанных с защитой КВОИ, и проанализировало конкретные культурные проблемы, связанные с каждым из них. В исследовании, например, подчеркивался разрыв между специалистами в области безопасности и охраны в том, как эти две группы управляют информацией. Хотя сотрудники службы безопасности привыкли обращаться с секретной информацией в ограниченных кругах людей, сотрудники службы безопасности, как правило, полагаются на открытые источники и не видят роли конфиденциальной информации. Тем не менее, «поскольку угрозы становятся все более сложными, когда поначалу может быть трудно определить событие как явную «нормальную» аварию или как террористический акт, необходимо хорошо и заранее развивать тесное сотрудничество, например, между полицейскими силами и службами экстренного реагирования» (Lindberg & Sundelius 2013, с.1301).

В то время как определенные различия в поведении могут быть обнаружены вдоль разрыва между гражданскими и военными, в исследовании отмечаются более явные препятствия для координации гражданско-гражданских отношений, главная причина в том, что «роли и обязанности в сложной гражданской сфере часто бывают менее четкими, а иногда даже частично совпадают. По мере развития угроз правила и процедуры могут отсутствовать или устареть. Линии юрисдикции могут рассматриваться как дополнительные или конкурирующие. Некоторое сопротивление для координации может быть обнаружено, и одной из причин, вероятно, является то, что взаимодействия с целью изменения поведения могут быть очень чувствительными среди гордых профессионалов» (Lindberg & Sundelius 2013, стр. 1300-1301).

Опыт и представления других стран могут значительно различаться в зависимости от конкретных институциональных, социальных и экономических структур, в которых действуют их различные профессии. Не обязательно стремясь «унифицировать» глубоко укоренившееся поведение, каждая страна может пожелать повысить осведомленность об этих проблемах и найти пути (например, путем открытого и регулярного обсуждения этих вопросов на совместных тренингах), чтобы гарантировать, что они в конечном итоге не ставят под угрозу продолжающиеся усилия, связанные с затратами времени и ресурсов, учитывая усилия по достижению устойчивости КВОИ.

6. УЛУЧШЕНИЕ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА ПО ЗАЩИТЕ КВОИ

Резолюция Совета Безопасности 2341 (2017)
Пункты 8 и 9 постановляющей части

Совет Безопасности (...)

8. Подтверждает, что инициативы в области регионального и двустороннего экономического сотрудничества и развития играют ключевую роль в достижении стабильности и процветания, и в этой связи призывает все государства расширять свое сотрудничество в целях защиты критически важных объектов инфраструктуры, в том числе региональных проектов развития сообщения и связанных с ними объектов трансграничной инфраструктуры, от террористических нападений путем использования, сообразно обстоятельствам, двусторонних и многосторонних механизмов обмена информацией, оценки рисков и совместной правоприменительной деятельности;

9. Настоятельно призывает все государства, которые в состоянии делать это, оказывать содействие в обеспечении эффективного и целенаправленного наращивания потенциала, профессиональной подготовки и других необходимых ресурсов, технической помощи, передачи технологий и реализации программ, когда это требуется, с тем чтобы все государства могли достичь цели защиты критически важных объектов инфраструктуры от террористических нападений;

6.1 Аспекты международного сотрудничества по ЗКВОИ

Одним из наиболее ярких проявлений глобализации является интернационализация цепочек поставок, будь то для доставки критически важных или не важных продуктов и услуг. Следовательно, взаимозависимости КВОИ и взаимосвязанность пересекают границы. Риски для стран с критически важными объектами инфраструктуры могут возникать в соседних (особенно в случае общей физической инфраструктуры) или очень отдаленных странах (особенно в случае кибератак). В случае кризиса ИКТ даже возможно, что чрезвычайная ситуация, разворачивающаяся в одной стране, может быть решена только в другой стране, которая, в свою очередь, не затронута напрямую.

Потенциальные сценарии, иллюстрирующие необходимость прочного включения международного сотрудничества в стратегии стран по ЗКВОИ, включают следующее:

- Две или более стран имеют одинаковый тип критически важных объектов инфраструктуры (трансграничные КВОИ);
- КВОИ, находящийся в одной стране, полностью или частично зависит от продуктов, услуг, технологий и т. д., поставляемых другой страной;
- Нарушения или аномалии в функционировании КВОИ, расположенного в одной стране, оказывают влияние на другие страны.

Текущие уровни международного сотрудничества по ЗКИ существенно различаются в зависимости от потребностей и восприятия страны. Оно может быть более или менее широким по объему в зависимости от конкретного типа действующих договоренностей, близости стран и уровней экономической интеграции.

При рассмотрении планов новых или усиленных трансграничных партнерств по ЗКВОИ, странам следует рассмотреть ряд областей. Как показывают тематические исследования в следующих разделах, усилия по международному сотрудничеству обычно сосредоточены на обмене информацией, регулировании кризисов и совместных учениях. Некоторые забытые области - международное правоохранительное и судебное сотрудничество по уголовным делам. Эти последние формы

международного сотрудничества, возможно, не служат исключительно целям ЗКВОИ, но остаются существенными компонентами в ответных мерах государства на террористические нападения на КВОИ. Поскольку резолюция 2341 (2017) Совета Безопасности требует установления уголовной ответственности, применение эффективных мер наказания неотделимо от необходимости того, чтобы страны полагались на эффективные каналы международного сотрудничества в области уголовного правосудия.

В этом контексте Интерпол I-24/7 предоставляет глобальную платформу для взаимодействия между правоохранительными органами. Система объединяет сотрудников правоохранительных органов во всех 192 странах-членах Интерпола и позволяет авторизованным пользователям обмениваться конфиденциальной и срочной полицейской информацией в безопасной среде со своими коллегами по всему миру 24 часа в сутки, 365 дней в году. I-24/7 - это сеть, обеспечивающая доступ к базе криминальных данных Интерпола. Авторизованные пользователи могут осуществлять поиск и перекрестную проверку данных в течение нескольких секунд, имея прямой доступ к базам данных о подозреваемых преступниках или разыскиваемых лицах, похищенных и утерянных проездных документах, угнанных транспортных средствах, отпечатках пальцев, профилях ДНК, похищенных административных документах и похищенных произведениях искусства. Установив I-24/7 во всех национальных центральных бюро, Интерпол в настоящее время сосредоточен на расширении доступа к услугам Интерпола за пределами NCB и внешним сотрудникам, таким как сотрудники иммиграционных и таможенных служб.

Изучение конкретной ситуации **39**
Международный обмен информацией об угрозах в области гражданской авиации

В авиационном секторе важным аспектом обмена информацией является обмен информацией об угрозах. В руководстве по безопасности ИКАО (документ Doc 8973 ограничен) рекомендуется устанавливать официальные и неофициальные линии связи между должностными лицами по авиационной безопасности государств для оказания помощи в быстром обмене информацией, включая любое повышение уровня угрозы. Обмен информацией о методах, используемых для попытки нарушения безопасности, опыте работы с оборудованием для обеспечения безопасности и методах эксплуатации, также чрезвычайно выгоден.

Формальные процедуры обмена информацией между определенными ответственными должностными лицами, включая публикацию списка телефонных номеров, уличных адресов, номеров телекса и факсимильной связи, а также адресов электронной почты и аэронавигационная служба стационарных средств связи (AFS), должны быть доступны для связи во время серьезного инцидента. Государствам следует разработать процедуры анализа и распространения информации об угрозах и обеспечить принятие соответствующих мер операторами воздушных судов и аэропортами для противодействия выявленной угрозе. Информация должна распространяться, когда это необходимо отдельным лицам для эффективного выполнения своих обязанностей, то есть принципа необходимости знать.

Государствам, имеющим ограниченные ресурсы для противодействия неминуемым угрозам или актам незаконного вмешательства, следует рассмотреть вопрос о проведении переговоров о правовой и процедурной помощи с соседними государствами, которые лучше оснащены для сбора и распространения информации об угрозах и инцидентах.

Запросы государства об особых мерах безопасности для конкретного рейса должны удовлетворяться при необходимости. Для обеспечения того, чтобы таким запросам уделялось надлежащее внимание, государствам следует определить процедуры и представителей правительства, воздушных судов и эксплуатантов аэропортов, которые должны знать об угрозе. Кроме того, параметры специальных мер безопасности, ответственность за дополнительные расходы и сроки начала действий должны быть согласованы с заинтересованным эксплуатантом воздушного судна и / или аэропортами.

Срочное взаимодействие может быть облегчено посредством использования сети центров безопасной связи в авиации (PoC) ИКАО, созданной для информирования о непосредственной угрозе гражданским воздушным перевозкам, в соответствии с мнениями, высказанными Римско-Лионской

группой «большой восьмерки» по борьбе с преступностью и противодействием терроризму. В соответствии с резолюцией A39-18 Ассамблеи: сводное заявление о постоянной политике ИКАО в области авиационной безопасности государствам, которые еще не сделали этого, настоятельно рекомендуется принять участие в сети PoC ИКАО. Цель Сети PoC ИКАО - предоставить подробную информацию о контактах по международной авиационной безопасности в каждом государстве, которые назначены в качестве соответствующего органа для отправки и получения сообщений в любое время дня и ночи, касающихся информации о непосредственной угрозе, запросов безопасности срочного характера и / или руководящих принципов для поддержки требований безопасности, чтобы противостоять надвигающейся угрозе. Центры контакта должны быть доступны в любое время, участвовать в процессе оценки угроз и быть близкими к процессу принятия решений по процедурам авиационной безопасности.

Источник: ИКАО, Руководство по безопасности, документ 8973, ограниченный доступ

6.2 Основные трансграничные инициативы

За последние несколько лет возросшее осознание того, что взаимозависимости КВОИ не прекращаются на государственных границах, способствовало заключению ряда международных соглашений и партнерств. Ввиду экономического веса участвующих стран и наличия очень сложных инфраструктурных сетей, связывающих их, в этом разделе рассматриваются структура ЕС и договоренности о сотрудничестве между США и Канадой на местах.

6.2.1 Европейский Союз

Усилия по обеспечению того, чтобы 27 стран-членов ЕС разработали общую стратегию, касающуюся ЗКВОИ, начались в 2005 году. По запросу Европейского совета Комиссия приняла Зеленую книгу, содержащую ряд вариантов политики по созданию программы ЗКВОИ. Полученные отзывы показали дополнительную ценность структуры Союза в этой области. В апреле 2007 года Совет заявил, что государства-члены несут главную ответственность за организацию мероприятий по ЗКВОИ в пределах своих национальных границ. В то же время он приветствует усилия Комиссии по разработке европейской процедуры идентификации и обозначения европейских критически важных объектоы инфраструктур (ECI). Нынешний подход ЕС в настоящее время закреплен в директиве 2008 года, в которой ECI определяется как «критически важный объект инфраструктуры, расположенный в государствах-членах, нарушение или разрушение которой окажет значительное влияние как минимум на два государства-члена. Значимость воздействия должна оцениваться с точки зрения комплексных критериев. Это включает эффекты, возникающие в результате межотраслевых зависимостей от других типов инфраструктуры» (статья 2b).

Важно отметить, что Директива концентрируется на энергетическом и транспортном секторах. Более того, она призвана дополнить, а не заменить существующие секторальные меры на уровне Союза и в государствах-членах. Там, где механизмы Союза уже существуют, они должны продолжать использоваться и будут способствовать общему осуществлению настоящей Директивы.

Процесс квалификации для ECI следует за несколькими шагами, которые включают обязанность государств-членов:

- Информировать другие государства-члены о потенциальных КВОИ, расположенных на его территории и влияющих на них, и вовлекать их в двусторонние или многосторонние дискуссии;

- Определить такие объекты инфраструктуры как ECI после соглашения с заинтересованными государствами-членами;
- Ежегодно информировать Комиссию о количестве квалифицированных КВОИ для каждого сектора и о количестве государств-членов, зависящих от каждого квалифицированного КВОИ;
- Сообщать заинтересованному владельцу / оператору, что его инфраструктура была квалифицирована как ECI;
- Проверить, что указанные ECI имеют План безопасности оператора (OSP), и что этот план регулярно анализируется;
- Проверить, что каждый ECI назначает сотрудника по связям с безопасностью в качестве координационного центра между ECI и соответствующим органом государства-члена;
- Провести оценку угроз в отношении подсекторов ECI в течение одного года после определения критически важной инфраструктуры на ее территории в качестве ECI в этих подсекторах;
- Каждые два года сообщать Комиссии общие данные на суммарной основе о типах рисков, угроз и уязвимостей, встречающихся в каждом секторе ECI, в котором ECI было квалифицировано;
- Назначить «Европейский контактный центр по защите критически важной инфраструктуры» (ECIP) для координации вопросов европейской защиты критически важных объектов инфраструктуры внутри страны, с другими государствами-членами и с Комиссией.

В 2013 году оценка состояния выполнения Директивы 2008 года выявила смешанную ситуацию. В то время как наличие общеевропейских рамок по ЗКВОИ было однозначно принято в качестве приоритета, обозначился ряд проблем. В частности, было отмечено, что «квалифицировано менее 20 европейских критически важных объектов инфраструктур и, следовательно, разработано очень мало новых планов безопасности операторов. Некоторые четкие критически важные объекты инфраструктуры европейского измерения, такие как основные сети передачи энергии, не включены. Несмотря на помощь в укреплении европейского сотрудничества в процессе ЗКВОИ, Директива в основном поощряла двустороннее участие государств-членов вместо реального европейского форума сотрудничества. Секторно-ориентированный подход Директивы также представляет собой проблему для ряда государств-членов, так как на практике анализ критичности не ограничивается отраслевыми границами и следует скорее «системному» или «сервисному» подходу (например, больницы, финансовые услуги)» (Европейская Коммиссия 2013 bis).

Соответственно, в 2013 году Европейская комиссия предложила переориентировать действие ЗКВОИ в новом, более практическом направлении, которое в основном переключилось бы с отраслевого подхода на системный. Новый подход начинается с пилотного проекта, нацеленного на оценку рисков, уязвимостей и мер по ЗКВОИ, реализованных четырьмя ECI, а именно: 1) сеть электропередач ЕС; 2) газотранспортная сеть ЕС; 3) EUROCONTROL; 4) GALILEO (Европейская программа глобальной спутниковой навигации).

Европейская комиссия предусматривает пилотный этап для предоставления «необходимых показателей, позволяющих сформировать подход ЕС по ЗКВОИ. Он будет основан на достигнутых результатах и пробелах, выявленных в результате работы с «четверкой», и будет стремиться предоставить полезные инструменты для улучшения защиты и устойчивости, в том числе посредством обеспечения более эффективных мер по снижению риска, обеспечения готовности и реагирования [...] Следующим шагом может стать внедрение этого подхода в регионах, где государства-члены заинтересованы в сотрудничестве друг с другом. Примеры могут включать концепцию устойчивости для всей критически важной транспортной инфраструктуры вокруг Балтийского моря и программы обеспечения критичности цепочки поставок в Дунайском регионе» (Европейская комиссия 2013 bis).

Изучение конкретной ситуации **40**
AIRPOL (авиа полиция) и RAILPOL (ж/д полиция)

Трансграничное сотрудничество по защите КВОИ в европейских странах не ограничивается рамками, установленными Директивой 2008 года. Это также происходит на форумах, которые, хотя и не посвящены конкретно защите КВОИ, в значительной степени способствуют достижению этой цели. Транспортный сектор, благодаря мероприятиям, осуществляемым авиа и ж/д полицией, предлагает два соответствующих примера.

AIRPOL, созданный в 2011 году, является координирующим органом правоохранительных органов в европейских аэропортах. Его задача - повысить общую безопасность в области гражданской авиации путем:

- Оптимизации эффективности и результативности работы правоохранительных органов и пограничных служб в аэропортах и авиации;
- Содействия более согласованному подходу к обеспечению соблюдения в этой области.

AIRPOL работает вокруг трех типов результатов:

- Создание постоянной и функциональной сети, ориентированной на обмен передовым опытом, разведывательными данными, общей информацией и персоналом в будущем в нескольких областях;
- Координация высокоэффективных трансграничных мероприятий
- Создание консультативной роли в качестве представительного органа экспертов

RAILPOL - это международная сеть организаций, ответственных за охрану железных дорог в государствах-членах ЕС. Ее целью является укрепление и интенсификация международного сотрудничества железнодорожной полиции в Европе, предотвращение угроз и обеспечение эффективности мер по борьбе с трансграничной преступностью. RAILPOL состоит из представителей организаций, ответственных за железнодорожную полицию в государствах-членах ЕС.

6.2.2 Канадско-американское сотрудничество

Граница Канады и США не только самая длинная в мире, помимо этого, в Канаде более 90% населения проживает в пределах 160 км от этой границы. Добавьте к этому тот факт, что несколько нефтеперерабатывающих заводов, атомных электростанций, крупных производственных предприятий и других КВОИ расположены близко к границе. Основным последствием является наличие большого числа зависимостей и трансграничных инфраструктур, защита которых в решающей степени зависит от инициатив двустороннего сотрудничества.

Основным инструментом трансграничного сотрудничества по ЗКВОИ является План действий Канады-США 2010 года. Хотя План основан на существующих секторальных договоренностях о сотрудничестве между двумя странами, стимулы для комплексного подхода в основном проистекают из:

- Необходимости поддерживать тесное сотрудничество с частным сектором через границу;
- Необходимости избегать дублирования усилий, которые неизбежны при использовании чисто отраслевых подходов;
- Необходимости повышения своевременности и точности общения с заинтересованными сторонами по КВОИ, как внутри страны, так и за ее пределами.

План действий Канада-США структурирован вокруг трех целей: i) Партнерство для обеспечения устойчивости критически важной инфраструктуры; ii) Обмен информацией; iii) Управление рисками.

i) Партнерство для обеспечения устойчивости критически важных объектов инфраструктуры

Методология, используемая для достижения этой цели, заключается в использовании существующих организационных и партнерских структур. В состав такой структуры входит Консультативная группа по чрезвычайным ситуациям (EMCG), созданная в соответствии с Соглашением между Канадой и США 2008 года о сотрудничестве в области управления чрезвычайными ситуациями 2008 года для обеспечения центрального контроля в поддержку совместного управления чрезвычайными ситуациями. Одна из рабочих групп, созданных в рамках EMCG, занимается конкретно КВОИ и была определена для «обеспечения направления и преемственности для поддержки плана действий Канада-США».

В соответствии с этой целью План действий также предусматривает «обеспечение механизмов и возможностей для отраслевых и правительственных координационных советов США и канадских отраслевых сетей для совместной работы по улучшению трансграничного сотрудничества в конкретных секторах». Кроме того, в Плане действий была создана виртуальная ячейка анализа рисков критически важной инфраструктуры Канада-США (VRAC) для «разработки и производства аналитических продуктов для совместной работы с трансграничным применением».

ii) Обмен информацией

В соответствии с этой целью две страны, в частности, обязались работать вместе, чтобы:

- Разрабатывать совместимые механизмы и протоколы для защиты и обмена важной информацией критически важных объектов инфраструктуры

- Определить требования к информации в государственном и частном секторах для поддержки разработки ценных аналитических продуктов;

- Обеспечить эффективный обмен информацией во время и после инцидента, затрагивающего критически важные объекты инфраструктуры.

iii) Управление рисками

В соответствии с Планом действий, управлению рисками по КВОИ обязывает обе страны «работать вместе для оценки рисков и разработки планов для решения приоритетных областей. Подпрограммы будут определены после тщательного анализа приоритетов каждой страны с учетом риска и определения областей взаимной заинтересованности».

6.2.3 Интерпол

В марте 2016 года Интерпол выпустил и разослал всем своим государствам-членам записку по оперативной информации, озаглавленную *«Беспилотные летательные аппараты (БПЛА) представляют растущую угрозу для критически важных объектов инфраструктуры и других уязвимых объектов»*. В записке делается вывод, что «поскольку БПЛА становятся все более популярными, дешевыми и легкими в приобретении и использовании, это лишь вопрос времени, когда эти устройства будут более широко использоваться в преступных целях (...). Правоохранительные органы во всем мире не оборудованы для борьбы с угрозой БПЛА». Действительно, в сообщениях говорится, что ИГИЛ использовало беспилотники в качестве устройства рассеивания взрывчатых веществ и для целей наблюдения в Сирии и Ираке. В записке также рекомендуется, что «правоохранительным органам следует рассмотреть возможность использования БПЛА, если они еще этого не делают, в качестве мультипликатора силы для борьбы не только с БПЛА, используемыми в нечистоплотных целях, но и для оказания помощи в расследованиях, особенно инцидентах с бомбами,

управлении ХБРЯ/HAZMAT (опасны вещества или предметы), контроле толпы, реагированию на чрезвычайные ситуации и стихийные бедствия и другие повседневные действия полиции».

Параллельно, хотя и актуально, Интерпол обеспечивает председательство в Рабочей группе целевой группы по осуществлению контртеррористических мероприятий Организации Объединенных Наций (ЦГОКМ ООН) по «Защите критически важных объектов инфраструктуры, уязвимых целей, безопасности интернета и туризма». В этих рамках несколько международных организаций и государств-членов указали на растущую угрозу использования беспилотников террористами и преступниками, не имея надлежащей правовой базы или оперативных возможностей для противодействия ей.

В ответ на это в октябре 2017 года инновационный центр Интерпола (IC) и Контртеррористический отдел (CTD) провели «1-е заседание рабочей группы по исследованию и расследованию беспилотников», в котором приняли участие 42 участника из 20 стран. Участники были в основном из правоохранительных органов, с 16% посетителей из частного сектора и научных кругов. Рабочая группа служила форумом для обмена информацией по актуальным вопросам и возникающим тенденциям, связанным с использованием беспилотных летательных аппаратов, такими как угроза беспилотных летательных аппаратов в тюрьмах, использование беспилотных летательных аппаратов террористами, контрмеры против беспилотников, подход с использованием инструментов криминалистической экспертизы, беспилотники для криминалистической экспертизы.

Интерпол действительно имеет уникальную возможность предоставить глобальную и нейтральную правоприменительную платформу, объединяющую экспертов из правительств, промышленности, научных кругов и частного сектора, чтобы помочь странам-членам в решении этой возникающей угрозы. Кроме того, эта инициатива будет представлять собой ведущую инициативу Интерпола и ее вклад в международное сообщество в рамках ответственности Организации в рамках РГ ЦГОКМ ООН по защите критически важных объектов инфраструктуры.

Программа планируется для запуска и базируется в IGCI Интерпола, Сингапур, и реализуется в тесном сотрудничестве с инновационным центром Организации, но в соответствии с мандатом CTD Организации и ее Подразделения по ХБРЯ и уязвимым целям. Это также увенчает специальные усилия, которые до сих пор предпринимались инновационным центром Интерпола, и отвечает за миссию и мандат прерогативы CTD по защите критически важной инфраструктуры (Ссылка на глобальную контртеррористическую стратегию Интерпола, канал действий 4.6 «Улучшение способности стран-членов защищать свою критически важные объекты инфраструктуры и уязвимые объекты от физических и кибертеррористических атак».

6.2.4 Другие инициативы

В последние несколько лет наблюдается рост числа инициатив, направленных на трансграничное измерение ЗКВОИ, как на субрегиональном, так и на межрегиональном уровнях.

В качестве примера субрегиональных инициатив стоит упомянуть сотрудничество в области управления чрезвычайными ситуациями в Северных странах. «Усиленная версия» этой операционной платформы была согласована в 2009 году, связав Данию, Швецию, Исландию, Норвегию и Финляндию. Инициатива построена вокруг ряда рабочих групп, которые ежегодно отчитываются перед компетентными министрами. В 2011 году была создана новая рабочая группа для устранения уязвимостей и перспектив совместной оперативной готовности в кибер-области. Конкретные направления сотрудничества включают в себя: спасательные службы; учения и обучение; готовность по ХБРЯ; кризисные порталы; набор добровольцев; исследования и разработки; тактическая противопожарная защита; стратегические воздушные перевозки в места стихийных бедствий; стратегический воздушный транспорт; поддержка принимающей страны.

С межрегиональной точки зрения проблема защиты КВОИ была объектом ежегодных встреч экспертов между ЕС и США, ЕС и Канадой. Как подчеркивалось в документе Комиссии 2013 года, «на этих заседаниях обсуждалась главным образом необходимость укрепления сотрудничества путем обмена знаниями, передовым опытом и информацией о ЗКВОИ, включая разработку инструментария для обеспечения глобальной безопасности объектов инфраструктуры. [...] На будущих совещаниях мы сосредоточим внимание на избранных темах, которые считаются все более важными для ЗКВОИ с точки зрения международного измерения, а именно: взаимозависимости за рубежом; взаимосвязи критически важной инфраструктуры; возможности глобальных каскадных эффектов; взаимозависимости физической и кибер-инфраструктуры» (Европейская комиссия 2013 bis, стр. +0,6).

6.3 Трансграничная техническая и финансовая помощь

ЗКВОИ не только требует значительных ресурсов в разных фазах и объемах, но также требует высокого уровня знаний в нескольких областях. Хотя ЗКВОИ действительно является приоритетом для всех стран, необходимые ресурсы и междисциплинарные навыки не всегда доступны во всех из них. С учетом этого составители резолюции 2341 (2017) Совета Безопасности прямо «настоятельно призывают [...] государства, способные сделать это, оказать помощь в обеспечении эффективного и целевого развития потенциала, подготовки кадров и других необходимых ресурсов, технической помощи, обмена технологиями и программами, где это необходимо, чтобы все государства могли достичь цели защиты критически важных объектов инфраструктуры от террористических атак».

В соответствии с этим, в области гражданской авиации, ИКАО призывает государства с ограниченными ресурсами для борьбы с неизбежными угрозами «рассмотреть вопрос о проведении переговоров о правовой и процедурной помощи с соседними государствами, которые лучше оснащены для сбора и распространения информации об угрозах»[29].

Конкретные правовые рамки для трансграничной технической и финансовой помощи предоставляются ЕС в отношении стран, не входящих в ЕС, в области антикризисного управления[30]. Конкретными целями являются:

- в ситуации кризиса или зарождающегося кризиса быстро содействовать стабильности путем обеспечения эффективного реагирования, призванного помочь сохранить, создать или восстановить условия, необходимые для надлежащего осуществления внешней политики и действий Союза [...];
- содействовать предотвращению конфликтов и обеспечению потенциала и готовности к урегулированию до и посткризисных ситуаций и построению мира;
- устранение конкретных глобальных и трансрегиональных угроз миру, международной безопасности и стабильности.

Важно отметить, что вышеупомянутая техническая и финансовая помощь может, в частности, включать «поддержку мер, необходимых для начала восстановления и реконструкции ключевых объектов инфраструктуры, жилья, общественных зданий и экономических активов, а также необходимых производственных мощностей, а также другие меры по восстановлению экономической деятельности, созданию рабочих мест и минимальных условий, необходимых для устойчивого социального развития».

Помимо той помощи по урегулированию кризисов, которая предусмотрена вышеупомянутым нормативным документом, страны могут также предусмотреть оказание помощи странам на этапе планирования для повышения устойчивости КВОИ. Это может, в частности, принять форму передачи знаний / «ноу-хау» в отношении различных циклов ЗКВОИ, от оценки рисков до создания соответствующей структуры управления. В соответствии с этим, в области КИИ, «Меридианный процесс» выдвинул предложение, согласно которому «странам с менее развитой политикой и деятельностью могут предлагаться ресурсы и знания, и они могут учиться у [руководства или стран-партнеров] в отношении ценных организационных или технологически целесообразных подходов и о ловушках, которых следует избегать. Таким образом, их ЗКВОИ может быть более быстрой, чем идти по пути в одиночку [...]. Предложения стать страной-ориентиром, когда страна опережает другие страны на пути ЗКВОИ, также приносит пользу. Страна-партнер может задавать вопросы по ЗКВОИ , которые страна-ориентир еще не рассмотрела. Более того, усиленная ЗКВОИ в стране-партнере создает более безопасный узел КИИ в киберпространстве. В то же время страны-ориентиры должны обеспечить, чтобы вся необходимая координация и авторизация были предприняты соответствующими министерствами и ведомствами в своих странах, прежде чем подходить к потенциальному партнеру. Однако можно начать с неформального обсуждения партнеров,

[29] Руководство по безопасности (Doc 8973-ограниченный доступ).
[30] Регламент (ЕС) № 230/2014, устанавливающий инструмент, способствующий стабильности и миру, по адресу: http://ec.europa.eu/dgs/fpi/documents/140311_icsp_reg_230_2014_en.pdf

чтобы установить совместимость и взаимные интересы, прежде чем каждая нация решит развивать более формальные дружеские отношения» (GFCE-Meridian 2016, стр.53).

7. ОТРАСЛЕВЫЕ МЕЖДУНАРОДНЫЕ ИНИЦИАТИВЫ

В этой главе представлен обзор ключевых инициатив, предпринятых учреждениями системы ООН в выбранном количестве секторов КВОИ. Ни список секторов, ни описанные инициативы не стремятся быть всеобъемлющими. Цель состоит скорее в том, чтобы направить читателей к ресурсам и инструментам, которые могут помочь им в разработке надежных отраслевых планов по ЗКВОИ в контексте более широких национальных стратегий.

7.1 Морская отрасль

Являясь ведущим международным агентством в этой области, ИМО решает вопросы защиты КВОИ, в том числе от террористических актов, в рамках своих инициатив по защите гражданской морской отрасли. Это включает в себя как судоходство, так и портовые секторы. Что касается последних, в частности, «в то время как многие страны рассматривают порты как [...] критически важный объект инфраструктуры, без четкого национального и местного законодательства, политики и руководства, координирующих всю эту деятельность, меры безопасности в лучшем случае [являются] фрагментированными. Для успеха режимов безопасности портов и портовых объектов - будь то для противодействия кражам или предотвращению доступа террористов к судам - (является) хорошо скоординированная профилактическая стратегия, основанная на оценке риска»[31]. Для решения этих проблем «ИМО [разработала] ряд руководств, инструментов для самооценки и учебных материалов для защиты портов, кораблей и морских объектов. По мере развития угроз ИМО сосредоточивается на ответных усилиях по борьбе с терроризмом, заменяя акцентом на профилактические меры [...], чтобы безопасность на море и обеспечение соблюдения законов в морском праве рассматривались как вопросы департаментов - для военно-морского флота, береговой охраны или полиции - а не как межведомственный вопрос [является] главным препятствием, так как эти ведомства часто конкурировали за скудные ресурсы.

В частности, программа ИМО по глобальной безопасности на море отвечает за разработку и реализацию проектов технического сотрудничества, в первую очередь направленных на оказание государствам помощи в реализации, проверке, соблюдении и обеспечении соблюдения различных правовых и оперативных рамок ИМО. Одной из ключевых рамок в этой области является Кодекс ISPS. Кодекс разделен на две части: часть A и часть B. Часть A является обязательной и содержит подробные требования, касающиеся морской и портовой безопасности, которых должны придерживаться стороны, являющиеся частью Международной конвенции по охране человеческой жизни на море (SOLAS), администрации портов и судоходных компаний. Часть B содержит серию необязательных руководящих принципов о том, как выполнять требования и обязательства, изложенные в Части A. Основные цели Кодекса ISPS включают в себя[32]:

- создание международной структуры, которая способствует сотрудничеству между договаривающимися правительствами, правительственными учреждениями, местными администрациями и судоходной и портовой промышленностью, в оценке и обнаружении

[31] Выступление представителя ИМО, Совета Безопасности, призывает государства-члены противостоять угрозам в отношении критически важной инфраструктуры, единогласно принимая резолюцию 2341 (2017) по сайту: https://www.un.org/press/en/2017/sc12714.doc.htm

[32] Источник: ИМО, Морская безопасность и пиратство, по сайту: www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx

потенциальных угроз безопасности для судов или портовых сооружений, используемых для международной торговли, с тем чтобы принять превентивные меры безопасности против таких угроз ;
- определение соответствующих ролей и обязанностей всех сторон, связанных с обеспечением безопасности на море в портах и на судах, на национальном, региональном и международном уровнях;
- обеспечение своевременного и эффективного сбора и обмена информацией, касающейся безопасности на море, на национальном, региональном и международном уровнях;
- обеспечение методологии оценки безопасности судов и портов, которая облегчает разработку планов и процедур безопасности судов, компаний и портовых средств, которые должны использоваться для реагирования на различные уровни безопасности судов или портов;
- обеспечение адекватных и соразмерных мер безопасности на море на борту судов и в портах.

Для управления потенциальными угрозами безопасности Кодекс ISPS требует, чтобы страны, портовые власти и судоходные компании назначали ответственных сотрудников службы охраны портовых объектов, ответственных сотрудников охраны судов и ответственных сотрудников безопасности компании соответственно. Они несут ответственность за разработку и реализацию конкретных планов безопасности.

В дополнение к Кодексу ISPS программа ИМО по безопасности на море опирается на ряд других нормативных документов безопасности на море, которые в 2012 году были включены в «Руководство по безопасности на море и Кодекс ISPS». Руководство призвано предоставить заинтересованным сторонам исчерпывающий источник рекомендаций.

7.2 Авиационная отрасль

Международная организация гражданской авиации (ИКАО) - это специализированное учреждение ООН, созданное государствами в 1944 году для управления и регулирования Конвенции о международной гражданской авиации (Чикагская Конвенция).[33]

ИКАО работает с 192 государствами-членами Конвенции и отраслевыми группами в целях достижения консенсуса в отношении международных стандартов и рекомендуемой практики (SARPS) в области гражданской авиации и политики в поддержку безопасного, эффективного, надежного, экономически устойчивого и экологически ответственного сектора гражданской авиации. Эти SARPS и политики используются государствами-членами ИКАО для обеспечения соответствия их операций и правил гражданской авиации местным нормам, что, в свою очередь, позволяет более чем 100 000 ежедневных рейсов в глобальной сети авиации обеспечивать безопасную и надежную работу в каждом регионе мира.

В дополнение к своей основной работе по разрешению согласованных международных SARPS и политики среди своих государств-членов и отрасли, а также среди многих других приоритетов и программ, ИКАО также координирует помощь и наращивание потенциала для государств в поддержку многочисленных целей развития авиации; разрабатывает глобальные планы по координации многостороннего стратегического прогресса в области безопасности полетов и аэронавигации; отслеживает и сообщает о многочисленных показателях деятельности воздушного транспорта; и проверяет возможности государств в области надзора за гражданской авиацией в области безопасности полетов и авиационной безопасности.

Что касается стратегической цели в области авиационной безопасности и упрощения формальностей, она в основном осуществляется в следующих областях:

[33] (док.7300/9)

- политические инициативы;
- аудиты, сосредоточенные на способности государств-членов контролировать свою деятельность в области авиационной безопасности;
- помощь в наращивании потенциала и подготовке кадров для улучшения соответствующих возможностей государства;
- разработка и реализация стратегии ИКАО по программе идентификации путешественников (TRIP);
- управление директорий открытых ключей ИКАО.

Работа ИКАО в этом секторе основывается на ряде договоров в области авиационной безопасности. Они были приняты в течение более пятидесяти лет и обычно рассматриваются как неотъемлемая часть универсальной правовой базы против терроризма:

- Конвенция 1963 года о преступлениях и определенных других актах, совершаемых на борту воздушных судов, и дополнительный протокол к ней 2014 года;
- Конвенция 1970 года о борьбе с незаконным захватом воздушных судов и дополнительный протокол к ней 2010 года;
- Конвенция 1971 года о борьбе с незаконными актами, направленными против безопасности гражданской авиации
- Протокол 1988 года о борьбе с незаконными актами насилия в аэропортах, обслуживающих международные гражданские перевозки, и дополнительный протокол 2010 года
- Конвенция 1991 года о маркировке пластиковых взрывчатых веществ для целей обнаружения;
- Конвенция 2010 года о борьбе с незаконными актами, касающимися международной гражданской авиации;
- Протокол 2014 года о внесении изменений в конвенцию о преступлениях и определенных других актах, совершенных на борту воздушного судна.

Основополагающим справочным документом для государств, промышленности, заинтересованных сторон и ИКАО для совместной работы с общей целью повышения авиационной безопасности во всем мире является глобальный план авиационной безопасности (GASeP). Утвержденный Советом ИКАО в 2017 году, GASeP устанавливает пять приоритетных результатов:

- повысить осведомленность о рисках и реагирование;
- развивать безопасность культуры и способности человека (оператора)
- улучшить технологические ресурсы и стимулировать инновации;
- улучшить надзор и обеспечение качества;
- расширить сотрудничество и поддержку.

Основным инструментом, разработанным ИКАО, является *Руководство по авиационной безопасности*[34] (которое предназначено для оказания государствам помощи в осуществлении стандартов и рекомендуемой практики, включенных в приложение 17[35] - *Безопасность* - к Конвенции о международной гражданской авиации (Чикагская конвенция). Последняя версия Руководства, опубликованная в 2017 году, содержит новый и обновленный инструктивный материал. Особый интерес для ЗКВОИ представляют инструктивные материалы, касающиеся безопасности зон приземления аэропортов, проверки персонала и транспортных средств, а также киберугроз критически важных систем авиации.

[34] Doc 8973. Доступ к Руководству классифицирован как ограниченный. Его распространение ограничено государственными органами гражданской авиации и, по запросу, другими организациями, ответственными за осуществление мер авиационной безопасности, такими как эксплуатанты аэропортов и воздушных судов, или другими организациями, утвержденными соответствующими государственными органами. Руководство по авиационной безопасности доступно в электронном виде для авторизованных пользователей по адресу: https://drm.icao.int/ вебсайт.

[35] Приложение 17 «Безопасность» включает, в частности, стандарты и рекомендуемую практику обеспечения безопасности полетов в международной авиации и постоянно пересматривается и дополняется в свете новых угроз и технологических достижений, которые влияют на эффективность мер, направленных на предотвращение актов незаконного вмешательства.

Другим важным инструментом является Заявление о глобальном контексте рисков в области авиационной безопасности. Ежегодно публикуемый этот «живой документ» предоставляет государствам наиболее актуальную информацию об условиях угрозы и риска. В нем содержится анализ глобальных угроз гражданской авиации, информация о последних изменениях в тактике терроризма, технический анализ конкретных угроз авиационной безопасности. В его последней версии подчеркивается, что ряд террористических групп продолжает изучать инновационные методы сокрытия самодельных взрывных устройств и обхода существующих мер безопасности.

Признавая срочность и важность защиты критически важных объектов инфраструктуры, информационных и коммуникационных технологий и данных гражданской авиации от киберугроз, 39-я сессия Ассамблеи ИКАО призвала к скоординированному подходу для достижения приемлемого и соразмерного потенциала кибер-устойчивости в глобальном масштабе. С этой целью резолюция A39-19 «Решение проблем кибербезопасности в гражданской авиации»[36] определяет действия, которые должны быть предприняты государствами и другими заинтересованными сторонами для противодействия киберугрозам гражданской авиации посредством межотраслевого, единого и совместного подхода.

Стратегия ИКАО TRIP была одобрена в 2013 году 38-й сессией Ассамблеи ИКАО. В ней подчеркивается целостный подход к управлению идентификацией с целью максимизации как авиационной безопасности, так и упрощения формальностей, и ожидается, что она расширит возможности государств по уникальной идентификации лиц путем предоставления властям эффективных инструментов и руководящих указаний по идентификации. Она обеспечивает основу для достижения значительных улучшений в области авиационной безопасности и упрощения формальностей, объединяя элементы управления идентификацией и опираясь на лидерство ИКАО в вопросах, связанных с МСПД. Пять взаимосвязанных элементов стратегии ИКАО TRIP: подтверждение личности, МСПД, выдача и контроль документов, системы и инструменты проверки и совместимые приложения. Технические спецификации, обеспечивающие глобальную совместимость проездных документов, приведены в документе Doc 9303 *«Машиносчитываемые проездные документы»* (МСПД).

Важные объекты инфраструктуры путешествий будут включать в себя киберфизическую и физические объекты инфраструктуры, которые поддерживают выдачу проездных документов, и системы пограничного контроля, которые объединяют системы и инструменты инспекции и совместимые приложения, которые используются для обработки пассажиров на границах. Объекты инфраструктуры безопасности национальной идентичности играют решающую роль в инфраструктуре путешествий.

Многочисленные руководящие материалы по TRIP, разработанные при поддержке технических экспертов технической консультативной группы, доступны по адресу:
www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

В целях поощрения участия в директории открытых ключей ИКАО в поправке 26 к Приложению 9 «Упрощение формальностей» введена новая Рекомендуемая практика (РП), РП 3.35.5, предназначенная для тех государств-членов ИКАО, которые используют систему автоматизированного пограничного контроля (АВС). Эта РП поощряет использование информации, доступной через ДОК ИКАО, в качестве средства проверки электронных паспортов путем сравнения распознавания лиц с фотографией владельца электронного паспорта.

[36] (Рез. A39-19, октябрь 2016, по адресу: www.icao.int/Meetings/a39/Documents/Resolutions/a39_res_en.pdf

7.3 Сектор информационных технологий

Защита КИИ от рисков кибербезопасности является приоритетной целью Международного союза электросвязи (МСЭ). План действий в Буэнос-Айресе, принятый на Всемирной конференции по развитию электросвязи 2017 года, включал в качестве цели 2 «Содействие развитию инфраструктуры и услуг, включая укрепление доверия и безопасности при использовании электросвязи / ИКТ»[37].

Работа МСЭ напрямую связана с повышением устойчивости КИИ (и соответственно КВОИ) к кибератакам, независимо от происхождения этих атак. Деятельность МСЭ вращается вокруг трех основных блоков: i) установление стандартов; ii) повышение осведомленности; iii) наращивание потенциала. Для каждого из этих блоков в следующих параграфах освещены ключевые текущие инициативы.

i) Установление стандартов

Работа по стандартизации проводится рядом технических исследовательских комиссий (ИК), в которых представители членов МСЭ разрабатывают рекомендации (стандарты) в различных областях международной электросвязи. В частности, 17-я Исследовательская комиссия (SGI7) занимается вопросами укрепления доверия и безопасности при использовании информационных и коммуникационных технологий для достижения более безопасной сетевой инфраструктуры, услуг и приложений. В рамках этой исследовательской комиссии более 350 стандартов[38] (рекомендации и дополнения МСЭ-Т) уже приняты.

Текущие области работы SGI7 включают, помимо прочего, кибербезопасность, управление безопасностью, архитектуры и структуры безопасности, управление идентификацией, безопасность приложений и аспекты безопасности облачных вычислений, IoT (интернет физических объектов), интеллектуальную транспортную систему, большие данные, технологию распределенных регистров и т. д. Ключевым справочником по стандартам безопасности является Рекомендация МСЭ-Т X.509 для электронной аутентификации в сетях общего пользования. МСЭ-Т X.509 считается знаковым инструментом для разработки приложений, связанных с инфраструктурой открытых ключей.

ii) Повышение осведомленности

Новаторским инструментом, разработанным МСЭ, является глобальный индекс кибербезопасности (GCI). Задуманный прежде всего как инструмент повышения осведомленности, GCI стремится измерить приверженность стран кибербезопасности. Эффективность каждой страны оценивается в пяти областях: правовые меры, технические меры, организационные меры, наращивание потенциала и сотрудничество.

Вопросы разработаны для оценки приверженности в каждом столпе. Впоследствии, после консультаций с группой экспертов, эти вопросы оцениваются, чтобы прийти к общему баллу GCI. Третья итерация GCI в настоящее время готовится.[39]

iii) Наращивание потенциала

В этой области МСЭ оказывает поддержку государствам-членам в создании национальных групп реагирования на компьютерные инциденты (CIRT). Они рассматриваются как национальные координационные центры для координации своевременного и эффективного реагирования на кибератаки. МСЭ полон решимости оказывать странам помощь на протяжении всего процесса

[37] Итоговый отчет конференции доступен по адресу: www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Documents/WTDC17 final report en.pdf

[38] Рекомендации МСЭ-Т, разработанные 17-й Исследовательской комиссией МСЭ-Т, размещены в открытом доступе на: http://www.itu.int/ITU-T/recommendations/index sg.aspx?sg=17

[39] (Рекоммендации МСЭ-Т, разработанные исследовательской группой 17 МСЭ-Т доступны публично на: http://www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=17

создания CIRT - от оценки их готовности до оказания помощи на этапах планирования и осуществления на основе принципа постоянного сотрудничества. МСЭ также организует регулярные региональные кибер учения (кибер-тренировки) для расширения сотрудничества между национальными CIRT в том же регионе.

7.4 Сектор обычного вооружения

В своей резолюции 2370 (2017) Совет Безопасности признает «ценность мер, [...] направленных на обеспечение эффективной физической безопасности и управления запасами стрелкового оружия и легких вооружений, в качестве важного средства, способствующего ликвидации поставок оружия террористам»[40].

В частности, в пункте 7 резолюции подчеркивается важность принятия государствами-членами надлежащих мер по предотвращению [...] разграбления или приобретения стрелкового оружия и легких вооружений из национальных запасов террористами, и в этой связи подчеркивается важность оказания государствам помощи в тех регионах, которые позволяют им контролировать и отслеживать запасы стрелкового оружия и легких вооружений, с тем чтобы террористы не могли их приобрести».

Что касается защиты критически важных объектов инфраструктур, то обеспечение физической безопасности и управление запасами обычных вооружений имеет решающее значение в двойном смысле. Во-первых, это снижает риск того, что такое оружие может быть использовано против таких организационных элементов, как транспортные системы, правительственные здания и любые другие объекты, которые отдельные страны считают критически важными. Во-вторых, эти самые запасы сами по себе могут рассматриваться как критически важные объекты инфраструктуры, которые играют важную роль в оборонительной политике стран.

Разнообразные международные и региональные документы являются частью международно-правового режима в отношении обычных вооружений. Хотя эти инструменты обеспечивают государствам прочную правовую и оперативную основу для укрепления их внутренних правовых режимов, они не обязательно образуют однородный набор инструментов. Например, Протокол против незаконного изготовления и оборота огнестрельного оружия, его составных частей и компонентов, а также боеприпасов к нему (Протокол об огнестрельном оружии)[41] рассматривает эту проблему с точки зрения уголовного правосудия, с целью принятия мер по решению проблемы транснационального характера этого явления и его связи с организованной преступностью. Другие документы, хотя и охватывают аналогичные темы, касаются проблемы с точки зрения разоружения, торговли или развития и в большей степени сосредоточены на мерах по сокращению накопления, распространения, утечки и злоупотребления огнестрельным оружием. В результате важно, чтобы государственные органы ознакомились с разнородной международно-правовой базой и обеспечили ее полное осуществление.

Нижеследующий список представляет собой неисчерпывающую подборку международных договоров и других руководящих документов, касающихся этой темы с разных сторон.

[40] Эти меры уже рассмотрены в «Программе действий по предотвращению и искоренению незаконной торговли стрелковым оружием и легкими вооружениями во всех ее аспектах и борьбе с ней». В рамках этой программы правительства договорились усовершенствовать национальные законы о стрелковом оружии, контроль за импортом / экспортом и управление запасами - и участвовать в сотрудничестве и помощи
(www.un.org/disarmament/convarms/salw/programme-of-action/).
[41] Протокол дополняет Конвенцию Организации Объединенных Наций против транснациональной организованной преступности

Организация Объединенных Наций

Договоры:

- Протокол против незаконного изготовления и оборота огнестрельного оружия, его составных частей и компонентов, а также боеприпасов к нему, дополняющий Конвенцию Организации Объединенных Наций против транснациональной организованной преступности (2001)
- Договор о торговле оружием (2013)

Другие инструменты:

- Программа действий по предотвращению и искоренению незаконной торговли стрелковым оружием и легкими вооружениями во всех ее аспектах и борьбе с ней (2001 год);
- Международный документ, позволяющий государствам своевременно и надежно выявлять и отслеживать незаконное стрелковое оружие и легкие вооружения (2005 год);

Африка

Договоры:

- Протокол о контроле над огнестрельным оружием, боеприпасами и другими соответствующими материалами Сообщества Развития Юга Африки (SADS) (2001)
- Найробский протокол о предотвращении, контроле и сокращении стрелкового оружия и легких вооружений в районе Великих озер и Африканского Рога (2004 год);
- Конвенция о стрелковом оружии и легких вооружениях, боеприпасах к ним и других соответствующих материалах (ЭКОВАС) (2006 год);
- Центральноафриканская конвенция о контроле за стрелковым оружием и легкими вооружениями, их боеприпасами, частями и компонентами, которые могут использоваться для их изготовления, ремонта и сборки (Конвенция Киншаса) (2010)

Другие инструменты

- Бамакская декларация об общей позиции африканских стран в отношении незаконного распространения, оборота и незаконной торговли стрелкового оружия и легких вооружений - политически обязывающая (2000 год);
- Стратегия Африканского союза по борьбе с незаконным распространением, оборотом и незаконной торговли стрелкового оружия и легких вооружений (2011 год);
- План действий по осуществлению Стратегии Африканского союза по борьбе с незаконным распространением, оборотом и незаконной торговли стрелкового оружия и легких вооружений

Северная и Южная Америка

Договоры:

- Межамериканская конвенция о борьбе с незаконным изготовлением и оборотом огнестрельного оружия, боеприпасов, взрывчатых веществ и других соответствующих материалов (CIFTA) (1997)

Другие инструменты

- Андский план предотвращения и пресечения незаконной торговли стрелковым оружием и легкими вооружениями во всех ее проявлениях и борьбы с ней - политически обязывающий (2003)
- Типовые правила CICAD - Типовые правила контроля за международным перемещением огнестрельного оружия, его составных частей и компонентов, а также боеприпасов к нему;

Типовые правила контроля за брокерами огнестрельного оружия, его составных частей и компонентов, а также боеприпасов к нему;
- Кодекс поведения государств Центральной Америки в отношении передачи оружия, боеприпасов, взрывчатых веществ и других соответствующих материалов (2006 год).

Азиатско-Тихоокеанский регион

Нормативные документы:

- Структура Nadi (Правовая основа для общего подхода к контролю над вооружениями);
- План действий по борьбе с транснациональной преступностью (АСЕАН) (1999 год)

Европа

Организация по безопасности и сотрудничеству в Европе:

- План действий по стрелковому оружию и легким вооружениям (документ ОБСЕ FSC. DEC / 2/10);
- Справочник по наилучшей практике в отношении обычных боеприпасов, Справочник по наилучшей практике в отношении обычных боеприпасов (2008 год);
- Принципы контроля за брокерскими операциями по стрелковому оружию и легкому вооружению, Форум по сотрудничеству в области безопасности, решение № 8/04 (2004 год);
- Стандартные элементы сертификатов конечного пользователя и процедуры проверки для экспорта стрелкового оружия и легких вооружений, Форум по сотрудничеству в области безопасности, решение № 5/04 (2004 год);
- Справочник по наилучшей практике в области стрелкового оружия и легких вооружений (2003 год);
- Принципы, регулирующие программу передачи обычных вооружений для незамедлительных действий Серия № 3 (DOC.FSC/3/96), (1993);
- Документ Организации по безопасности и сотрудничеству в Европе (ОБСЕ) о стрелковом оружии и легких вооружениях (2000, переиздан в 2012 году);
- Решение № 11/08 Внедрение передового опыта по предотвращению дестабилизирующей передачи стрелкового оружия и легких вооружений воздушным транспортом и по соответствующей анкете (2008 г.)

Европейский Союз

- Совместное решение Совета от 12 июля 2002 года о вкладе Европейского союза в борьбу с дестабилизирующим накоплением и распространением стрелкового оружия и легких вооружений;
- Общая позиция Совета ЕС по брокерской деятельности 2003/468 /CFSP;
- Общая позиция 2008/944 / CFSP;
- Постановление Европейского парламента и Совета 258/2012 об осуществлении статьи 10 Протокола против незаконного изготовления и оборота огнестрельного оружия, его составных частей и компонентов и боеприпасов к нему, дополняющего Конвенцию Организации Объединенных Наций против транснациональной организованной преступности, и об установлении разрешения на экспорт, а также ввозных и транзитных мер по огнестрельному оружию, его частям, компонентам и боеприпасам (Официальный журнал Европейского Союза, L 94, 2012);
- Кодекс поведения ЕС в отношении экспорта оружия (1998 год);
- Стратегия ЕС по борьбе с незаконным накоплением и оборотом стрелкового оружия и легких вооружений и их боеприпасов (2005 год).

7.5 Секторы химического, биологического, радиологического и ядерного оружия (ХБРЯ)

Перспектива того, что негосударственные субъекты, в том числе террористические группы и их сторонники, получат доступ к оружию и материалам массового уничтожения и смогут использовать их, представляют собой серьезную угрозу международному миру и безопасности. Признавая распространенность этой озабоченности, Генеральный секретарь ООН поставил предотвращение в центр своей повестки дня в области мира и безопасности. В своей резолюции (A / RES / 70/291), завершающей пятый обзор Глобальной контртеррористической стратегии ООН (A / RES / 60/288), Генеральная Ассамблея ООН также призвала все государства-члены «не допустить захвата террористами оружия массового уничтожения (ОМУ) и средств его доставки и (поощряемого) сотрудничества между государствами-членами и между ними и соответствующими региональными и международными организациями в целях укрепления национального потенциала в этой области». Совет Безопасности ООН также выступил с аналогичными заявлениями, в том числе с резолюцией 2325 от 15 декабря 2016 года, в которой содержится призыв ко всем государствам-членам укреплять свои национальные режимы нераспространения оружия при реализации своей основополагающей резолюции 1540 (2004).

i) КТУ ООН

В июне 2017 года, в соответствии с резолюцией Генеральной Ассамблеи (A / RES / 71/291) было создано контртеррористическое управление ООН (КТУ ООН), в состав которого входят Целевая группа ООН по осуществлению контртеррористических мероприятий (ЦГОКМ) и Контртеррористический центр ООН (КТЦ ООН). С 2006 года Рабочая группа ЦГОКМ по предотвращению и реагированию на террористические атаки с применением ОМУ способствовала интерактивному обмену знаниями, обмену информацией о существующих мероприятиях и планах действий в чрезвычайных ситуациях подразделений ООН и международных организаций в области предотвращения и реагирования на нападения с использованием ОМУ или связанных с ним материалов. С 2013 года КТЦ ООН поддерживает проект Рабочей группы «Обеспечение эффективной межведомственной совместимости и скоординированной связи в случае химических и / или биологических атак». В рамках проекта оценивается, как система ООН и международные организации будут коллективно реагировать на террористический акт, когда используется химическое и биологическое оружие или материалы, и уровень планируемой координации между различными организациями для содействия быстрому оказанию помощи пострадавшему государству / государствам.

В 2018 году КТЦ ООН начал расширять свою контртеррористическую деятельность, связанную с ОМУ / ХБРЯ, в соответствии с четырьмя стратегическими целями: 1) содействовать пониманию угрозы терроризма ОМУ / ХБРЯ; 2) Расширить деятельность по наращиванию потенциала для поддержки мер по предотвращению, обеспечению готовности и реагированию в государствах-членах в соответствии с Глобальной контртеррористической стратегией ООН, в том числе в областях пограничного и таможенного контроля, стратегического контроля за торговлей, незаконного оборота и обеспечения безопасности критически важных объектов инфраструктуры; 3) Развивать партнерские отношения для содействия усилиям международного сообщества по наращиванию потенциала; 4) Улучшение прозрачности и поддержка мобилизации дополнительных ресурсов.

ii) ЮНИКРИ

В рамках инициативы Европейского союза по Центрам передового опыта по химическому, биологическому, радиологическому и радиационному риску», ЮНИКРИ оказал поддержку нескольким государствам-членам ООН в разработке национальных планов действий по ХБРЯ (НПД), в которых выделены основные риски и приоритеты по созданию национального потенциала. НПД охватили различные аспекты предотвращения и борьбы как с преднамеренными, так и

непреднамеренными рисками ХБРЯ, включая безопасность и защиту критически важной инфраструктуры.

Кроме того, ЮНИКРИ руководил реализацией многорегионального проекта в рамках Совета Европы по ХБРЯ ЕС (проект 19), озаглавленного «Разработка процедур и руководящих принципов для создания и совершенствования надежной системы управления информацией и механизмов обмена данными для материалов ХБРЯ, находящихся под регулирующим контролем». Этот проект, который был реализован в 2013–2015 годах, направлен на укрепление национального потенциала для безопасного управления информацией и обмена данными о материалах и средствах ХБРЯ, а также на создание группы экспертов, состоящей из ведущих специалистов из государственного и частного секторов.

iii) Интерпол

В 2010 году 80-я Генеральная Ассамблея Интерпола приняла историческое решение[42] о создании комплексного потенциала ХБРЯ по предотвращению терроризма и реагированию на него в поддержку 192 стран-членов Организации. В 2016 году Глобальная контртеррористическая стратегия Интерпола закрепила миссию Организации в области ХБРЯ в ее канале действий «Оружие и материалы», *помогая странам-членам в выявлении, отслеживании и перехвате незаконного оборота оружия и материалов, необходимых для террористической деятельности*. В Стратегии далее определяются основные действия, которые должны быть предприняты «Подотделом по CBRNE (химическое, биологическое, радиологическое, ядерное оружие и усовершенствованные стандартные виды оружия) и уязвимым целям» в отношении оказания помощи странам-членам в предотвращении глобальных угроз ХБРЯ, основанных на негосударственном субъекте, и реагировании на них:

- *Действие 4.3:* Содействовать обмену разведданными между странами-членами по вопросам и способам действий, связанным с инцидентами ХБРЯ и СВУ;
- *Действие 4.4:* Расширить возможности стран-членов по предотвращению и реагированию на атаки ХБРЯ и СВУ путем создания программ противодействия;
- *Действие 4.5:* Разработать координацию трансграничных, межведомственных операций, проводимых разведкой, для пресечения незаконного оборота материалов ХБРЯ и компонентов СВУ;
- *Действие 4.7:* Поддерживать и развивать стратегическое партнерство с ХБРЯ в глобальном масштабе.

При осуществлении вышеупомянутых действий - и в соответствии с Конституцией Интерпола[43] - Организация ориентирована исключительно на устранение угроз ХБРЯ негосударственных субъектов. Соответственно, Интерпол воздерживается от решения вопросов, связанных с распространением оружия массового уничтожения (ОМУ), спонсируемого государством, которые тщательно рассматриваются другими международно-правовыми и институциональными механизмами. Тем не менее, спектр негосударственных субъектов включает не только террористические группы, одиночек и других преступников в качестве потенциальных конечных пользователей, но и широкую картину незаконного оборота материалов ХБРЯ и его различных компонентов. Поставщики, посредники, покупатели и сети контрабанды - все это входит в компетенцию Интерпола.

С глобальным осознанием решающей роли правоохранительных органов в предотвращении и реагировании на угрозы ХБРЯ, основанные на негосударственных субъектах, Интерпол постепенно стал одной из ключевых международных организаций, вносящих вклад в глобальные усилия по борьбе с терроризмом ХБРЯ. Кроме того, Организация объединила все основные многонациональные структуры и установила тесные связи со всеми соответствующими международными партнерами в конкретной интерпретации межведомственного подхода в глобальном масштабе.

[42] AS-2011-RES-10

[43] Статья 3 Конституции Интерпола закрепляет руководящий принцип нейтралитета, прямо запрещая Интерполу заниматься вопросами политического, военного, религиозного или расового характера.

Явное упоминание резолюции 1540 Совета Безопасности ООН о негосударственных субъектах сделало эту резолюцию естественным ориентиром для деятельности Интерпола, связанной с ХБРЯ. С первых дней деятельности Интерпола в области ХБРЯ, Организация обменивалась официальными письмами с Комитетом 1540 с изложением условий их продолжающегося сотрудничества и назначением соответствующих центров связи. В последнее время Интерпол играл активную роль в рамках всеобъемлющего обзора резолюции 2016 года. В более широком смысле Интерпол является «вспомогательным агентством-провайдером» в соответствии с резолюцией 1540 Совета Безопасности ООН, и большая часть его деятельности в области ХБРЯ поддерживает - прямо или косвенно - реализацию резолюции.

Интерпол поддерживает тесные рабочие отношения с Управлением Организации Объединенных Наций по вопросам разоружения (UNODA), особенно в деле содействия деятельности по наращиванию потенциала реестра экспертов, входящих в «Механизм Генерального секретаря по расследованию предполагаемого использования химического, бактериологического (биологического) или токсинового оружия» (UNSGM).

В Интерполе специализированные группы занимаются предотвращением трех видов терроризма:

- радиологического и ядерного терроризма
- биотерроризма
- химического и взрывного терроризма

Деятельность Интерпола варьируется от анализа данных, учебных семинаров и командно-штабных учений до международных конференций и операций на местах. Методология Интерпола по противодействию угрозе ХБРЯ состоит из трех основных столпов:

i. Обмен информацией и анализ разведывательных данных: Помимо оценки и анализа угроз, мы публикуем регулярный аналитический отчет: Ежемесячный дайджест Интерпола по ХБРЯ. Предоставленный нашим странам-членам и другим подписчикам, он обобщает отчеты из открытых источников по всем аспектам преступности и терроризма ХБРЯ и предоставляет аналитическую точку зрения по конкретным вопросам;
ii) Наращивание потенциала и обучения: Организация помогает своим странам-членам в наращивании их потенциала, навыков и знаний в целях противодействия угрозе ХБРЯ. Это делается для:
    - Повышения уровня осведомленности о ХБРЯ в правоохранительных органах;
    - Проведение учебных занятий для расширения возможностей правоохранительных органов;
    - Предоставления методики по профилактике для использования государствами-членами.

    Оперативная и следственная поддержка: По запросу Интерпол может оказывать оперативную поддержку своим государствам-членам в форме группы реагирования на инциденты. В случае террористического нападения в эти группы могут быть направлены сотрудники с опытом работы в сфере ХБРЯ. Кроме того, мы осуществляем ряд инициатив, проектов и операций в поддержку международного правоохранительного сообщества в борьбе с незаконным оборотом материалов ХБРЯ.

7.5.1 Химический сектор

Организация по запрещению химического оружия (ОЗХО) рассматривает вопрос защиты КВОИ с точки зрения продвижения надежных методов управления безопасностью процессов и химических объектов. В 2016 году Организация составила руководство по наилучшей практике, которое собирает и обрабатывает информацию, полученную от шестнадцати государств-членов (ОЗХО, 2016 год).

Подход ОЗХО заключается, в частности, в решении вопросов безопасности (понимаемых как меры, направленные на «преднамеренные» выбросы токсичных химикатов), неразрывно связанных с вопросами безопасности (то есть мер по противодействию «непреднамеренным выбросам»). Главными целями ОЗХО в этой области являются обеспечение охвата странами следующих аспектов безопасности и охраны:

- *Профилактика:* относится к пониманию и осуществлению мер по снижению вероятности возникновения химической аварии или инцидента безопасности. Инцидент химической безопасности может включать в себя кражу химических материалов для последующего неправильного использования или злонамеренного выброса химических веществ в окружающую среду;

- *Обнаружение:* относится к системам и процессам, которые поддерживают раннее обнаружение выброса или утечки химического вещества, а также подтверждение использования химического вещества после предполагаемого выброса (случайного или злонамеренного). Системы обнаружения должны включать процессы информирования о рисках.

- *Реагирование:* относится как к реагированию на уровне объекта, так и к реагированию на национальном уровне в случае химической аварии или инцидента, связанного с химической безопасностью. Системы реагирования включают в себя привлечение, оснащение и обучение сотрудников служб реагирования, таких как пожарные, аварийные, спасательные и полицейские службы.

С 2009 по 2016 год программы по наращиванию потенциала в области комплексного управления химическими рисками, осуществляемые техническим секретариатом ОЗХО, охватили более 1400 участников более чем из 130 государств-членов. Деятельность основана на стандартах, установленных международными правилами (главным образом, Конвенцией о химическом оружии) и нормами национального уровня. Среди существующих международных документов и инициатив ОЗХО выделила следующие элементы, включающие полезные элементы по вопросам химической безопасности и защиты:

- *Резолюция 1540 Совета Безопасности ООН*, которая обязывает государства, в частности, воздерживаться от оказания поддержки негосударственными субъектами любыми средствами в разработке, приобретении, производстве, хранении, транспортировке, передаче или использовании ядерного, химического или биологического оружия и систем его доставки. Важно то, что этот нормативный документ фокусируется на элементах превентивного измерения управления рисками химической безопасности;
- *Базельская конвенция*, касающаяся международного перемещения опасных материалов. Хотя Конвенция направлена на предотвращение выброса токсичных химических веществ в окружающую среду, «принимаемые меры могут способствовать безопасному обращению с химическими веществами и уменьшать объем химических веществ на транспорте и в системе отходов, поддерживая как лучшие методы химической безопасности, так и лучшие методы химической сохранности»;
- *Стокгольмская конвенция*, направленная на сокращение производства и использования стойких органических загрязнителей. Правила и передовые методы, принятые для

осуществления настоящей Конвенции, способствуют повышению химической безопасности и управлению рисками безопасности;

- *Роттердамская конвенция*, поддерживающая маркировку и обращение с опасными химическими веществами, в частности в международной торговле. Она содержит стандарты и инструкции, полезные для поддержки практики безопасности цепочки поставок;
- *Директива Севезо* (I, II и III), нормативные документы ЕС, направленные на повышение безопасности объектов, содержащих большое количество опасных веществ;
- *Согласованная на глобальном уровне система классификации опасности и маркировки химической продукции (СГС)* - это стандарт, управляемый ООН, созданный для замены множества схем классификации и маркировки опасных материалов, которые ранее использовались странами во всем мире. Будучи добровольными по своему характеру, законодательства некоторых стран сделали его обязательным для внутреннего применения;
- *Ответственная забота* - глобальная инициатива химической промышленности, нацеленная, среди прочего, на повышение безопасности продуктов и процессов и «предоставление помощи и консультаций для стимулирования ответственного управления химическими веществами всеми, кто управляет ими и использует их на протяжении всей цепочки продуктов»[44];
- *Международная организация по стандартизации (ISO),* которая установила ряд стандартов, поддерживающих элементы химической безопасности и защиты, в частности: 13000 по управлению рисками, 28000 по цепочке поставок химических веществ, 14000 по управлению окружающей средой и 9000 по управлению качеством.

Сосредоточившись более конкретно на угрозе терроризма, создаваемой негосударственными субъектами, в 2017 году ОЗХО провело «Экспертный семинар по международной координации химической безопасности»[45]. На семинаре проведено обзорное мероприятие «с целью подвести итоги существующего международного сотрудничества и координации в области химической безопасности, выявить пробелы и обсудить будущую деятельность, включая будущие механизмы координации». Ключевой рекомендацией было создание международного координационного механизма, «чтобы позволить ключевым международным субъектам, поддерживающим развитие глобального потенциала в области химической безопасности, [...] обсуждать приоритеты и методологии, использовать ресурсы друг друга, сотрудничать, где это необходимо, для удовлетворения потребностей отдельных государств, и поднять международный профиль потребностей и помощи в области химической безопасности». Другим ключевым итогом встречи стала рекомендация о создании «типовой методологии обеспечения химической безопасности».

7.5.2 Ядерный сектор

Защита ядерных и других радиоактивных материалов и связанных с ними объектов от террористических атак и других опасностей является приоритетной задачей Международного агентства по атомной энергии (МАГАТЭ). Её инициативы в этой области осуществляются в рамках программы физической ядерной безопасности, в которой рассматриваются все вопросы, связанные с предотвращением и обнаружением краж, диверсий, несанкционированного доступа и незаконной передачи или других злонамеренных действий, связанных с ядерными и другими радиоактивными материалами и связанных с ними объектов, и реагированием на них. Правовые основы, лежащие в основе программы, представляют собой сеть международных инструментов, которые включают, в частности:

[44] http://www.cefic.org/Responsible-Care

[45] Семинар экспертов по международной координации в области химической безопасности, 7 декабря 2017 года, по адресу: https://www.opcw.org/fileadmin/OPCW/Protection-Against-CW/OPCW_Chemical_Security_Workshop_-_Informal_Summary-October_2017_-_for_release.pdf

- Конвенция о физической защите ядерного материала (с поправкой 2005 года);
- Кодекс поведения по безопасности и охране радиоактивных источников;
- Резолюции Совета Безопасности ООН 1373, 1540 и 2325;
- Международная конвенция о борьбе с актами ядерного терроризма.

Серия публикаций МАГАТЭ по физической ядерной безопасности дополняет вышесказанное, предоставляя передовой опыт, технические руководства, учебные пособия и т. д. в интересах государств-членов.

Среди таких публикаций - инструктивное руководство по «Созданию инфраструктуры физической ядерной безопасности для ядерной энергетической программы» (МАГАТЭ, 2013 г.). В Руководстве содержатся технические указания по развитию объектов инфраструктуры физической ядерной безопасности, включая правовые, нормативные и институциональные рамки и национальную стратегию физической ядерной безопасности. Его обоснование заключается в необходимости «обеспечить, чтобы ядерный и другой радиоактивный материал не попадал в руки сторон, которые могли бы использовать этот материал для преступных или террористических актов, и предотвращать акты диверсий в отношении объектов и связанной с ними деятельности, в том числе во время транспортировки».

13 сентября 2017 года Совет управляющих МАГАТЭ утвердил план физической ядерной безопасности Организации на период 2018–2021 годов (МАГАТЭ, 2017 год). Заявленные цели Плана заключаются в следующем:

- содействовать глобальным усилиям по достижению эффективной физической ядерной безопасности путем разработки всеобъемлющих руководящих указаний по физической ядерной безопасности и, по запросу, содействия их использованию посредством экспертных обзоров и консультативных услуг и наращивания потенциала, включая образование и подготовку кадров;
- содействовать присоединению и осуществлению соответствующих международно-правовых документов, а также укреплять международное сотрудничество и координацию помощи;
- играть центральную роль и расширять международное сотрудничество в области физической ядерной безопасности в ответ на приоритеты государств-членов, выраженные в решениях и резолюциях органов Агентства по разработке политики.

Мероприятия, предусмотренные в этом Плане, направлены на оказание помощи странам, по их просьбе, в создании эффективных и устойчивых национальных режимов физической ядерной безопасности, а также на содействии соблюдению соответствующих международных документов. В Плане, в частности, определен ряд приоритетных областей и подразделов для вмешательства посредством мероприятий по оказанию технической помощи и созданию потенциала под следующими заголовками:

Управление информацией

- Оценка потребностей и приоритетов в области физической ядерной безопасности
- Обмен информацией
- Информационная и компьютерная безопасность и услуги информационных технологий

Ядерная безопасность материалов и связанных с ними объектов

- Подходы к ядерной безопасности для всего цикла ядерного топлива
- Повышение безопасности ядерных материалов с использованием учета и контроля.
- Повышение безопасности радиоактивных материалов и связанных с ними объектов.
- Ядерная безопасность при транспортировке ядерных и других радиоактивных материалов.

Ядерная безопасность материалов вне регулирующего контроля

- Институциональная инфраструктура для материалов вне регулирующего контроля
- Архитектура обнаружения и реагирования ядерной безопасности
- Радиологическое управление на месте преступления и ядерная криминалистика

Разработка программ и международное сотрудничество

- Международное сотрудничество в области сетей и партнерств по физической ядерной безопасности.
- Программы обучения и подготовки кадров для развития людских ресурсов.
- Координация инструкторских и консультационных служб по ядерной безопасности

СПИСОК ЛИТЕРАТУРЫ

Акерман 2007, Оценка мотивации террористов для нападения на критически важные инфраструктуры, Центр исследований по нераспространению, Монтерейский институт международных исследований, по адресу: https://e-reports-ext.llnl.gov/pdf/341566.pdf

Arie H.2017, Японский подход к решению проблем кибербезопасности, по адресу: www.japanindustrynews.com/2017/01/japans-approach-tackling-cybersecurity-challenges/

Австралия-Новая Зеландия, 2015 г., Национальное руководство по защите критически важной инфраструктуры от терроризма, Австралия-Новая Зеландия, Контртеррористический комитет, по адресу: www.nationalsecuritv.gov.au/Media-and-publications/publications/documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf

Канада 2005, Стратегия и План действий по устойчивости к химическим, биологическим, радиологическим и ядерным взрывчатым веществам для Канады, по адресу: www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/chmcl-blgcl-rdlgcl-en.aspx

Клементе, 2013, Кибербезопасность и глобальная взаимозависимость: что является критически важным? Chatham House, февраль 2013, по адресу: www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr cvber.pdf

Расследования следователя в отношении взрывов в Лондоне от 7 июля 2005 года, 6 мая 2011 года, по адресу: http://image.guardian.co.uk/svs-files/guardina/docuemnts/2011/05/06/rule43-report.pdf

ИДКТК 2017, Физическая защита критически важной инфраструктуры от террористических атак, Отчет о тенденциях, Исполнительная дирекция по борьбе с терроризмом, по адресу: www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf

Европейская комиссия 2005, Зеленая книга по Европейской программе защиты критически важной инфраструктуры, COM (2005) 576 итог.

Европейская Комиссия 2013, Стратегия кибербезопасности Европейского Союза, JOIN (2013) 1 выпуск, по адресу: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec comm en.pdf

Европейская комиссия 2013 бис. Рабочий документ о новом подходе к Европейской программе по защите критически важной инфраструктуры - создание более безопасной европейской критически важной инфраструктуры, SWD(2013) 318 итог, по адресу: https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

Европейская комиссия 2017, План действий по поддержке защиты общественных пространств, 18.10.2017 COM (2017) 612 итог, по адресу: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-securitv / 20171018_action_plan_to_improve_the_protection_of_public_spaces_en.pdf

Федеральный Сигнал 2013, Основы взаимодействия для экстренной связи, Thought Paper, по адресу: www.fedsig.com/sites/default/files/news/pdf/The%20bais%20of%20Interoperability%20for%20Emergency%20Communications.pdf

Франция 2014, Генеральная межведомственная инструкция по безопасности жизнедеятельности (доступна только на французском языке), Генеральный секретариат по обороне и национальной безопасности (№6600 / SGDSN / PSE / PSN), по адресу: http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir 37828.pdf

Германия 2009, Национальная стратегия защиты критически важной инфраструктуры, Федеральное министерство внутренних дел, по адресу:
http://ccpic.mai.gov.ro/docs/Germania_сшз_stategv.pdf

GGE 2015, Отчет Группы правительственных экспертов по событиям в области информации и телекоммуникаций в контексте международной безопасности, Генеральная Ассамблея (Doc.A / 70/174), по адресу: https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf

GFCE-Meridian 2016, Руководство по эффективной практике защиты критически важной информационной инфраструктуры для правительственных политиков, по адресу:
www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

Япония 2015, Стратегия кибербезопасности, по адресу:
www.nisc.go.jp/eng/PDF/CS-strategy-en.pdf

МАГАТЭ 2013, Создание инфраструктуры физической ядерной безопасности для ядерной энергетической программы - Руководство по реализации, по адресу:
www-pub.iaea.org/books/iaeabooks/10436/Establishing-the-Nuclear-Security-Infrastructure-for-a-Nuclear-Power-Program

МАГАТЭ 2017, План физической ядерной безопасности на 2018-2021 гг., Док. GC (61) / 24, по адресу: www.iaea.org/About/Policy/GC/GC61 / GC61 Documents / English / gc61-24 ru.pdf

Колесникова 2017, Вызовы для ГЧП во время новых видов угроз безопасности, Доклад о мировой безопасности, по адресу: www.worldsecurity-index.com/

Lindberg & Sundelius 2013, Устойчивость всего общества к стихийным бедствиям: шведский путь, в «Справочнике по национальной безопасности Макгроу-Хилла» (2-е издание) / [ed] Дэвид Камиен, Нью-Йорк: Макгроу-Хилл, по адресу: www.msb.se/Upload/Nyheter_press/McGraw-Hill%20Homeland%20Security%20Handbook,%20Helena%20Lindberg%20and%20Bengt%20Sundelius.pdf

McAfee 2011, «В темноте: критически важные отрасли противостоят кибератакам», второй годовой отчет McAfee по критически важной инфраструктуре, по адресу: www.mcafee.com/in/about/news/2011 / q2 / 20110419-01.aspx

Michel-Kerjan 2018, Финансовая защита критически важной инфраструктуры: неопределенность, страховка и риск терроризма, Institut Veolia Environnement, по адресу:
file:///Users/SM/downloads/financial_protection_of_critical_infrastructure_Un.pdf

NIPC 2002, Заинтересованность террористов в системах водоснабжения и АСУТП, Информационный бюллетень 02-001, 30 января.

NIPP 2013, Партнерство по обеспечению безопасности и устойчивости критически важной инфраструктуры, Департамент внутренней безопасности, 2013, с.15, по адресу:
https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

ОЭСР 2008, Рекомендация Совета по защите критически важных информационных инфраструктур, C (2008) 35, по адресу: www.oecd.org/sti/40825404.pdf

ОБСЕ 2013, Руководство по передовой практике по защите неядерной критически важной энергетической инфраструктуры от террористических атак с акцентом на угрозы, исходящие из киберпространства, 2013, по адресу: www.osce.org/atu/103500?download=true

ОЗХО 2016, Потребности и лучшие практики по химической безопасности и управлению безопасностью, по адресу: www.opcw.org/fileadmin/OPCW/ICA/ICB/OPCW_Report_on_Needs_and_Best Practices on Chemical Safete_and_Security_ManagementV3-2_1.2.pdf

RECIPE 2011, Руководство по надлежащей практике по ЗКИ политики и для политиков в Европе, по адресу: file:///Users/SM/Downloads/RECIPE_manual%20(l).pdf

Shea 2003, Критически важная инфраструктура: системы управления и террористическая угроза, Служба исследований Конгресса, по адресу:
https://fas.org/irp/crs/RL31534.pdf

Синай 2016, Новые тенденции в борьбе с терроризмом в предпринимательском секторе, Институт Маккензи, по адресу:
Http://mackenzieinstitute.eom/new-trends-in-terrorisms-targeting-of-the-business-sector/#reference-27

Швеция 2014, Руководство по повышению безопасности в промышленных информационных и управляющих системах, министерство по чрезвычайным ситуациям, по адресу: https://www.msb.se/RibData/Filer/pdf/27473.pdf

Швеция 2016, Оценка национального риска и возможности, министерство по чрезвычайным ситуациям:
www.msb.se/Upload/Forebyggande/Krisberedskap/National%20risk%20and%20capability%20assessment%202016%20-%20Summary%20English.pdf

Нидерланды, 2018, «Устойчивая критически важная инфраструктура», Национальный координатор по безопасности и борьбе с терроризмом, Министерство юстиции и безопасности, по адресу:
https://english.nctv.nl/binaries/Factsheet%20Critical%20Infrastructure%20ENG%202018_tcm32-240750.pdf

Украина 2017, Разработка системы защиты критически важной инфраструктуры на Украине, Национальный институт стратегических исследований по адресу:
http://en.niss.gov.ua/content/articles/files/niss EnglCollection druk-24cce.pdf

МСУОБ 2009, Терминология по сокращению опасности бедствий, по адресу:
www.unisdr.org/we/inform/publications/7817

UP KRITIS 2014, Государственно-частное партнерство по защите критически важной инфраструктуры - основа и цели, www.upkritis.de

Вишванат 2015, «Водные войны, которые ведет Исламское государство», Стратфор, по адресу: www.stratfor.com/weekly/water-wars-waged-islamic-state

ПРИЛОЖЕНИЕ I - ИЗБРАННЫЕ ГОСУДАРСТВЕННЫЕ РЕСУРСЫ ПО ЗКВОИ[46]

Страна	Название документа	Тип	Описание	Год	Веб адрес
Австралия	Устойчивость критически важных объектаов инфраструктуры: план	Документ по вопросам стратегии / политики	Нацелен на поддержку продолжения работы КВОИ перед лицом всех опасностей. Ключевые результаты, которых Стратегия стремится достичь: 1. Крепкое и эффективное партнерство бизнеса и власти; 2. Улучшенное управление рисками операционной среды; 3. Эффективное понимание и управление стратегическими вопросами; и 4. Зрелое понимание и применение организационной устойчивости. В документе изложены основные мероприятия, которые будут предприняты на национальном уровне для достижения этих результатов.	2015	https://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlan.PDF
Австралия	Национальные руководящие принципы по защите критически важных объектаов инфраструктуры от терроризма	Документ по вопросам стратегии / политики	Дополнить Стратегию устойчивости КВОИ, обеспечив основу для национального подхода по защите КВОИ от терроризма.	2015	https://www.national security.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf
Австралия	Стратегия по кибербезопасности Австралии	Документ по вопросам стратегии / политики	Эта Стратегия кибербезопасности излагает философию и программу правительства Австралии по решению двойных задач цифровой эры - продвижение и защита интересов Австралии в Интернете. Эта стратегия устанавливает пять тем действий для кибербезопасности Австралии в течение следующих четырех лет до 2020 года: национальное кибер-партнерство, сильная киберзащита, глобальная ответственность и влияние, рост и инновации, киберразумная нация.	2016	https://cybersecuritystrategy.pmc.gov.au/index.html
Бельгия	Закон от 1 июля 2011 о безопасности и защите критически важных объектах инфраструктуры	Нормативный документ	Вместе с Королевским указом от 2 декабря 2011 года по критически важной инфраструктуре в подсекторе воздушного транспорта, этот закон представляет собой транспонирование Директивы Совета 2008/114 / ЕС от 8 декабря 2008 года.	2011	https://centredecrise.be/sites/default/files/loi_du_1er_juillet_2011_sur_les_ic_0.pdf
Канада	Система управления чрезвычайными ситуациями в Канаде	Документ по вопросам стратегии / политики	Устанавливает общий подход для различных федеральных, провинциальных и территориальных (FPT) инициатив по управлению чрезвычайными ситуациями. Рамочная основа направлена на обеспечение консолидации совместной работы FPT и обеспечении более согласованных, взаимодополняющих действий среди различных правительственных инициатив FPT. Она подчеркивает ключевые компоненты управления чрезвычайными ситуациями. Она также вводит новые термины и пересматривает существующие	2011	https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-frmwrk/mrgnc-mngmnt-frmwrk-eng.pdf

[46] Документы, представленные в этом Приложении, не образуют какой-либо исчерпывающий перечень существующих государственных ресурсов по ЗКИ. Материалы были отобраны на основе актуальности, открытого и полного доступа через Интернет, географического представительства и наличия переводов на английский язык.

			определения для новых терминов, таких как «все опасности» и «устойчивость», чтобы отразить современные разработки в области управления чрезвычайными ситуациями.		
Канада	Стратегия по кибербезопасности	Документ по вопросам стратегии / политики	Стремится укрепить кибер-системы и сектора КВОИ, опираясь на три основных элемента: обеспечение безопасности государственных систем; партнерство для обеспечения безопасности жизненно важных кибер систем за пределами федерального правительства; помощь канадцам в безопасности в Интернете.	2010	https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf
Канада	Национальная стратегия по критически важным объектам инфраструктуры	Документ по вопросам стратегии / политики	Основываясь на принципах механизма управления чрезвычайными ситуациями, в Стратегии предлагается, чтобы федеральное, провинциальное и территориальное правительства и сектора КВОИ сотрудничали в целях повышения устойчивости КВОИ в Канаде. Сотрудничество основано на развитии партнерских отношений, основанных на существующих мандатах и обязанностях. Для укрепления этих партнерств в Стратегии излагаются механизмы для более эффективного обмена информацией и защиты информации, а также подчеркивается важность подхода к управлению рисками.	2009	https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
Канада	План действий по критически важным объектам инфраструктуры	Документ по вопросам стратегии / политики	Основывается на первоначальном Плане действий 2010 года, дополнительно излагая элементы действий для каждой из целей, изложенных в Национальной стратегии в отношении критически важной инфраструктуры.	2014	https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf
Канада	Центр реагирования на кибер-инциденты	Координационный центр	CCIRC является национальным координационным центром, ответственным за снижение киберрисков, с которыми сталкиваются ключевые системы и службы Канады. CCIRC работает в рамках общественной безопасности Канады в партнерстве с провинциями, территориями, муниципалитетами, организациями частного сектора и международными партнерами. Он координирует национальное реагирование на любые серьезные инциденты кибербезопасности		https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx
Канада-США	Соглашение о сотрудничестве в чрезвычайных ситуациях	Международное соглашение	Излагаются принципы взаимного двустороннего сотрудничества в чрезвычайных ситуациях. Учреждает Консультативную группу Канада - США.	2008	http://www.treaty-accord.gc.ca/text-texte.aspx?id=105173
Канада-США	Система для перемещения товаров и людей через границу во время и после чрезвычайной ситуации	Документ по вопросам стратегии / политики	Излагаются принципы коммуникации и управления границами в случае инцидента (включая явные террористические акты), которые способствуют значительному нарушению работы границы.		www.publicsafety.gc.ca/cnt/ntnl-scrt/cnt/ntnl-nfrstrctr/cnd-ntd-stts-frmwrk-en.aspx
Канада-США	План действий по критически важным объектам инфр-ы	Документ по вопросам стратегии / политики	Нацелен на более эффективное решение ряда вопросов по трансграничной критически важных объектов инфраструктуры и совместной работе по обмену информацией/передовым опытом, определение взаимозависимостей и проведении совместных учений.	2010	https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx

Канада-США	Соглашение о сотрудничестве в чрезвычайных ситуациях	Международное соглашение	Излагаются принципы взаимного двустороннего сотрудничества в чрезвычайных ситуациях. Учреждает Консультативную группу Канада - США.	2008	http://www.treaty-accord.gc.ca/text-texte.aspx?id=105173
Канада-США	Система для перемещения товаров и людей через границу во время и после чрезвычайной ситуации	Документ по вопросам стратегии / политики	Излагаются принципы коммуникации и управления границами в случае инцидента (включая явные террористические акты), которые способствуют значительному нарушению работы границы.		https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cnd-ntd-stts-frmwrk-en.aspx
Канада-США	План действий по критически важным объектам инфраструктуры	Документ по вопросам стратегии / политики	Нацелен на более эффективное решение ряда вопросов по трансграничной критически важной инфраструктуре и совместной работе по обмену информацией/передовым опытом, определение взаимозависимостей и проведении совместных учений.	2010	https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx

Китай	Положение о безопасности и защите КВОИ (проект)	Нормативный документ	Первый проект национального закона, направленный на определение политики Китая по защите КИИ.	2017	https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/ (Unofficial English translation)

Франция	Указ № 2007- 585 от 23 апреля 2007 года о некоторых нормативных положениях первой части Кодекса обороны (на французском языке)	Нормативный документ	Вносит изменения в Кодекс обороны, представляя ряд статей, которые устанавливают институциональные рамки для защиты жизненно важных видов деятельности ("activités d'importance vitale") (см. Статьи R. 1332-1 по 1332-42)	2007	https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B3D2B93BA4D5B3162AC56B149F71F4EC.tplgfr30s_3?cidTexte=JORFTEXT000006615627&dateTexte=20070424
Франция	Белая книга по обороне и национальной Безопасности	Документ по вопросам стратегии / политики	Излагаются основные участники защиты КВОИ в более широком контексте подхода Франции к национальной безопасности	2013	http://www.livreblancdefenseetsecurite.gouv.fr/pdf/the_white_paper_defence_2013.pdf
Франция	Межведомственная инструкция по обеспечению безопасности жизненно важных мероприятий (№ 6600 / SGDSN / PSE / PSN от 7 января	Нормативный документ	Принятая Генеральным секретариатом по обороне и национальной безопасности, Инструкция содержит положения по внедрению французской институциональной архитектуры по защите КВОИ	2014	http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf

	2014)				
Франция	Национальная стратегия по цифровой безопасности	Документ по вопросам стратегии / политики	Излагаются стратегические цели и институциональный подход для обеспечения устойчивости Франции против кибернетических угроз, в том числе угроз против КИИ.	2015	https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
Франция	План «Vigipirate»	Документ по вопросам стратегии / политики	Предусматривает 300 мероприятий, охватывающих 13 основных областей деятельности, таких как транспорт, здравоохранение и сети. Они могут быть активированы в соответствии с развитием угрозы и уязвимостей. На основе оценки террористической угрозы, сделанной разведывательными службами, Генеральный секретариат по обороне и национальной безопасности издает руководящие принципы, определяющие меры, которые должны быть приняты субъектами, занимающимися бдительностью, предотвращением и защитой от угроз террористических действий. Операторы КВОИ должны перевести мероприятия плана VIGIPIRATE в свои планы безопасности.	2015	http://www.gouvernement.fr/sites/default/files/risques/pdf/brochure_vigipirate_gp-bd_0.pdf
Германия	Национальная стратегия защиты КВОИ	Документ по вопросам стратегии / политики	Обобщает цели и задачи федеральной администрации и ее политико-стратегический подход. Стратегия также является отправной точкой для закрепления достигнутых к настоящему времени результатов и их дальнейшего развития с учетом новых проблем.	2009	https://www.kritis.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf?__blob=publicationFile
Германия	Защита КВОИ - Базовая концепция защиты - Рекомендации для компаний	Инструкции/ Практическое руководство	Этот документ, разработанный Федеральным министерством внутренних дел, Федеральным ведомством гражданской защиты и реагирования на стихийные бедствия и Федеральным управлением уголовной полиции, с экспертизой делового сообщества, предоставляет немецким компаниям рекомендации с точки зрения внутренней безопасности.	2006	https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/Baseline%20Protection%20Concept.pdf?__blob=publicationFile
Германия	Стратегия Германии по кибербезопасности	Документ по вопросам стратегии / политики	Обеспечивает оси национальной политики в области кибербезопасности	2011	https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
	Национальный план защиты информационной инфраструктуры	Документ по вопросам стратегии / политики	Нацелен на полную защиту КИИ в Германии, ставя три стратегические цели: профилактика, готовность, устойчивость	2005	http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf
Германия	План реализации ЗКВОИ национального плана защиты информац	Документ по вопросам стратегии / политики	План реализации представляет собой руководство по информационной безопасности для операторов КВОИ, целью которого является содействие принятию политических решений и национальному и международному сотрудничеству, и рекомендуется компаниям в качестве руководства по внедрению адекватного уровня безопасности ИТ.		https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP%20Implementation%20Plan.pdf?__blob=publicationFile

	ионной инфраструктуры				
Германия	UP Kritis - Государственно-частное партнерство по ЗКВОИ	Документ по вопросам стратегии / политики	Обзор достижений и новое видение программы государственно-частного партнерства Германии по ЗКВОИ	2014	https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.pdf?__blob=publicationFile

Япония	Основы политики ЗКВОИ	Документ по вопросам стратегии / политики	Создана в качестве основы для политики, связанной с мерами информационной безопасности для КВОИ Японии.	2015	https://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf
Япония	Стратегия по кибербезопасности	Информационный бюллетень	Устанавливает национальные приоритеты и цели по кибербезопасности и посвящает раздел ЗКВОИ	2015	https://www.nisc.go.jp/eng/pdf/cs-strategy-en-pamphlet.pdf
Япония	Национальная стратегия по безопасности	Документ по вопросам стратегии / политики	Устанавливает фундаментальные подходы страны к национальной безопасности и ее цели. Хотя он не имеет прямого отношения к КВОИ, он предусматривает усиление мер, непосредственно влияющих на КВОИ, таких как укрепление морской и кибербезопасности, разведывательных возможностей и т. д.	2013	https://www.mofa.go.jp/fp/nsp/page1we_000081.html
Япония	Основной закон о кибербезопасности	Нормативный документ	Первый специальный закон о кибербезопасности введенный среди стран G7, в дополнение к обязанностям государства и местных властей по кибербезопасности, предписывает обязанности по кибербезопасности операторов КВОИ, университетов и других образовательных или исследовательских учреждений в экономической сфере. Предполагается, что в будущем обязанности для этих бизнес-операторов могут быть более подробно прописаны в более конкретных законах.	2014	http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&vm=02&id=2760

Малайзия	Портал КИИ	Координационный центр	Онлайн портал, на котором операторы критически важной инфраструктуры работают вместе, обмениваясь информацией по вопросам безопасности, предоставляет информацию о национальной политике кибербезопасности, которая направлена на устранение рисков для критически важной национальной информационной инфраструктуры (КИИ) в десяти критически важных секторах.		https://cnii.cybersecurity.my/main/index.html

Нидерланды	Устойчивые критические и важные инфраструктуры	Информационная брошюра / Информационный бюллетень	Информационный бюллетень, подготовленный национальным координатором по вопросам безопасности и борьбы с терроризмом, иллюстрирует сдвиг, произошедший в 2014 году, в подходе правительства к политике ЗКВОИ.	2018	https://english.nctv.nl/binaries/Factsheet%20Critical%20Infrastructure%20ENG%202018_tcm32-240750.pdf

Новая Зеландия	Пособие по системе национальной безопасности	Документ по вопросам стратегии / политики	Излагает договоренности Новой Зеландии в отношении как управления национальной безопасностью, так и в ответ на потенциальный, возникающий или реальный кризис национальной безопасности. Оно разделено на четыре раздела: • Часть 1. Система национальной безопасности; • Часть 2. Структуры управления национальной безопасностью; • Часть 3. Ответ на потенциальное, возникающее или реальное событие; • Часть 4: Дополнительные приложения	2016	https://www.dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf
Новая Зеландия	Стратегия кибербезопасности	Документ по вопросам стратегии / политики	Устанавливает национальные приоритеты и цели по кибербезопасности и посвящает раздел ЗКВОИ.	2015	https://www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-december-2015.pdf
Новая Зеландия	Национальный центр кибербезопасности (NCSC)	Координационный центр	Основанный в 2011 году, он специализируется на предоставлении специализированных консультаций по вопросам безопасности и поддержки наиболее значимым организациям и информационным системам Новой Зеландии. Он включает в себя правительственные департаменты, ключевых экономических производителей, нишевых экспортеров, исследовательские институты и операторов критически важной национальной инфраструктуры. Центр помогает этим организациям защищать свои сети от типов угроз, которые, как правило, недоступны коммерчески доступным инструментам, и от угроз, которые могут потенциально повлиять на эффективное функционирование государственной администрации или ключевых секторов экономики.	2011	https://www.ncsc.govt.nz/
Новая Зеландия	Стратегия кибербезопасности: годовой отчет по плану действий	Документ по вопросам стратегии / политики	Поддерживает стратегию кибербезопасности, устанавливая конкретные шаги по защите информационно-технологических систем	2015	https://www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-action-plan-december-2015.pdf
Новая Зеландия	Стратегия кибербезопасности: годовой отчет по плану действий	Документ по вопросам стратегии / политики	Это первый годовой отчет о реализации целей, изложенных в Стратегии и плане действий по кибербезопасности 2015 года.	2016	https://www.dpmc.govt.nz/sites/default/files/2017-06/nzcss-action-plan-annual-report-2016.pdf

Польша	Национальная программа по ЗКВОИ	Документ по вопросам стратегии / политики	Излагает основные концепции ЗКВОИ в Польше и разделения труда между заинтересованными сторонами на основе правовых принципов и определений, содержащихся в Законе о кризисном регулировании 2007 года.	2015	http://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf
Польша	Национальная стратегия безопасности	Документ по вопросам стратегии / политики	Определяет национальные интересы и стратегические цели в области безопасности. В разделе о «защитных мерах» в стратегии национальной безопасности прямо упоминается ЗКВОИ.	2014	https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf

Российская Федерация	Закон о безопасно	Нормативный документ	Излагаются базовые основы и принципы обеспечения безопасности российских КВОИ, в	2017	http://en.kremlin.ru/acts/news/55146

	сти КВОИ		том числе основы функционирования государственной системы по выявлению, предотвращению и ликвидации последствий кибератак на информационные ресурсы Российской Федерации. Это унифицированная система, распределенная по всей стране и наделенная возможностями и ресурсами, необходимыми для обнаружения, предотвращения и ликвидации последствий кибератак и реагирования на кибер-инциденты. Федеральный закон устанавливает механизм предотвращения кибер инцидентов на важных компонентах КИИ. Он определяет полномочия государственных органов по обеспечению безопасности КИИ, права и обязанности различных субъектов в этой области.		

Сенегал	Стратегия национальной кибербезопасности	Документ по вопросам стратегии / политики	Включает в себя следующие элементы: - оценка стратегического контекста кибербезопасности в Сенегале, включая текущие и будущие угрозы; - видение правительства о кибербезопасности и достижении стратегических целей; - общие принципы, роли и обязанности, которые могут усилить указанную стратегию; - логическая основа для ее реализации. Стратегическая цель 2 конкретно касается «Укрепления важнейших информационных систем защиты инфраструктуры (КИИ) и информационных систем государства Сенегал».	2017	http://www.numerique.gouv.sn/sites/default/files/SNC2022-vf.pdf

Сингапур	Стратегия национальной безопасности	Документ по вопросам стратегии / политики	Объясняет приоритеты безопасности Сингапура и стратегию, принятую для борьбы с терроризмом, устанавливает архитектуру национальной безопасности, которая организует различные органы вокруг трех основных столпов безопасности политики, операций и развития потенциала и координирующей роли Координационного секретариата национальной безопасности.	2004	https://www.files.ethz.ch/isn/156810/Singapore-2004.pdf
Сингапур	Стратегия кибербезопасности	Документ по вопросам стратегии / политики	Определяет видение, цели и приоритеты Сингапура в области кибербезопасности, в том числе в отношении повышения устойчивости КИИ.	2016	https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf
Сингапур	Агентство по кибербезопасности	Координационный центр	Курирует стратегию кибербезопасности страны. Оно является частью аппарата премьер-министра и управляется министерством связи информации. Среди его целей - защита важнейших секторов, таких как энергетика, водоснабжение и банковское дело.		https://www.csa.gov.sg/
Сингапур	Закон о защите объектов инфраструктуры	Нормативный документ	Учрежден в рамках контртеррористической стратегии Министерства внутренних дел по защите зданий, в которых размещены жизненно важные услуги или в которых много людей. Он стремится обеспечить наличие адекватных мер безопасности в зданиях в качестве средства, чтобы помочь удержать и препятствовать злоумышленникам, а также минимизировать жертвы и ущерб при нападении.	2017	https://sso.agc.gov.sg/Acts-Supp/41-2017/Published/20171031?DocDate=20171031

Сингапур	Законопроект о кибербезопасности	Законодательный акт	Законопроект преследует четыре цели: - Обеспечить основу для регулирования критически важной информационной инфраструктуры (КИИ). Это формализует обязанности владельцев КИИ по обеспечению кибербезопасности в соответствующих КИИ. - Предоставить Агентству кибербезопасности (CSA) полномочия по управлению и реагированию на угрозы и инциденты кибербезопасности. - Создать основу для обмена информацией по кибербезопасности с CSA, и защите такой информации. - Создать легкую систему лицензирования для поставщиков услуг кибербезопасности.	2017	https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en

Испания	Закон 8/2011, устанавливающий меры по КВОИ (на испанском языке)	Нормативный документ	Стремится координировать действия всех государственных органов и содействовать сотрудничеству и вовлечению владельцев и операторов КВОИ. Закон вносит в национальное законодательство меры, включенные в Директиву ЕС 2008/114 / ЕС, в частности, определение и классификацию критически важных инфраструктур в Европе.	2011	http://www.cnpic.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf
Испания	Нормативный документ	Королевский указ 704/2011 об утверждении Положения о защите КВОИ	Реализует рамочные положения, содержащиеся в законе 8/2011.	2011	http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf
Испания	Координационный центр	Национальный центр по ЗКВОИ и кибербезопасности	Министерский орган, отвечающий за продвижение, координацию и надзор за всеми мероприятиями, порученными Министерством внутренних дел в отношении ЗКВОИ на национальной территории.	2007	http://www.cnpic.es/index.html
Испания	Документ по вопросам стратегии / политики	Национальная стратегия по безопасности (на испанском)	Угрозы КВОИ полностью интегрированы в документ как угрозы национальной безопасности.	2017	http://www.cnpic.es/Biblioteca/Eventos/Estrategia_Seguriad_Nacional_2017.pdf
Испания	Документ по вопросам стратегии / политики	Национальная стратегия кибербезопасности (на испанском)	Излагаются цели и подходы стратегии Испании, среди тех, которые имеют отношение к ЗКВОИ	2013	https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf

Швеция	План действий по защите жизненно важных социальных функций и критически важных объектов инфраструктуры	Документ по вопросам стратегии / политики	План действий, подготовленный Шведским гражданским агентством по чрезвычайным ситуациям, создает условия, позволяющие всем жизненно важным социальным функциям и критически важным инфраструктурам осуществлять систематическую работу по обеспечению безопасности своих операций на местном, региональном и национальном уровнях к 2020 году.	2014	https://www.msb.se/RibData/Filer/pdf/27412.pdf
Швеция	Руководство по повышению безопасности в промышленных информационных и управляющих системах	Документ по вопросам стратегии / политики	Руководство, подготовленное Шведским гражданским агентством по чрезвычайным ситуациям, содержит 17 основных рекомендаций по повышению безопасности и благодаря широкому распространению достигло статуса шведского отраслевого стандарта. Рекомендации основаны на международно признанных стандартах, практиках и рабочих методах.	2014	https://www.msb.se/RibData/Filer/pdf/27473.pdf

Швеция	Оценка национального риска и возможностей	Документ по вопросам стратегии / политики	Представляется правительству гражданским агентством по чрезвычайным ситуациям на ежегодной основе, Оценка обеспечивает стратегическую основу для направления и дальнейшего развития при гражданских чрезвычайных ситуациях.	2016	https://www.msb.se/en/Prevention/National-risk-and-capability-assessment/

Швейцария	Национальная стратегия по ЗКВОИ 2018-2022	Документ по вопросам стратегии / политики	Принятая федеральным бюро по защите населения, она обновляет изначальную стратегию 2012 года, устанавливая более высокие цели для заинтересованных сторон. Пересмотренная стратегия должна перевести завершенную работу в институциональный процесс, чтобы закрепить ее в законодательстве и дополнить ее по ситуации.	2017	https://www.babs.admin.ch/fr/aufgabenbabs/ski.html
Швейцария	Национальная стратегия по защите от кибер рисков	Документ по вопросам стратегии / политики	В этой стратегии, федеральный совет, в тесном сотрудничестве с деловым сообществом и операторами КВОИ, стремится снизить кибер риски, которым ежедневно подвергаются все данные участники. Стратегия включает 16 мероприятий для реализации к 2017 году. Новая стратегия вступит в силу в 2018 году.	2012	https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

Великобритания	Национальная стратегия безопасности	Документ по вопросам стратегии / политики	Излагает основы и цели видения страны по защите национальной безопасности. Посвящает раздел по КВОИ.	2015	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
Великобритания	Центр защиты национальных объектов инфраструктуры	Координационный центр	Предоставляет советы по защите и безопасности для предприятий и организаций по всей национальной инфраструктуре. Консультация направлена на снижение уязвимости КВОИ к терроризму и другим угрозам.	2007	https://www.cpni.gov.uk/
Великобритания	Национальный центр кибербезопасности	Координационный центр	Предоставляет консультации и поддержку государственному и частному сектору о том, как избежать угроз компьютерной безопасности.	2016	https://www.ncsc.gov.uk/
Великобритания	План обеспечения безопасности и устойчивости сектора на 2017 год	Документ по вопросам стратегии / политики	Определяет устойчивость наиболее важной инфраструктуры Великобритании к соответствующим рискам, указанным в Национальной оценке рисков. Ежегодно составляются планы для министров, чтобы предупредить их о любых предполагаемых уязвимостях, с программой мер по повышению устойчивости, где это необходимо. Индивидуальные планы классифицируются, но Кабинет министров сводит каждую версию в единый общий план устойчивости сектора для критически важной инфраструктуры.	2017	https://www.gov.uk/government/collections/sector-resilience-plans

Великобритания	Национальный реестр рисков чрезвычайных ситуаций	Документ по вопросам политики	Предоставляет обзор ключевых рисков, которые могут привести к значительным сбоям в Великобритании. Объясняет типы чрезвычайных ситуаций, которые могут возникнуть, что делают правительство и партнеры, чтобы смягчить их, и как вы, в качестве физического лица, семьи или малого предприятия, можете помочь защитить себя. Ряд разделов непосредственно посвящен защите КВОИ от злоумышленных, террористических актов.	2017	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf

Украина	Зеленая книга по ЗКВОИ в Украине	Документ по вопросам стратегии / политики	Формулирует стратегические цели государственной политики в области ЗКВОИ в Украине.	2016	http://en.niss.gov.ua/content/articles/files/niss_EnglCollection_druk-24cce.pdf
Украина	Решение Совета национальной безопасности и обороны о совершенствовании мер по обеспечению защиты критически важных объектов инфраструктуры (введены в действие Указом Президента от 16 января 2016 года №8/2017)	Нормативный документ	Устанавливает график постепенного введения комплексной национальной политики и правовой базы по ЗКВОИ	2016	http://en.niss.gov.ua/content/articles/files/niss_EnglCollection_druk-24cce.pdf

США	Стратегическая национальная оценка риска	Документ по вопросам стратегии / политики	Стремится выявить типы инцидентов, которые представляют наибольшую угрозу для национальной безопасности страны. Критически важные активы, системы и сети сталкиваются со многими классифицированными угрозами, включая террористов и других участников, которые стремятся причинить вред и нарушить работу жизненно важных служб.	2011	https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf
США	Национальный План Защиты Инфраструктуры (NIPP)	Документ по вопросам стратегии / политики	Описывает, как представители правительства и частного сектора в сообществе КВОИ работают вместе для управления рисками и достижения результатов в отношении безопасности и устойчивости.	2013	https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf
США	Президентская политическая директива 21 (PPD-21): Безопасность и устойчивость КВОИ	Нормативный документ	Поручает исполнительной власти: -Развить возможность ситуационной осведомленности, которая Рассматривает как физические аспекты, так и кибер-аспекты того, как инфраструктура функционирует почти в реальном времени -Понимать каскадные последствия сбоя инфраструктуры -Оценивать и развивать государственно-частное партнерство - Обновлять национального плана защиты инфраструктуры -Разработать план комплексных исследований и разработок	2013	https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

США	Распоряжение (ЕО) 13636: улучшение кибербезопасности КВОИ	Нормативный документ	Поручает исполнительной власти: -Разработку добровольной системы технологически-нейтральной кибербезопасности - Содействие и стимулирование принятия практики кибербезопасности -Увеличить объем, своевременность и качество обмена информацией о киберугрозах. - Реализовать высокую защиту персональных данных и гражданских свобод в каждой инициативе, чтобы обеспечить нашу критически важную инфраструктуру - Изучить использование существующих правил для содействия кибербезопасности	2013	https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
США	Безопасность и устойчивость NIPP	Механизм финансировани я	Предоставляет сообществу КВОИ возможность помогать в разработке технологий, инструментов, процессов и методов, которые удовлетворяют насущные потребности и укрепляют долгосрочную безопасность и устойчивость критически важной инфраструктуры. Это помогает выявлять и финансировать инновационные идеи, которые могут предоставить технологии и инструменты для сообщества КВОИ, которые готовы или почти готовы к использованию.	2017	https://www.dhs.gov/sites/default/files/publications/nipp-challenge-overview-fact-sheet-2017-508.pdf

ПРИЛОЖЕНИЕ II - РЕЗОЛЮЦИЯ СОВЕТА БЕЗОПАСНОСТИ 2341 (2017)

«Совет Безопасности,

На основании своих резолюций 1373 (2001), 1963 (2010), 2129 (2013) и 2322 (2016),

Вновь подтверждая свою главную ответственность за поддержание международного мира и безопасности в соответствии с Уставом Организации
Объединенных Наций,

Вновь заявляя о своем уважении суверенитета, территориальной целостности и политической независимости всех государств в соответствии с Уставом Организации Объединенных Наций,

Вновь подтверждая, что терроризм во всех его формах и проявлениях представляет собой одну из самых серьезных угроз международному миру и безопасности и что любые акты терроризма являются преступными и не имеющими оправдания деяниями, независимо от их мотивов, когда бы, где бы и кем бы они ни совершались, и *сохраняя решимость* и далее способствовать повышению эффективности общих усилий по борьбе с этим злом на глобальном уровне,

Вновь подтверждая, что терроризм представляет собой угрозу международному миру и безопасности и что для противодействия этой угрозе требуются коллективные усилия на национальном, региональном и международном уровнях на основе уважения международного права, включая международное право прав человека и международное гуманитарное право, и Устава Организации Объединенных Наций,

Вновь подтверждая, что терроризм не должен ассоциироваться с какой-либо конкретной религией, национальностью, цивилизацией или этнической группой,

Подчеркивая, что активное участие и сотрудничество всех государств и международных, региональных и субрегиональных организаций необходимо для того, чтобы блокировать, ослабить, изолировать и обезвредить террористическую угрозу, и *отмечая* важность осуществления Глобальной контртеррористической стратегии Организации Объединенных Наций (ГКТС), изложенной в резолюции 60/288 Генеральной Ассамблеи от 8 сентября 2006 года, и ее последующих обзоров,

Вновь подтверждая необходимость принятия мер для предотвращения терроризма и борьбы с ним, в частности посредством лишения террористов доступа к средствам для осуществления их нападений, о чем говорится в разделе II Глобальной контртеррористической стратегии Организации Объединенных Наций, включая необходимость активизировать усилия по укреплению безопасности и защиты особо уязвимых объектов, таких как объекты инфраструктуры и места общественного пользования, а также усилению противодействия террористическим нападениям, в частности в области защиты гражданского населения, признавая в то же время, что государствам может потребоваться помощь в этом отношении,

Признавая, что каждое государство само определяет, какие объекты его инфраструктуры являются критически важными и как обеспечить их эффективную защиту от террористических нападений,

Признавая растущее значение обеспечения надежности и устойчивости критически важных объектов инфраструктуры и их защиты от террористических нападений для национальной безопасности, общественной безопасности и экономики соответствующих государств, а также для благосостояния и благополучия их населения,

Признавая, что обеспечение готовности к террористическим нападениям охватывает их предотвращение, защиту от них, смягчение их последствий, реагирование на них и восстановление после них с уделением особого внимания повышению безопасности и устойчивости критически важных объектов инфраструктуры, в том числе, сообразно обстоятельствам, в рамках государственно-частного партнерства,

Признавая, что усилия по защите должны осуществляться в многочисленных областях, таких как планирование; общественная информация и предупреждение; оперативная координация; обмен разведывательными данными и информацией; воспрещение и нейтрализация; скрининг, поиск и обнаружение; контроль доступа и проверка личности; безопасность в кибернетическом пространстве; меры физической защиты; управление рисками в рамках программ и мероприятий по защите; и обеспечение целостности и безопасности производственно-сбытовых цепочек,

Признавая жизненно важную роль, которую просвещенные, бдительные общины играют в повышении осведомленности и информированности о существовании террористических угроз и, в частности, в выявлении подозрительной деятельности и направлении информации о ней правоохранительным органам, и важность расширения осведомленности и участия общественности и государственного-частного партнерства, сообразно обстоятельствам, особенно в отношении потенциальных террористических угроз и факторов уязвимости, путем регулярного проведения диалога, подготовки кадров и информационно-пропагандистских мероприятий на общенациональном и местном уровнях,

Отмечая усиление взаимозависимости между странами в том, что касается критически важных объектов трансграничной инфраструктуры, например таких, которые используются, в частности, для производства, передачи и распределения электроэнергии, воздушного, наземного и морского транспорта, предоставления банковских и финансовых услуг, водоснабжения, распределения продовольствия и общественного здравоохранения,

Признавая, что вследствие усиливающейся взаимозависимости между критически важными инфраструктурными секторами некоторые критически важные объекты инфраструктуры могут оказаться подверженными воздействию все более многочисленных и разнообразных угроз и факторов уязвимости, которые создают новые проблемы в области безопасности,

Выражая озабоченность по поводу того, что террористические нападения на критически важные объекты инфраструктуры могут существенно нарушить функционирование как государственного, так и частного сектора и вызвать цепную реакцию за пределами инфраструктурного сектора,

Подчеркивая, что эффективная защита критически важных объектов инфраструктуры невозможна без применения секторальных и межсекторальных подходов к управлению рисками и что она предусматривает, в частности, выявление террористических угроз и обеспечение готовности к ним для снижения уязвимости критически важных объектов инфраструктуры, предупреждение и пресечение террористических заговоров против критически важных объектов инфраструктуры, когда это возможно, сведение к минимуму последствий и сроков восстановления в случае причинения ущерба в результате террористического нападения, определение причин ущерба или источника нападения, сохранение доказательств нападения и привлечение к ответственности тех, кто несет ответственность за нападение,

Признавая в этой связи, что эффективность защиты критически важных объектов инфраструктуры значительно повышается, если защита осуществляется на основе концепции, учитывающей все угрозы и опасности, в частности связанные с террористическими нападениями, и когда при этом регулярно проводятся предметные консультации и обеспечивается сотрудничество с операторами критически важных объектов инфраструктуры и должностными лицами правоохранительных органов и служб безопасности, отвечающих за защиту критически важных объектов инфраструктуры, и, сообразно обстоятельствам, с другими заинтересованными сторонами, в том числе с владельцами частного бизнеса,

Признавая, что защита критически важных объектов инфраструктуры требует как внутреннего, так и трансграничного сотрудничества с правительственными органами, иностранными партнерами и владельцами частного бизнеса и операторами объектов такой инфраструктуры, а также обмена их знаниями и опытом в том, что касается разработки политики, передовой практики и извлеченных уроков,

Напоминая о том, что в резолюции 1373 (2001) содержится призыв к государствам-членам найти возможности активизации и ускорения обмена оперативной информацией, особенно о действиях или передвижениях террористов или террористических сетей; подделанных или

фальсифицированных проездных документах; торговле оружием, взрывчатыми веществами или материалами двойного назначения; использовании террористическими группами коммуникационных технологий; и угрозе, которую представляет владение террористическими группами оружием массового уничтожения, и сотрудничать, особенно в рамках двусторонних и многосторонних механизмов и соглашений, в целях предотвращения и пресечения террористических нападений,

Отмечая работу соответствующих международных, региональных и субрегиональных организаций, структур, форумов и совещаний по повышению уровня защиты, безопасности и устойчивости критически важных объектов инфраструктуры,

Приветствуя продолжающееся сотрудничество в борьбе с терроризмом между Контртеррористическим комитетом (КТК), Международной организацией уголовной полиции (Интерпол) и Управлением Организации Объединенных Наций по наркотикам и преступности, в частности в вопросах оказания технической помощи и укрепления потенциала, и между всеми другими органами Организации Объединенных Наций и *настоятельно рекомендуя* и впредь взаимодействовать с Целевой группой Организации Объединенных Наций по осуществлению контртеррористических мероприятий (ЦГОКМ) для обеспечения общей координации и согласованности в рамках контртеррористических усилий системы Организации Объединенных Наций,

1. *Рекомендует* всем государствам прилагать согласованные и скоординированные усилия, в том числе на основе международного сотрудничества, в целях улучшения осведомленности и информированности о проблемах, создаваемых террористическими нападениями, и их понимания и повышения тем самым готовности к таким нападениям на критически важные объекты инфраструктуры;

2. *Призывает* государства-члены рассмотреть возможность разработки или дальнейшего совершенствования своих стратегий уменьшения рисков террористических нападений на критически важные объекты инфраструктуры — стратегий, которые должны предусматривать, в частности, оценку и улучшение понимания соответствующих рисков, принятие мер по обеспечению готовности, в том числе эффективного реагирования на такие нападения, а также содействие повышению оперативной совместимости в области безопасности и ликвидации последствий и поддержку эффективного взаимодействия всех заинтересованных сторон;

3. *Ссылается* на свое содержащееся в резолюции 1373 (2001) решение о том, что все государства должны квалифицировать террористические акты как серьезные уголовные правонарушения во внутригосударственных законах и положениях, и *призывает* все государства-члены обеспечить, чтобы они установили уголовную ответственность за террористические акты, направленные на уничтожение или дезактивацию критически важных объектов инфраструктуры, а также за планирование, подготовку, финансирование и материально-техническую поддержку таких нападений;

4. *Призывает* государства-члены изыскать возможности для обмена соответствующей информацией и активно сотрудничать в деле предотвращения террористических нападений, планируемых в отношении критически важных объектов инфраструктуры, и обеспечения защиты от них и готовности к ним, а также смягчения последствий уже совершенных нападений, их расследования, реагирования на них и восстановления после них;

5. *Призывает далее* государства установить или укрепить национальные, региональные и международные партнерские отношения с заинтересованными сторонами, как государственными, так и частными, сообразно обстоятельствам, в целях обмена информацией и опытом и тем самым предотвращения террористических нападений на критически важные объекты инфраструктуры, обеспечения защиты от них, смягчения их последствий, их расследования, реагирования на них и восстановления после причиненного ими вреда, в том числе путем проведения совместных учебных мероприятий и применения или создания соответствующих сетей связи или экстренного оповещения;

6. *Настоятельно призывает* все государства обеспечить, чтобы все их соответствующие национальные ведомства, агентства и другие учреждения тесно и эффективно взаимодействовали в вопросах защиты критически важных объектов инфраструктуры от террористических нападений;

7. *Рекомендует* Организации Объединенных Наций, а также тем государствам-членам и соответствующим региональным и международным организациям, которые разработали надлежащие стратегии защиты критически важных объектов инфраструктуры, сотрудничать со всеми государствами и соответствующими международными, региональными и субрегиональными организациями и структурами в целях выявления и широкого применения передовой практики и мер по регулированию риска террористических нападений на критически важные объекты инфраструктуры;

8. *Подтверждает*, что инициативы в области регионального и двустороннего экономического сотрудничества и развития играют ключевую роль в достижении стабильности и процветания, и в этой связи *призывает* все государства расширять свое сотрудничество в целях защиты критически важных объектов инфраструктуры, в том числе региональных проектов развития сообщения и связанных с ними объектов трансграничной инфраструктуры, от террористических нападений путем использования, сообразно обстоятельствам, двусторонних и многосторонних механизмов обмена информацией, оценки рисков и совместной правоприменительной деятельности;

9. *Настоятельно призывает* все государства, которые в состоянии делать это, оказывать содействие в обеспечении эффективного и целенаправленного наращивания потенциала, профессиональной подготовки и других необходимых ресурсов, технической помощи, передачи технологий и реализации программ, когда это требуется, с тем чтобы все государства могли достичь цели защиты критически важных объектов инфраструктуры от террористических нападений;

10. *Поручает* КТК продолжать, сообразно обстоятельствам и при поддержке Исполнительного директората Контртеррористического комитета (ИДКТК), в рамках их соответствующих мандатов, анализировать усилия государств-членов по защите критически важных объектов инфраструктуры от террористических нападений в контексте осуществления резолюции 1373 (2001) в целях выявления передовой практики, недостатков и факторов уязвимости в этой области;

11. *Рекомендует* в этой связи КТК при поддержке ИДКТК и ЦГОКМ продолжать работать сообща в целях содействия оказанию технической помощи и наращиванию потенциала и повышения осведомленности в области защиты критически важных объектов инфраструктуры от террористических нападений, в частности посредством укрепления своего диалога с государствами и соответствующими международными, региональными и субрегиональными организациями и тесного сотрудничества, в том числе путем обмена информацией со всеми соответствующими двусторонними и многосторонними субъектами, оказывающими техническую помощь;

12. *Призывает* Рабочую группу ЦГОКМ по защите критически важных объектов инфраструктуры, включая Интернет, уязвимые цели и обеспечение безопасности туризма, продолжать оказывать содействие и — в сотрудничестве с другими специализированными учреждениями Организации Объединенных Наций — помощь в укреплении потенциала в интересах более эффективного осуществления таких мер, по просьбе государств-членов;

13. *Просит* КТК представить Совету через двенадцать месяцев обновленную информацию о ходе осуществления этой резолюции;

14. *Постановляет* продолжать заниматься этим вопросом.

ПРИЛОЖЕНИЕ III - ЦЕЛЕВАЯ ГРУППА ООН ПО ОСУЩЕСТВЛЕНИЮ КОНТРТЕРРОРИСТИЧЕСКИХ МЕРОПРИЯТИЙ (ЦГОКМ)

Секретариат, учреждения, фонды и программы Организации Объединенных Наций, а также связанные с ними организации вносят вклад в осуществление глобальной контртеррористической стратегии Организации Объединенных Наций как в рамках своих индивидуальных мандатов, так и путем членства в целевой группе по осуществлению контртеррористических мероприятий.

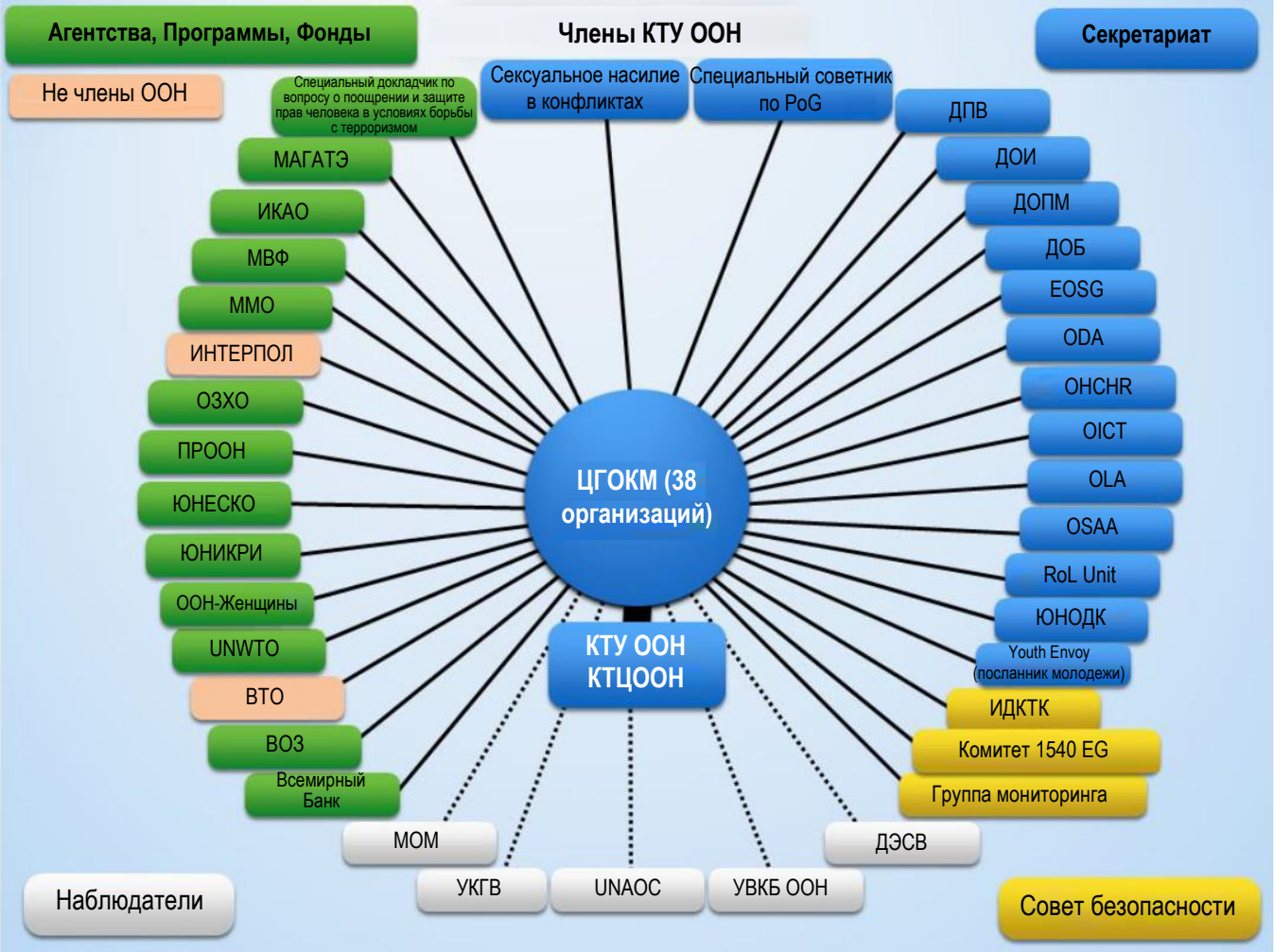
Целевая группа состоит из 38 международных организаций и Интерпола, которые в силу своей работы заинтересованы в многосторонних усилиях по борьбе с терроризмом. Каждый субъект вносит взносы в соответствии со своим мандатом. Члены Целевой группы:

1. Группа еаблюдения по Аль-Каиде/Талибану
2. Исполнительный директорат контртеррористического комитета (ИДКТК)
3. Департамент операций по поддержанию мира (ДОПМ)
4. Департамент по политическим вопросам (ДПВ)
5. Департамент общественной информации (ДОИ)
6. Департамент по вопросам охраны и безопасности (ДОБ)
7. Группа экспертов Комитета 1540
8. Международное агентство по атомной энергии (МАГАТЭ)
9. Международная организация гражданской авиации (ИКАО)
10. Международная морская организация (ММО)
11. Международный валютный фонд (МВФ)
12. Международная организация уголовной полиции (ИНТЕРПОЛ)
13. Управление по вопросам разоружения (ODA)
14. Управление Верховного Комиссара ООН по Правам Человека (OHCHR)
15. Управление по правовым вопросам (OLA)
16. Офис Генерального секретаря (OSG)
17. Офис специального советника по предупреждению геноцида
18. Офис специального представителя генерального секретаря по вопросу о положении детей и вооруженных конфликтах (CAC)
19. Офис посланника генерального секретаря по делам молодежи
20. Организация по запрещению химического оружия (ОЗХО)
21. Специальный докладчик по вопросам поощрения и защиты прав человека в условиях борьбы с терроризмом
22. Программа развития ООН (ПРООН)
23. Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО)
24. Межрегиональный научно-исследовательский институт ООН по вопросам преступности и правосудия (ЮНИКРИ)
25. Управление ООН по наркотикам и преступности (ЮНОДК)
26. Офис специального советника Организации Объединенных Наций по Африке (OSAA)
27. Группа ООН по вопросам верховенства права
28. «ООН-Женщины»
29. Всемирная туристская организация ООН (UNWTO)
30. Всемирная таможенная организация (ВТО)
31. Всемирный банк
32. Всемирная организация здравоохранения (ВОЗ)

Наблюдатели:

33. Международная организация по миграции (МОМ)

34. Управление координатора по гуманитарным вопросам (УКГВ)
35. Департамент ООН по экономическим и социальным вопросам (ДЭСВ)
36. Управление верховного комиссара Организации Объединённых Наций по делам беженцев (УВКБ ООН)
37. Альянс цивилизаций ООН (UNAOC)



В рамках целевой группы была создана рабочая группа по защите критически важной инфраструктуры, включая уязвимые цели, безопасность интернета и туризма.

Мандат:

Мандат рабочей группы взят из глобальной контртеррористической стратегии Организации Объединенных Наций (A / RES60 / 288):

- *«Работать с Организацией Объединенных Наций с должным учетом конфиденциальности, уважения прав человека и соблюдения других обязательств по международному праву, изучить пути и средства для: a) координации усилий на международном и региональном уровнях по борьбе с терроризмом во всех его формах и проявлениях в Интернете» (раздел II, параграф 12);*
- *«Активизировать все усилия по повышению безопасности и защиты особо уязвимых объектов, таких как инфраструктура и общественные места…, признавая при этом, что государствам может потребоваться помощь с этой целью». (Раздел II, параграф 18);*

- *«Призывать Организацию Объединенных Наций сотрудничать с государствами-членами и соответствующими международными, региональными и субрегиональными организациями в целях выявления и обмена передовым опытом для предотвращения террористических нападений на особо уязвимые объекты. Мы приглашаем международную организацию уголовной полиции сотрудничать с генеральным секретарем, чтобы он мог представить предложения на этот счет. Мы также признаем важность развития государственно-частного партнерства в этой области».* (Раздел III, параграф 13).

Учитывая, что в глобальной контртеррористической стратегии подтверждается, что «поощрение и защита прав человека для всех и верховенство права» в качестве «важной для всех компонентов Стратегии», Рабочая группа учитывает правозащитные аспекты в своей работе.

Цели:

Цели рабочей группы ЦГОКМ по защите критически важной инфраструктуры, включая уязвимые цели, безопасность Интернета и туризма, заключаются в следующем:

- создать соответствующие механизмы для содействия разработке и распространению передового опыта по защите уязвимых мест, общественных мест или критически важной инфраструктуры, которые имеют значение для их соответствующих государств и регионов или имеют международное значение;
- укрепить потенциал как государственного, так и частного секторов и активизировать развитие партнерских отношений между государственным и частным секторами в области защиты критически важной инфраструктуры, включая безопасность в Интернете, кибернетической сфере и туризме, с тем, чтобы эффективно предотвращать и реагировать на потенциальные риски и угрозы соответствующим объектам, в том числе путем повышения осведомленности и понимания необходимого баланса между вопросами экономики и безопасности.
- повысить отзывчивость и устойчивость путем продвижения методов планирования, профилактики, кризисного управления и восстановления;
- содействовать обмену информацией и передовым опытом и создать сеть экспертов;
- оказывать поддержку государствам в реализации положений глобальной контртеррористической стратегии ООН, которые имеют отношение к основным направлениям деятельности рабочей группы (как указано в разделе «Мандат» ниже).

Участвующие субъекты:

- Международная организация уголовной полиции (Интерпол) (Председатель)
- ЦГОКМ Офис (сопредседатель)
- Исполнительный директорат контртеррористического комитета (ИДКТК)
- Группа наблюдения по Аль-Каиде / Талибану
- Департамент общественной информации (ДОИ)
- Управление Верховного Комиссара ООН по Правам Человека (OHCHR)
- Специальный докладчик по вопросу о продвижении и защите прав человека и основных свобод в условиях борьбы с терроризмом
- Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО)
- Отделение ООН по наркотикам и преступности / предупреждению терроризма (ЮНОДК / ТРВ)
- Департамент по вопросам охраны и безопасности (ДОБ)
- Межрегиональный научно-исследовательский институт ООН по вопросам преступности и правосудия (ЮНИКРИ)
- Департамент по политическим вопросам (ДПВ)
- Департамент операций по поддержанию мира (ДОПМ)
- Международная организация гражданской авиации (ИКАО)

- Международная морская организация (ММО)
- Программа развития ООН (ПРООН)
- Всемирная таможенная организация (ВТО)
- Всемирная туристская организация ООН (UNWTO)
- Управление по координации гуманитарных вопросов (ОСНА)