Техническое Руководство по Защите Критически Важной Энергетической Инфраструктуры от Террористических Атак

Сентябрь 2024 года

КОНТРТЕРРОРИСТИЧЕСКОЕ УПРАВЛЕНИЕ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ

Глобальная программа по противодействию террористическим угрозам в отношении уязвимых целей

Реализуется в партнерстве с: UNITED NATIONS SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE (CTED) UNAOC United Nations Alliance of Civilizations unicri United Nations Interregional Crime and Justice Research Institute

Техническое руководство по защите критически важной энергетической инфраструктуры от террористических атак

Глобальная программа ООН по защите уязвимых целей от террористических угроз

Сентябрь 2024

Отказ от ответственности

Мнения, выводы, заключения и рекомендации, изложенные в настоящем документе, не обязательно отражают точку зрения Организации Объединенных Наций или любых других привлеченных национальных, региональных или международных организаций. Данный отчет не является руководством, а скорее представляет собой обзор текущей практики, применяемой в разных странах мира. Описанные здесь практики следует рассматривать как актуальные на момент подготовки документа, они не являются обязательными и не отменяют рекомендаций национальных органов власти. Данная публикация дополняет прочую соответствующую текущую работу с опорой на имеющиеся исследования и опыт стран. В ней также учтена работа, проводимая другими международными организациями.

Используемые обозначения и представленные в настоящей публикации материалы не подразумевают выражения какого-либо мнения со стороны Секретариата Организации Объединенных Наций в части правового статуса какой-либо страны, территории, города или района распространения ее полномочий или делимитации ее границ или рубежей.

Содержание данной публикации может быть цитировано или воспроизведено при условии надлежащего указания на источник информации. Контртеррористическое управление ООН (КТУ ООН) просит предоставить копию документа, в котором используется или цитируется данная публикация.

Слова благодарности

Настоящее техническое руководство стало возможным благодаря финансовой поддержке Российской Федерации и Туркменистана. Перевод с английского языка на русский язык подготовлен Антитеррористическим центром государств – участников Содружества Независимых Государств.

Авторские права

405 E 45th Street
New York, NY 10017

Email: OCT-info@un.org
Website: www.un.org/counterterrorism/

Предисловие

Террористы все чаще используют уязвимости государственных и частных коммунальных предприятий, включая критически важную энергетическую инфраструктуру (КВЭИ). Взаимозависимость и взаимосвязанный характер критически важной инфраструктуры (КВИ), расположенной по разные стороны границ, вызывают дополнительные опасения и требуют принятия двусторонних или региональных мер реагирования.

Хотя масштабных террористических атак против КВИ, имеющих значительные каскадные последствия, пока не произошло, сохраняется угроза реализации таких сценариев, что требует от стран принятия адекватных мер по предотвращению, реагированию и обеспечению устойчивости.

Настоящее техническое руководство по защите критически важной энергетической инфраструктуры от террористических атак разработано с целью предоставления должностным лицам государственного сектора, специалистам-практикам, гражданскому обществу, международным и региональным организациям, научным кругам, частному сектору и всем соответствующим заинтересованным сторонам надлежащей передовой практики, инструментов и практических примеров из разных стран мира для поддержки усилий государств-членов по защите КВЭИ.

Генеральная Ассамблея и Совет Безопасности ООН уже на протяжении нескольких лет уделяют пристальное внимание этой теме. В Глобальной контртеррористической стратегии Организации Объединенных Наций (ГКС) в рамках Компонента II, посвященного мерам по предотвращению терроризма и борьбе с ним, государства-члены постановили «активизировать все усилия по укреплению безопасности и защиты особо уязвимых объектов, таких, как объекты инфраструктуры и места общественного пользования, а также повысить эффективность реагирования на террористические нападения и другие бедствия, в частности в области защиты гражданского населения, признавая, что для этого государствам может потребоваться помощь».

В дополнение к более общим призывам к предотвращению этой угрозы, содержащимся в резолюциях 1373 (2001) и 1566 (2004), Совет Безопасности принял резолюцию 2341 (2017), которая стала первым глобальным документом, полностью посвященным важности защиты КВИ от террористических атак. В частности, в этой резолюции Совет напомнил, что все государства-члены должны признать террористические акты серьезными уголовными преступлениями в своем национальном законодательстве и нормативных актах, и призвал их обеспечить установление уголовной ответственности за террористические акты, направленные на уничтожение или выведение из строя КВИ, а также за планирование, подготовку, финансирование и материально-техническую поддержку таких атак.

В резолюции 2396 (2017) Совет Безопасности признал, что «Исламское государство Ирака и Леванта» (ИГИЛ), также известное как ДАИШ, призывала своих сторонников и свои филиалы, особенно иностранных боевиков-террористов, возвращающихся из зон вооруженных конфликтов, планировать и осуществлять нападения на места общественного пользования и объекты коммунального хозяйства. В этой резолюции Совет подчеркнул необходимость создания или укрепления государствами-членами национальных, региональных и международных партнерств с субъектами, как государственными, так и частными, для обмена информацией и опытом в целях предотвращения, защиты, минимизации, расследования, реагирования и восстановления ущерба от террористических атак в отношении уязвимых объектов.

В 2018 году Контртеррористический комитет (КТК) принял дополнение к Мадридским руководящим принципам 2015 года, в котором подчеркивается важность защиты уязвимых объектов, как того требуют принципы 50 и 51. Кроме того, резолюция 2617 (2021) Совета Безопасности также включает конкретные положения о защите КВИ и так называемых уязвимых объектов в рамках нового мандата Исполнительного директората Контртеррористического комитета (ИДКТК) и признает решающую важность сотрудничества с Контртеррористическим управлением ООН (КТУ ООН) в этой области.

В июне 2023 года в ходе восьмого обзора ГКС государства-члены пришли к консенсусу, что защита уязвимых объектов должна стать приоритетом в наших общих действиях по борьбе с терроризмом. Резолюция Генеральной Ассамблеи 77/298 включила два преамбульных и четыре постановляющих пункта по этой теме, осудив террористические атаки на критические энергетические объекты и подчеркнув необходимость объединения всех соответствующих заинтересованных сторон — государств-членов, международных и региональных организаций, частного сектора, гражданского общества и научных кругов — для эффективного противодействия беспрецедентной угрозе, которую представляют террористические атаки в отношении КВИ и уязвимых объектов.

За последние четыре года государства-члены активно адаптировали свои правовые, институциональные и операционные рамки к защите КВЭИ. Это техническое руководство продемонстрирует читателям, с какой скоростью меняется ландшафт защиты КВЭИ.

Глобальная программа ООН по защите уязвимых целей от террористических угроз, реализуемая совместно Контртеррористическим управлением Организации Объединенных Наций (КТУ ООН), Исполнительным директоратом Контртеррористического комитета (ИДКТК), Межрегиональным научно-исследовательским институтом Организации Объединенных Наций по вопросам преступности и правосудия (ЮНИКРИ) и Альянсом цивилизаций Организации Объединенных Наций (АЦООН) в сотрудничестве с Международной организацией уголовной полиции (ИНТЕРПОЛ), с 2021 года оказывает поддержку государствам-членам в наращивании их потенциала, развитии связей между экспертами и выявлении передовой практики в области защиты КВИ. Настоящее техническое руководство по защите критически важной энергетической инфраструктуры от террористических атак дополнит реестр интеллектуальных инструментов, разработанных Программой за последние три года, включая пять технических руководств по защите общественных пространств/«уязвимых» целей и Сборник передовой практики по защите критически важной инфраструктуры.

Я уверен, что данное Техническое руководство, создание которого стало возможным благодаря щедрому финансированию Глобальной программы со стороны Российской Федерации и Туркменистана, станет основополагающим инструментом в этой области на благо всех государств-членов.

Владимир Воронков
Заместитель Генерального секретаря
Контртеррористическое управление Организации Объединенных Наций

Содержание

Вставки

Анализ практических примеров

Инструменты

Таблицы

Сокращения

ADMM	Совещание министров обороны Ассоциации государств Юго-Восточной Азии
ИИ	Искусственный интеллект
ASEAN	Ассоциация государств Юго-Восточной Азии
BCK	Байесовская сеть – Следствие – Знание
CBRNE	Химические, биологические, радиологические, ядерные и взрывчатые вещества
КВЭИ	Критически важная энергетическая инфраструктура
CEII	Сведения о критически важной энергетической инфраструктуре
КВИ	Критически важная инфраструктура
CII	Критически важная информационная инфраструктура
CIP	Защита критически важной инфраструктуры
СНГ	Содружество Независимых Государств
АТЦ СНГ	Антитеррористический центр государств - участников СНГ
ОДКБ	Организация Договора о коллективной безопасности
ИДКТК	Исполнительный директорат Контртеррористического комитета Совета Безопасности ООН
DDos	Распределенный отказ в обслуживании
DoS	Отказ в обслуживании
ГКС	Глобальная контртеррористическая стратегия ООН
ИКТ	Информационно-коммуникационные технологии
СВУ	Самодельное взрывное устройство
Интерпол	Международная организация уголовной полиции
ИГИЛ (ДАИШ)	Исламское государства Ирака и Леванта
СПГ	Сжиженный природный газ
ОБСЕ	Организация по безопасности и сотрудничеству в Европе
ГЧП	Государственно-частное партнерство
PSIM	Управление информацией о физической безопасности
ROUV	Дистанционно управляемый подземный аппарат
ЛСО	Легкое и стрелковое оружие
АСУТП	Автоматизированная система управления технологическим процессом
БАС	Беспилотная авиационная система
БПЛА	Беспилотный летательный аппарат
КТЦ ООН	Контртеррористический центр КТУ ООН
УСРБ	Управление ООН по снижению риска бедствий
ЮНИДИР	Институт ООН по исследованию проблем разоружения
КТУ ООН	Контртеррористическое управление Организации Объединенных Наций

1. Краткое изложение

Объекты энергетики являются привлекательными целями для террористических атак по ряду причин: значительные финансовые затраты и каскадный эффект, психологическое воздействие, публичность и символичность. Потенциально высокие последствия успешных атак могут нанести значительный экономический, социальный и экологический ущерб. Эти атаки могут нарушить мировую экономику, дестабилизировать правительства и привести к массовым жертвам. Психологический эффект таких атак может запугать население и подорвать доверие общественности к способности государств обеспечивать безопасность. Кроме того, атаки на энергетическую инфраструктуру привлекают значительное внимание средств массовой информации, повышая известность террористических группировок и их предполагаемую мощь. Возможность атак в отношении определенных объектов из-за их особой уязвимости еще больше привлекает террористические организации. Помимо этого, террористы могут использовать эти атаки как средство финансирования своих операций за счет выкупа, кражи или вымогательства.

Современные террористические атаки в отношении КВЭИ претерпели значительные изменения, превратившись из символических актов в тщательно спланированные, скоординированные операции, которые часто сочетают физические атаки с использованием информационно-коммуникационных технологий (ИКТ) в вредоносных целях. Тенденция к совершенствованию атак подразумевает, что террористы используют передовые технологии для достижения максимального эффекта. Более того, скоординированные атаки в отношении нескольких объектов могут создать сложные проблемы для систем безопасности и реагирования на чрезвычайные ситуации.

Уязвимости КВЭИ многогранны и обусловлены несколькими неотъемлемыми характеристиками. Объекты КВЭИ, такие как трубопроводы и нефтеперерабатывающие заводы, являются ресурсоемкими и географически распределенными, что усложняет принятие комплексных мер безопасности и увеличивает их стоимость. Рост цифровизации энергетического сектора влечет за собой новые риски информационной безопасности, поскольку зависимость от интеллектуальных устройств и АСУТП создает потенциальные точки входа для атак с использованием ИКТ. Взаимозависимость КВЭИ и других критически важных секторов, таких как транспорт, связь и водоснабжение, усугубляет последствия атак, потенциально приводя к каскадным сбоям в нескольких инфраструктурах.

Быстрое развитие беспилотных авиационных систем (БАС) и связанных с ними технологий увеличило потенциальные угрозы для КВЭИ. БАС предоставляют террористическим группировкам определенные преимущества, такие как удаленное управление и возможность обходить традиционные меры безопасности. БАС можно использовать как для осуществления непосредственных атак, например, для бомбардировки объектов, так и для разведки, сбора важной информации о расположении и уязвимых местах целевой инфраструктуры. Распространение БАС вкупе со снижением их стоимости и расширением возможностей для применения делает их привлекательным и доступным инструментом для террористов. Возможность «роевых» атак с использованием БАС, когда несколько БАС одновременно используются для преодоления обороны, еще больше усложняет ситуацию с безопасностью.

В Техническом руководстве приведены подробные примеры, инструменты и передовой опыт многих стран, а также международных и региональных организаций из разных регионов мира. Эти примеры подчеркивают важность адаптированных национальных стратегий, международного сотрудничества, надежных правовых рамок, эффективной межведомственной координации и государственно-частного партнерства (ГЧП) в усилении мер безопасности против террористических атак.

Эффективная защита КВЭИ требует комплексного подхода к управлению рисками, включающего регулярные оценки уязвимости, в том числе постоянный мониторинг сценариев террористических угроз. Соответственно, требуется адаптировать существующие меры безопасности к меняющимся вызовам. Представленные в Руководстве различные методологии и подходы облегчают оценку рисков и разработку стратегий их минимизации. Выявление и обеспечение безопасности критически важных элементов на КВЭИ имеет решающее значение для снижения уязвимости и повышения устойчивости.

В Техническом руководстве рассматривается несколько ключевых областей, чтобы обеспечить всестороннее понимание проблем, которые необходимо учитывать, и стратегий, которые можно принять для эффективной защиты этих жизненно важных объектов. В введении представлен контекст, область применения, цели и методология Руководства, дается основополагающее понимание значимости защиты КВЭИ и подхода, применяемого для решения этой проблемы. Во второй части «Понимание вызова» рассматриваются мотивы террористических атак на КВЭИ, общие закономерности и характеристики таких атак, а также меняющиеся методы работы террористических групп. Подчеркиваются конкретные уязвимости КВЭИ, включая взаимозависимости с другими критически важными секторами и последствия трансграничных взаимосвязей, а также меняющийся ландшафт безопасности, обусловленный появлением новых технологий и угроз информационной безопасности.

В третьей части «Национальные подходы к снижению связанных с терроризмом рисков для критически важной энергетической инфраструктуры» рассматриваются правовые основы, институциональные механизмы и оперативная готовность. В руководстве подчеркивается важность включения защиты КВЭИ в перечень приоритетов национальной безопасности, установления стандартов и протоколов, а также учета аспектов прав человека. В четвертой части «Международные усилия по защите критической энергетической инфраструктуры» подчеркивается важность трансграничного сотрудничества, международных организаций и межведомственной координации. Подчеркивается необходимость проведения совместных учений, обучения и налаживания связей для эффективного обмена информацией. В пятой части «Защита инфраструктуры возобновляемой и нетрадиционной энергетики» рассматриваются уникальные проблемы, связанные с инфраструктурой возобновляемой и нетрадиционной энергетики, подчеркивается необходимость принятия индивидуальных мер защиты для этого нового сектора.

В настоящем Техническом руководстве подчеркивается необходимость динамичного и гибкого подхода к защите КВЭИ. Благодаря интеграции передовой практики, передовых методов управления рисками и надежных правовых и операционных основ государства-члены могут повысить устойчивость и безопасность своих энергетических инфраструктур. В Руководстве подчеркивается

важность обмена знаниями и сотрудничества между субъектами для эффективного реагирования на меняющийся ландшафт угроз. Обеспечение непрерывного функционирования КВЭИ имеет решающее значение для защиты общества и экономики от разрушительных последствий террористических атак, что самым обеспечивает стабильность и процветание наших сообществ.

Методологически данное Руководство было разработано на основе тщательного изучения документарных документов и благодаря вкладу членов Глобальной программы ООН по защите уязвимых целей от террористических угроз, Глобальной сети экспертов ООН по защите уязвимых целей[1] и Рабочей группы по новым угрозам и защите критически важной инфраструктуры Глобального договора ООН по координации контртеррористической деятельности.

[1] В состав Сети входят более двухсот экспертов из 84 государств-членов, в том числе из государственного сектора, академических кругов, гражданского общества, частного сектора, а также международных и региональных организаций. Для получения более подробной информации: Launch of the United Nations Network of Experts on the Protection of Vulnerable Targets Against Terrorist Attacks и Threat to vulnerable targets.

2. Введение: контекст, область применения, цели и методология

2.1 Контекст

За последние десятилетия террористы все чаще проявляют интерес к нападению практически на все уязвимые цели, включая КВЭИ, из-за потенциальных последствий таких атак. Учитывая жизненно важную роль энергетического сектора в функционировании современных обществ, существующие или возможные физические уязвимости энергетической инфраструктуры делают ее стратегически привлекательной целью для потенциальных злоумышленников. Террористическая атака, которая приводит к повреждению, нарушению или уничтожению энергетической инфраструктуры, с высокой долей вероятности усугубит ее последствия, в том числе в отношении широкого спектра прав человека, учитывая роль, которую такая инфраструктура часто играет в поддержании или обеспечении жизненно важных общественных функций.

Хотя масштабные террористические атаки на КВЭИ, повлекшие за собой существенные каскадные последствия, не были пока осуществлены, угроза по-прежнему весьма значительна и требует от стран разработки адекватных планов превентивных мер, мер реагирования на непредвиденные обстоятельства и мер по обеспечению устойчивости. Учитывая, что террористы адаптируют свои действия к изменениям в сфере безопасности и используют новые технологии, для обеспечения успешного, гибкого и динамичного подхода к повышению защищенности объектов решающее значение имеют сотрудничество государств-членов, обмен опытом и передовой практикой по эффективному противодействию этой угрозе.

В 2017 году Совет Безопасности ООН принял резолюцию 2341 (2017),[2] которая является первым глобальным документом, полностью посвященным важности защиты КВИ от террористических атак. В резолюции Совет Безопасности отмечается, в частности, «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...» (преамбула, S/RES/2341 (2017)). В ней также делается отсылка на резолюцию 1373 (2001),[3] которая призывает, чтобы все государства-члены признали террористические акты серьезными уголовными преступлениями в своем национальном законодательстве и нормативных актах, при этом резолюция 2341 (2017) призывает все государства-члены обеспечить, чтобы они установили уголовную ответственность за террористические акты, направленные на уничтожение или дезактивацию КВИ, а также за планирование, подготовку, финансирование и материально-техническую поддержку таких нападений.

В своем восьмом обзоре Глобальной контртеррористической стратегии Организации Объединенных Наций (A/RES/77/298)[4] Генеральная Ассамблея «решительно осуждает все террористические акты,

[2] S/RES/2341 (2017). Доступ по ссылке S/RES/2341(2017).
[3] S/RES/1373 (2001). Доступ по ссылке S/RES/1373(2001).
[4] A/RES/77/298. Доступ по ссылке A/RES/77/298.

направленные против критически важной инфраструктуры, включая критически важные объекты энергетики…» (пункт 72). В той же резолюции Генеральная Ассамблея также призывает государства-члены активизировать усилия по улучшению безопасности и защиты особо уязвимых объектов и рекомендует им рассмотреть возможность разработки или дальнейшего совершенствования своих стратегий по снижению рисков для КВИ от террористических атак (пункт 74). Кроме того, в резолюции признается важность развития государственно-частного партнерства в этой области и содержится призыв к структурам Глобального договора по координации борьбы с терроризмом, включая КТУ ООН, продолжать оказывать поддержку в наращивании потенциала запрашивающим государствам-членам, а также выявлять и обмениваться передовым опытом в целях предотвращения террористических атак в отношении особо уязвимых объектов.

Государства-члены также уделяют пристальное внимание важнейшей роли надежности поставок энергоносителей для международной безопасности и развития. Генеральная Ассамблея Организации Объединенных Наций приняла несколько резолюций по пункту повестки дня об устойчивом развитии, включая резолюцию A/RES/78/149[5] от 19 декабря 2023 года «Ключевая роль надежной и стабильной энергетической связуемости в обеспечении устойчивого развития», инициированную Туркменистаном. В этой резолюции Генеральная Ассамблея, в частности, предлагает провести в 2024 году международную встречу экспертов для обсуждения стратегий и развития сотрудничества в области укрепления энергетической связуемости и поставок. Резолюция 78/149 стала третьей резолюцией, принятой Генеральной Ассамблеей, в которой признается важность стабильного, эффективного и надежного энергоснабжения и международного сотрудничества в этой области (в т.ч. резолюция A/RES/63/210, принятая в 2008 году, и A/RES/67/263, принятая в 2013 году). В этом контексте правительство Туркменистана провело в Ашхабаде 23 апреля 2009 года Конференцию высокого уровня по надежному и стабильному транзиту энергоносителей и его роли в обеспечении устойчивого развития и международного сотрудничества, в которой приняли участие представители государств-членов, международных организаций и промышленности.

Запущенная в 2021 году Глобальная программа ООН по защите уязвимых целей от террористических угроз (далее «Глобальная программа») отвечает на призыв государств-членов, в том числе через Генеральную Ассамблею (ГКС и резолюция A/RES/77/298 с восьмым обзором) и Совет Безопасности (резолюции 2341 (2017) и 2396 (2017)[6]; а также Мадридские руководящие принципы Совета Безопасности в отношении иностранных боевиков-террористов и Дополнение к ним 2018 года[7]), оказывать государствам-членам поддержку в решении приоритетных задач, устранении пробелов и проблем в защите уязвимых целей, к которым относятся КВИ и общественные места («мягкие» цели). В частности, Совет Безопасности ООН в своей резолюции 2341 (2017) признал «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» (преамбула). Кроме того, Совет Безопасности «призывает все государства прилагать согласованные и скоординированные усилия, в том числе на основе международного сотрудничества, в целях улучшения осведомленности и информированности о проблемах, создаваемых террористическими

5 A/RES/78/149. Доступ по ссылке: A/RES/78/149.
6 S/RES/2396 (2017). Доступ по ссылке: S/RES/2396(2017).
7 S/2018/1177. Доступ по ссылке: Security Council Guiding Principles on Foreign Terrorist Fighters.

нападениями, и их понимания и повышения тем самым готовности к таким нападениям на критически важные объекты инфраструктуры» (пункт 2). Кроме того, Дополнение 2018 года к Мадридским руководящим принципам (S/2018/1177) содержит две конкретные рекомендации (№ 50 и 51) о мерах «по защите критически важной инфраструктуры и уязвимых целей от террористических атак» и подчеркивает необходимость обеспечения эффективного и целенаправленного развития потенциала, обучения и других необходимых ресурсов, а также технической помощи.

Глобальная программа направлена на укрепление потенциала государств-членов по предотвращению, защите, смягчению, расследованию, реагированию и восстановлению после террористических атак против уязвимых целей на национальном, региональном и глобальном уровнях. Мандат Программы охватывает как КВИ, так и «незащищенные» цели или общественные места, а также их подверженность угрозам, связанным с использованием БАС в террористических целях. КТУ ООН осуществляет руководство реализацией Программы в партнерстве с ИДКТК, Альянсом цивилизаций ООН (АЦООН) и Межрегиональным научно-исследовательским институтом ООН по вопросам преступности и правосудия (ЮНИКРИ), а также при консультации с Интерполом.

Глобальная программа уделяет особое внимание сбору и распространению передового международного опыта, а также продуктов и инструментов развития знаний в качестве справочных документов для усиления защиты уязвимых целей от террористических атак. В 2023 году КТУ ООН, ИДКТК и Интерпол выпустили обновленное второе издание Сборника передовой практики по защите критически важной инфраструктуры. Кроме того, в 2022 году КТУ ООН опубликовало пять специализированных модулей, посвященных «незащищенным целям» (т.е. общей защите уязвимых целей; городских центров, туристических объектов, религиозных объектов и БАС). В этом контексте настоящее техническое руководство разработано с целью предоставить государствам-членам доступ к международному передовому опыту и инструментам по защите инфраструктуры энергетического сектора от террористических атак.[8]

2.2 Область применения

В резолюции 2341 (2017) Совета Безопасности Организации Объединенных Наций прямо признается, что «каждое государство само определяет, что составляет его критически важную инфраструктуру» (преамбула). Определения того, что представляет собой КВЭИ, могут существенно различаться в разных странах. Обычно это относится к широкому спектру объектов производства и передачи энергии, таких как трубопроводы, электросети, хранилища, нефтеперерабатывающие заводы, терминалы, суда, танкеры, гидроэлектростанции и атомные электростанции и т.д.

Для целей настоящего документа определение КВЭИ включает объекты, которые обеспечивают добычу (морские нефтяные платформы, компрессорные станции, заводы по производству сжиженного природного газа (СПГ), нефтеперерабатывающие заводы и т.д.), хранение (резервуары для хранения, надземные и подземные хранилища природного газа и т.д.), транспортировку и распределение (трубопроводы и топливные терминалы, морская система погрузки, нефтяные и СПГ-танкеры и т. д.) и передачу источников энергии как внутри одного государства, так и через границу. Например, нефте- и газопроводы могут иметь протяженность в тысячи километров, требуют

[8] Данные публикации доступны по ссылке: https://www.un.org/counterterrorism/vulnerable-targets

больших затрат ресурсов и их сложно полностью обезопасить на каждом участке. Кроме того, инфраструктура может быть рассредоточена географически и пересекать границы нескольких юрисдикций. Даже в пределах одного государства она может принадлежать, эксплуатироваться и использоваться разными субъектами.

Учитывая большой опыт многих государств-членов в защите инфраструктуры традиционного энергетического сектора и высокую уязвимость этого сектора к террористическим атакам, в исследовании в основном рассматривается международная практика защиты нефтегазовой инфраструктуры, которая может быть применена и к другим секторам энергетики. Защита секторов возобновляемой и нетрадиционной энергетики будет рассмотрена в шестой главе настоящего Технического руководства.

2.3 Цель

Техническое руководство содержит передовой международный опыт, инструменты, подходы и справочные материалы по защите КВИ в секторе энергетики от террористических атак. Целью доклада не является выработка общепринятого на международном уровне определения понятия «КВЭИ», а скорее обмен полезными подходами и методами, используемыми во всем мире для противодействия террористическим угрозам в отношении КВЭИ. Таким образом, в настоящем документе приводятся примеры, передовой опыт и инструменты, которые помогут политикам, практикам, исследователям и другим государственным и частным субъектам предотвращать или минимизировать последствия террористических атак на энергетическую инфраструктуру. То есть, Руководство предназначено для использования в качестве практического пособия.

Международный опыт, практика, инструменты и другие соответствующие материалы, собранные в ходе проведения данного исследования, образуют цифровую библиотеку по защите энергетической инфраструктуры и доступны членам Глобальной сети экспертов ООН по защите уязвимых целей на платформе Connect and Learn КТУ ООН.

2.4 Методология

Данное Руководство было разработано на основе тщательного изучения открытых источников информации и материалов, поступивших от членов Глобальной программы ООН по защите уязвимых целей от террористических угроз, Глобальной сети экспертов ООН по защите уязвимых целей, Рабочей группы по новым угрозам и защите критически важной инфраструктуры Глобального договора ООН по координации контртеррористической деятельности и сотрудников КТУ ООН.

Кроме того, в исследовании использовались такие методологические инструменты, как опросы, специализированные инструменты сбора данных и тематические исследования, которые позволяют проводить углубленный анализ конкретных тем. Таблицы включены для того, чтобы позволить читателям легко находить меры, принятые в разных странах, и помочь им сформулировать те из них, которые наилучшим образом соответствуют их собственному институциональному и национальному контексту. Техническое руководство содержит передовой международный опыт в области как правовых, так и оперативных основ для предотвращения, минимизации или ликвидации последствий террористических атак на энергетические объекты.

3. Понимание вызова

3.1.1. Почему террористы выбирают в качестве цели критически важные объекты энергетики

Безопасная энергетическая инфраструктура жизненно важна для современного общества. Перебои в энергоснабжении могут иметь катастрофические последствия, такие как экономические потери, социальные беспорядки, ухудшение состояния окружающей среды и снижение качества жизни, а также иметь далеко идущие последствия для широкого спектра прав человека.

В последние десятилетия критически важные объекты энергетики часто становились целями террористических организаций. Изучение инцидентов на газопроводах показывает, что преднамеренные действия являются наиболее частой причиной повреждений.[9] Эти объекты представляют собой привлекательную цель для террористов, стремящихся повлиять на мировую экономику, нарушить цепочки поставок или вызвать массовые жертвы.

В период с 1970 по 2018 год произошло почти 2000 нападений, основной целью которых стала энергетическая инфраструктура (во многих случаях объекты газовой или нефтяной промышленности).[10] Согласно исследованию, основанному на статистике Глобальной базы данных по терроризму Мэрилендского университета (США), в период с 1970 по 2018 год финансовые издержки физического ущерба в результате нападений на энергетическую инфраструктуру были выше, чем в других секторах (около 234–552 тыс. долларов США на каждый инцидент).[11] Более того, успешные атаки на объекты энергетики могут сказать на дефиците энергии, что приведет к экономическим потерям и ущербу окружающей среде.

ИГИЛ (ДАИШ) и «Аль-Каида» и их филиалы продолжают совершать атаки на объекты, связанные с нефтегазовой промышленностью. Среди инцидентов можно назвать, среди прочего, взрыв газопровода в пригороде Дамаска (Сирия) в 2020 году, который привел к отключению электроэнергии в городе и его окрестностях;[12] а также вооруженное нападение на город Пальма, расположенный недалеко от завода «Mozambique LNG», в 2021 году, что привело к эвакуации более 2500 человек.[13]

ИГИЛ (ДАИШ) в Ливии объявило иностранные нефтяные объекты в стране законной целью, осуществив вооруженные нападения на штаб-квартиру Ливийской национальной нефтяной корпорации в Триполи и нефтяные месторождения в стране в 2018 году,[14] а также на нефтяной объект Зиллах в 2019 году, в результате чего погибли пять человек.[15] Эти инциденты, наряду с нападениями

---

9 Donya Fakhravar, Nima Khakzad, Genserik Reniers, Valerio Cozzani, *Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network*, Process Safety and Environmental Protection, Volume 111, 2017, Pages 714-725, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2017.08.036.

10 Lee, Chia-yi. (2022). *Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructure*. Energy Research & Social Science. 87. 102459. 10.1016/j.erss.2021.102459.

11 Лаврухин, М. *Терроризм в энергетической промышленности.* Энергетическая политика, том 179, 2023. стр. 24-37. https://doi.org/10.46920/2409-5516.2023_1179.24.

12 Доступно по ссылке: https://www.reuters.com/article/us-syria-blast-electricity/explosion-on-syria-gas-pipeline-a-terrorist-attack-minister-idUSKBN25K062/.

13 Доступно по ссылке: https://totalenergies.com/media/news/press-releases/mozambique-lng-totalenergies-response.

14 Доступно по ссылке: https://www.aljazeera.com/news/2018/9/10/libya-national-oil-corporations-tripoli-offices-attacked.

15 Доступно по ссылке: https://www.aa.com.tr/en/energy/energy-security/daesh-attacks-oil-facilities-in-libya/26031.

на трубопроводы в Йемене, на Синайском полуострове и в Ираке, демонстрируют постоянную угрозу энергетической инфраструктуре со стороны террористических группировок.

Вставка 1

Причины, по которым объекты энергетики привлекают террористов

Соответствующие исследования осуществления актов терроризма в отношении энергетического сектора показывают, почему КВЭИ является привлекательной целью. К таким причинам относятся[16]:

- Высокие финансовые потери и каскадные эффекты: успешно проведенное нападение может привести к масштабным и трудно поддающимся количественной оценке последствиям. Например, нападение «Аль-Каиды» на алжирское газовое месторождение в 2016 году существенно повлияло на добычу в стране;[17]
- Запугивание (психологический эффект): нападения на энергетическую инфраструктуру могут иметь глубокий психологический эффект на тех, кого они непосредственно затрагивают. Эти атаки также могут быть направлены на дестабилизацию страны или работы конкретной компании путем подрыва их способности обеспечивать безопасность.[18] Например, после теракта в Мозамбике французская нефтяная компания Total приостановила свою деятельность из соображений безопасности, поставив под угрозу инвестиции в размере 20 миллиардов долларов США в объекты по сжижению газа в стране.[19]
- Публичность и символизм: некоторые нападения направлены не на нанесение существенного ущерба, а на привлечение внимания к деятельности террористической группировки. Кроме того, некоторые нападения зачастую способствуют вербовке — например, если такие нападения приносят пользу определенному району и приводят к улучшению подачи энергии и предоставлению общественных услуг сообществу, большее количество мужчин и женщин может почувствовать тягу к поддержке террористической группировки.[20]
- Возможность осуществления нападения: уровень защищенности и возможности террористической группировки определяют возможность осуществления нападения. Относительно легкий доступ может побудить террористов нанести удар.
- Финансирование: в некоторых исследованиях указывается, что нападения на объекты энергетики считаются неотъемлемой частью стратегии по финансированию дальнейшей террористической деятельности. Такой подход, например, используют террористические группировки, такие как ИГИЛ (ДАИШ) в Ираке и Сирии.[21] Террористы могут похищать персонал и требовать выкуп с энергетических объектов, а также захватывать нефтяные или танкеры для транспортировки СПГ. Террористические группы могут также финансировать и поддерживать нападения посредством других противоправных действий, таких как кража нефти или газа из трубопроводов, вымогательство или продажа сырья.[22]

16 Lee, Chia-yi. (2022). *Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructure*. Energy Research & Social Science. 87. 102459. 10.1016/j.erss.2021.102459; Toft, Peter & Duero, Arash & Bi, Ar. (2010). Terrorist targeting and energy security. Energy Policy. 38. 4411-4421. 10.1016/j.enpol.2010.03.070.; James A. Piazza, *Oil and Terrorism: An Investigation of Mediators*, Public Choice 169 (2016): 251–68, https://doi.org/10.1007/s11127-016-0357-0.

17 Доступно по ссылке: https://www.reuters.com/article/idUSKCN0WL0AM/.

18 Piazza James A., *Oil and Terrorism: An Investigation of Mediators*, Public Choice 169 (2016): 251–68, https://doi.org/10.1007/s11127-016-0357-0.

19 Доступно по ссылке: https://www.reuters.com/world/africa/frances-total-declares-force-majeure-mozambique-lng-project-2021-04-26/.

20 Это имело место, например, в отношении инфраструктур, связанных с водными ресурсами. См. UNOCT-CTED *Compendium of Good Practices on Critical Infrastructure Protection*, p. 27.

21 Tichý, Lukáš. (2019). *Energy Infrastructure as a Target of Terrorist Attacks from the Islamic State in Iraq and Syria*. International Journal of Critical Infrastructure Protection. 25. 10.1016/j.ijcip.2019.01.003.

22 Там же.

3.1.2. Общие закономерности и характеристики террористических атак на КВЭИ

За последние несколько десятилетий тактика и методы совершения террористических атак на энергетическую инфраструктуру претерпели изменения. Сегодня эксперты предупреждают о переходе террористических атак от символических к тщательно спланированным скоординированным физическим и виртуальным атакам, т.е. использованию ИКТ в противоправных целях.[23] В некоторых случаях террористические действия носят еще более изощренный характер: нападения на физические объекты энергетической инфраструктуры сопровождаются атаками на их системы управления и/или другие технологии на базе ИКТ.

Несмотря на многообразие террористических атак на критически важные объекты энергетики, их можно классифицировать по следующим критериям:

- Природа (физическая или информационная): в то время как физическое нападение направлено на уничтожение инфраструктуры, ее ослабление или вывод из строя полностью или частично, использование ИКТ в вредоносных целях направлено на отключение или ограничение доступа к технологическим системам, имеющим решающее значение для функционирования энергетической инфраструктуры, и/или на фальсификацию данных.
- Происхождение (внутреннее или внешнее): эффективная защита энергетической инфраструктуры от внешних нападений, которые являются наиболее распространенными, требует от заинтересованных сторон принятия многочисленных мер. Внутренние угрозы возникают, когда сотрудники, поставщики или подрядчики, имеющие доступ к конфиденциальной информации, злоупотребляют своими полномочиями в целях использования уязвимостей внутри организации. Эти угрозы представляют значительную угрозу безопасности КВЭИ и являются серьезной проблемой. Несмотря на то, что объект может быть хорошо защищен от внешних нападений, внутренние нарушители все равно могут получить доступ к ценной информации и нанести значительный ущерб.
- Контекст, в котором они происходят (отдельные или множественные цели): нападения на объекты энергетики могут быть как изолированным актом, так и частью более широкого и сложного плана по нанесению ущерба энергетической инфраструктуре, например, различным объектам или частям инфраструктуры, расположенным в одном районе. Как уже отмечалось, в последние годы террористические группировки продемонстрировали свою способность планировать и осуществлять сложные атаки одновременно в отношении нескольких целей. С ростом стабильности энергетической инфраструктуры частота подобных нападений может увеличиться, поскольку для осуществления обесточивания террористам необходимо одновременно отключить несколько линий электропередач.[24]

[23] Wang L., Wang X., Zhao Q., Zhao Y. *Multi-objective policing emergency logistics scheduling on multi-location coordinated terrorist attacks*, 2017, Xitong Gongcheng Lilun yu Shijian/System Engineering Theory and Practice. 37, доступно на: https://www.researchgate.net/publication/322482361_Multi-objective_policing_emergency_logistics_scheduling_on_multi-location_coordinated_terrorist_attacks.

[24] Lilliestam, J. (2014): *Vulnerability to terrorist attacks in European electricity decarbonisation scenarios: comparing renewable electricity imports to gas imports*, Energy Policy 66, pp. 234-248, Доступ по ссылке: http://dx.doi.org/10.1016/j.enpol.2013.10.078.

- Уровень планирования (спонтанный/специальный или скоординированный): нападения могут быть разовыми, несистемными по своей природе или быть частью сложной стратегии, включающей различные этапы и фазы планирования, которые могут варьироваться от выявления наиболее уязвимых частей объекта до одновременного раскрытия различных зон.
- Выбор целей (непосредственная или косвенная): в то время как непосредственное нападение направлено на нарушение функционирования инфраструктуры посредством воздействия на цель, косвенные атаки могут спровоцировать нарушение в результате атак на другие КВИ, что приведет к «каскадному эффекту».

3.1.3. Методы осуществления террористических нападений

Анализ террористических нападений показывает, что осуществленные в последнее время нападения на КВЭИ можно классифицировать следующим образом:

- Вооруженное нападение. Такие нападения могут быть предприняты с целью:
  - Захвата объектов: террористические группы могут попытаться захватить объект энергетической инфраструктуры, который в свою очередь может использоваться для финансирования террористической деятельности.
  - Захвата заложников: террористы могут похищать персонал энергетических объектов с целью получения выкупа или получения инсайдерской информации.

  Недавний пример такого нападения датируется маем 2023 года, когда 50 террористов напали на объекты нефтеперерабатывающего завода компании MOL Pakistan Oil and Gas Company в районе Хангу (Пакистан).[25]
- Нарушение физических структур критически важных энергетических объектов путем:
  - Диверсии, минирования, взрыва бомбы: объекты энергетики, такие как трубопроводы, можно заминировать и уничтожить дистанционно. Например, большинство нападений ИГИЛ (ДАИШ) на газопроводы на Синайском полуострове (Египет) были совершены путем минирования объекта.[26]
  - Поджог: энергоснабжение, в частности, обеспечение нефтью и газом, предполагает хранение и транспортировку взрывоопасных жидкостей. Эти жидкости особенно уязвимы к открытому огню и поджогам и могут нанести огромный ущерб.
- Нападения с использованием ИКТ: нападения на энергетическую инфраструктуру могут быть направлены, в частности, на промышленные системы управления с целью уничтожения или ограничения функциональности служб КВИ.[27] Такие нападения могут быть направлены на одного поставщика услуг, но их воздействие может иметь каскадный характер и нарушать работу других взаимозависимых инфраструктурных служб. Нападения с использованием ИКТ на энергетическую инфраструктуру могут быть направлены на повреждение систем промышленной

[25] Доступен на: https://www.reuters.com/world/asia-pacific/islamist-militants-kill-six-gas-oil-extraction-plant-pakistan-2023-05-23/.
[26] Доступен на: https://www.aljazeera.com/economy/2020/2/3/gas-pipeline-in-egypts-sinai-attacked-israel-imports-unaffected; https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=202012240006.
[27] Более подробную информацию и статистику можно найти в отчетах «Лаборатории Касперского» об основных инцидентах в области безопасности промышленных информационно-коммуникационных технологий за 2020, 2021, 2022, 2023 годы, доступных по адресу: https://ics-cert.kaspersky.com/publications/reports/.

автоматизации и управления, несанкционированный доступ к системам или данным, отключение или ограничение доступа к критически важным системам или повреждение физического оборудования из-за нарушения технологического процесса.

3.2 Уязвимости КВЭИ

Хотя до настоящего времени не было зафиксировано ни одного масштабного террористического нападения на энергетическую инфраструктуру со значительными каскадными эффектами, эта угроза достаточно значительна, чтобы потребовать от государств-членов принятия адекватных превентивных мер и планов действий в чрезвычайных ситуациях на основе существующих правовых рамок. Действительно, осуществленные в прошлом террористические акты выявили уязвимость ряда энергетических объектов.

3.2.1. Факторы уязвимости, характерные для КВЭИ

Конкретные уязвимости КВЭИ обусловлены несколькими факторами:

- Зависимость от широкого спектра ресурсов, включая воду, телекоммуникации, данные, финансы и другие, может привести к ситуации, когда даже незначительное воздействие или кратковременный сбой могут привести к нарушению работоспособности всего объекта и связанных с ним отраслей. Такая зависимость имеет значительные последствия для населения, учитывая решающую роль, которую эта инфраструктура часто играет в поддержании и обеспечении жизненно важных общественных функций. В свою очередь, нападения также могут иметь далеко идущие последствия для широкого спектра прав человека: от права на жизнь и безопасность личности до права на здоровье и здоровую окружающую среду, права на образование, а также других аспектов права на достаточный уровень жизни.
- Значительные проблемы создают протяженность и географическая разбросанность объектов транспортировки энергоносителей, таких как нефте- и газопроводы. Такие трубопроводы, являющиеся неотъемлемой частью КВЭИ, могут простираться на тысячи километров, что затрудняет и удорожает их комплексную физическую защиту. Основными характеристиками трубопроводов являются их большая протяженность, прохождение по территории нескольких стран и относительно легкий доступ. Кроме того, инфраструктура часто пересекает границы нескольких юрисдикций и международных вод, что затрудняет усилия по предотвращению террористических атак. Даже в пределах одного государства права собственности и управление часто раздроблены между различными субъектами, включая государственные структуры, частные компании и местные сообщества. Такая раздробленность может создавать оперативные, организационные и коммуникационные препятствия, затрудняя эффективное реагирование на потенциальные террористические угрозы.
- Интенсивная цифровизация энергетического сектора создала зависимости от функционирования информационных и управляющих систем. Во многих странах энергетический сектор является лидером цифровой трансформации, используя Интернет вещей,[28] технологии ИИ и системы дистанционного управления. В результате широкое использование дистанционного управления и

[28] Интернет вещей — это система взаимосвязанных вычислительных устройств, способных собирать и передавать данные по беспроводной сети без участия человека.

интеллектуальной обработки данных привело к высокой зависимости от стабильности и правильности работы информационных систем, поддерживающих эти процессы. В этом контексте все большую актуальность приобретают различные уязвимости, связанные с безопасностью информационно-коммуникационных технологий, такие как искажения систем мониторинга и несанкционированный доступ к системам управления.

- Высокая зависимость энергетической инфраструктуры от других важнейших секторов, таких как надлежащее функционирование цепочек поставок и транспортных систем, имеет решающее значение для своевременного и безопасного перемещения сотрудников, оборудования и других необходимых ресурсов. Кроме того, водоснабжение систем охлаждения и телекоммуникационных систем имеет решающее значение для хранения данных, передачи и дистанционного управления КВЭИ.
- Сложные, наукоемкие и технологические процессы, используемые в операциях КВЭИ, создают высокий риск внутренних угроз. Источником этих угроз могут быть сотрудники, подрядчики, отдельные лица или другие лица, тесно связанные с объектом энергетики и обладающие соответствующими знаниями и доступом к конфиденциальной информации, что может способствовать успешному осуществлению нападения. Сочетание сложных операционных процессов и возможности злоупотребления доступом со стороны инсайдеров подчеркивает острую необходимость в надежных мерах безопасности для защиты от этих внутренних угроз.
- Уязвимости, присущие конкретному объекту (производство, хранение, передача и распределение), добавляют еще один уровень риска. Характер объекта энергетики, в том числе наличие на нем высокоопасных конструкций, таких как газоперекачивающие агрегаты, создает дополнительные уязвимости, связанные с его специфическими функциями. Например, электросети, которые тесно взаимосвязаны и часто зависят от централизованного управления, более подвержены атакам с использованием ИКТ, чем физическим нападениям.
- Уязвимости, характерные для местоположения:
    - Климатические и погодные условия: Меры защиты не одинаково эффективны в районах с различными климатическими и погодными условиями. Это может создать дополнительные уязвимости. Например, средства обнаружения БАС могут работать некорректно в районах с преимущественно туманной или дождливой погодой.[29]
    - Высокий уровень активности местных террористических группировок. В частности, для КВЭИ, расположенных в регионах с социально-экономической нестабильностью и высоким уровнем вербовки террористов, риск стать объектом нападений может быть выше.
    - Легкий доступ в связи с географическим положением. Например, эксперты отмечают, что морские районы подвержены большему риску из-за их, как правило, более низкого уровня контроля по сравнению с наземной инфраструктурой.[30]

[29] Luo K., Luo R, Zhou Y. et al (2021) *UAV detection based on rainy environment*, 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), доступ по ссылке: https://ieeexplore.ieee.org/document/9482383.

[30] T. Prodan, *Maritime Terrorism and Resilience of Maritime Critical Infrastructure*, National Security and the Future, 1-2/18 (2017), p. 103. pp. 103-122.

Таблица 1

Уязвимости различных типов нефтегазовых объектов

Нефтяные и СПГ танкеры	Из-за своих размеров и относительно низкой скорости нефтяные танкеры более уязвимы для физических нападений, в том числе со стороны БАС, чем другие суда. Кроме того, нефтяные танкеры часто следуют по предсказуемым маршрутам, проходят через узкие проливы и контрольно-пропускные пункты, которые ограничивают их маневренность, что делает их более легкой мишенью для злоумышленников. Международные правила и соображения безопасности обычно ограничивают возможность оборудования нефтяных танкерах системами вооружения, что делает их более уязвимыми с точки зрения захвата террористами.
Наземные нефтяные и газовые трубопроводы	Нефте- и газопроводы обеспечивают транспортировку легковоспламеняющихся веществ под высоким давлением, что делает их уязвимыми к разрыву и возгоранию в случае повреждения взрывчатыми веществами. Из-за их большой протяженности и расположения как в густонаселенных, так и в отдаленных, малонаселенных районах обычно трудно предотвратить или даже обнаружить попытки заложить бомбы вдоль трубопроводов. Террористы часто прячут взрывчатку вблизи или под трубопроводной инфраструктурой. Например, в 2020 году ИГИЛ (ДАИШ) повредило газопровод на Синайском полуострове в Египте, взорвав бомбу, заложенную под объектом.[31]
Подводные нефтяные и газовые трубопроводы	Подводные объекты трудно защитить традиционными средствами, такими как патрулирование или наблюдение. Их безопасность в основном контролируется компьютерными системами, которые получают данные/оповещения от различных датчиков, которые можно отключить или манипулировать.
Нефтеперерабатывающие заводы, нефтегазовые заводы	Сложность технологических процессов, реализуемых на нефтегазовых и нефтеперерабатывающих заводах, существенно увеличивает риск диверсии со стороны сотрудников. Кроме того, на таких объектах обычно работает большое количество персонала, привлекаются внешние поставщики и подрядчики, что создает дополнительные трудности в предотвращении инсайдерских угроз. Террористическая атака в отношении газового завода Tigentourine в Алжире в 2013 году продемонстрировала, что такие объекты уязвимы для прямых атак, особенно если они поддержаны изнутри, и могут привести к многочисленным жертвам.[32]
Портовые терминалы	По своей природе портовые терминалы сталкиваются с естественными проблемами безопасности. Они требуют обеспечения доступа с суши и моря и часто расположены в густонаселенных районах, что создает сложности с обеспечением безопасности. Из-за высокой интенсивности процессов и загруженности портов обеспечение безопасности на входе зачастую представляет собой сложную задачу, подвергая порты риску диверсии и других видов преступной деятельности. Зачастую морские порты имеют хранилища нефти или СПГ, а также нефтеперерабатывающие заводы или примыкают к ним, что влечет за собой дополнительную уязвимость.

31 Доступен на: https://www.aljazeera.com/economy/2020/2/3/gas-pipeline-in-egypts-sinai-attacked-israel-imports-unaffected.

32 The *In Amenas Attack, Report of the Investigation into the Terrorist Attack on In Amenas*, Statoil, February 2013, доступ по ссылке: www.statoil.com/en/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf.

	Более того, большинство операторов морских портов используют высоко интегрированные информационные системы, которые могут подвергаться атакам с использованием ИКТ.
Морские нефтяные платформы	Из-за своего удаленного расположения нефтяные платформы сталкиваются со значительными проблемами безопасности. Их изоляция затрудняет быстрое развертывание дополнительных сотрудников службы безопасности или подкреплений в ответ на такие угрозы, как поджоги или инсайдерские атаки.
Резервуары для хранения нефти и СПГ	В хранилищах содержится значительное количество взрывоопасных материалов. Поэтому резервуары для хранения более уязвимы для взрывчатых веществ, включая атаки с использованием БАС.

Вставка 2

Инсайдерская угроза энергетической инфраструктуре

Терроризм в виде инсайдерской угрозы принимает форму противоправных действий со стороны сотрудников, подрядчиков, иных лиц, тесно связанных с энергетическим объектом и обладающих соответствующими знаниями и доступом к конфиденциальной информации, которые могут способствовать успешной атаке на КВЭИ в террористических целях.[33] В этой связи инсайдерские угрозы представляют собой серьезную проблему безопасности энергетической инфраструктуры, поскольку успешная инсайдерская атака может нанести ущерб активам и прервать предоставление критически важных услуг, от которых зависит общество.

Сложные, наукоемкие и технологические процессы, используемые в операциях КВЭИ, создают высокий риск инсайдерских угроз. За последние годы энергетический сектор значительно развился, отчасти из-за глобализации и увеличения объемов аутсорсинга. Хотя инсайдерские угрозы часто связаны с сотрудниками или подрядчиками объектов, в некоторых случаях они также касаются деятельности посторонних лиц, которые могут собирать конфиденциальную информацию. Диверсификация поставщиков, краткосрочный найм и другие факторы иногда снижают способность операторов КВЭИ осуществлять тщательную проверку персонала. В этой ситуации необходима система упреждающих мер и раннего оповещения.

Меры безопасности для предотвращения инсайдерских атак могут включать:

- Проведение занятий для сотрудников служб безопасности: проведение регулярных учебных занятий для сотрудников службы безопасности с целью повышения их готовности и реагирования.
- Комплексная проверка сотрудников: внедрение процедур тщательной проверки биографических данных и отбора всех потенциальных сотрудников для минимизации инсайдерских угроз.
- Психологическое тестирование и мониторинг поведения: возможность проведения психологической оценки и мониторинга поведения в качестве потенциальных инструментов выявления лиц, которые могут представлять угрозу безопасности.

[33] Помимо КВЭИ инсайдерские угрозы вызывают озабоченность и в других секторах. Например, в секторе авиационной безопасности. *См. ICAO Insider Threat Toolkit*, доступ по ссылке https://www.icao.int/Security/Security-Culture/Pages/ICAO-Insider-Threat-Toolkit.aspx.

Исследования, в частности, показали, что признаки подозрительного поведения можно обнаружить еще до совершения террористического акта, но о таком поведении обычно не сообщается.[34] Соответствующие заинтересованные стороны могут устранить эту уязвимость, организовав специализированное обучение для выявления тревожного поведения, которое может указывать на риск планируемого или готовящегося террористического акта при его анализе наряду с другими факторами риска, а также путем создания четких и конфиденциальных каналов информирования. К подозрительным признакам поведения часто относятся прогулы, неоправданные опоздания, нечестность, конфликты с другими сотрудниками, неоднократные случаи прихода в офис в нерабочее время или быстрый рост благосостояния. [35]

3.2.2. Взаимозависимость различных секторов КВИ (транспорт, связь, финансы и общественная инфраструктура)

Межсекторальная КВИ представляет собой сложную, взаимосвязанную экосистему, и их взаимозависимость приводит к появлению дополнительных уязвимостей.

Многообразие возможных последствий террористических атак связано с тем, что все секторы экономики зависят от энергии. Таким образом, использование слабых мест в корпоративной инфраструктуре сети может привести к возникновению «каскадного эффекта», который может затруднить или остановить работу в других секторах, таких как транспорт, финансы и связь. Повреждение или разрушение этой инфраструктуры может привести к нарушению или прерыванию предоставления услуг в различных секторах, а иногда и за пределами национальных границ.

Таблица 2

Взаимозависимости КВИ с акцентом на энергетическую инфраструктуру

(Под)сектор, предоставляющий услугу	(Под)сектор, получающий услугу			
	Энергетика	Транспорт	Связь	Водоснабжение
Энергетика	-	Электроэнергия для воздушных линий электропередач и электромобилей, топливо для работы транспортных средств	Энергия для работы вышек сотовой связи и другого передающего оборудования, топливо для резервного питания	Топливо для работы насосов, управления водными ресурсами и очистки воды
Транспорт	Доставка материалов, топлива и сотрудников		Доставка материалов, топлива и сотрудников	

[34] Bell, Alison & Rogers, Brooke & Pearce, Julia. (2018). The *Insider Threat: Behavioral indicators and factors influencing likelihood of intervention*. International Journal of Critical Infrastructure Protection. 24. 10.1016/J.ijcip.2018.12.001. Доступ по ссылке: https://www.researchgate.net/publication/329419966.

[35] Там же.

(Под)сектор, предоставляющий услугу	(Под)сектор, получающий услугу				
	Энергетика		Транспорт	Связь	Водоснабжение
Связь	Обнаружение и обеспечение операций и передачи электроэнергии	Обнаружение поломок и утечек, а также удаленный контроль операций	Выявление и определение местонахождения неисправных транспортных средств, рельсов и дорог		Обнаружение и контроль водоснабжения и качества
Водоснабжение	Охлаждающая и техническая вода	Техническая вода	Вода для эксплуатации транспортных средств; очистка	Вода для оборудования и очистки	

Источник: DEFENDER D6.2: CEI Security Stakeholder Group Manifest, доступ по ссылке: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b7096f83&appId=PPGMS

3.2.3. Трансграничные взаимозависимости

Постоянно растущая сложность и взаимозависимость энергетической инфраструктуры не только привели к появлению новых рисков и уязвимостей, но и могут усугубить серьезность и масштаб потенциальных последствий, которые не ограничиваются территориями отдельных объектов энергетики.

Например, Европейский союз принял политику Трансъевропейских энергетических сетей (TEN-E), направленную на объединение энергетической инфраструктуры стран ЕС для обеспечения безопасности поставок.[36] Такая интегрированная энергетическая сеть могла бы помочь избежать или минимизировать перебои в подаче электроэнергии в силу различных обстоятельств, включая террористические атаки.

Еще одним ярким примером трансграничного КВЭИ является нефтепровод Keystone, проходящих из США в Канаду. Он проходит от Западно-Канадского осадочного бассейна в Альберте до нефтеперерабатывающих заводов в Иллинойсе и Техасе (США), а также до нефтебаз и распределительного центра нефтепровода в Оклахоме (США).[37]

Современная энергетическая инфраструктура включает трубопроводы протяженностью в тысячи километров, соединяющие нефтяные и газовые заводы с потребителями. Трансграничная энергетическая инфраструктура, вероятно, будет расширяться, поскольку месторождения энергии вблизи традиционных рынков истощаются из-за растущего спроса. Хорошим примером этого являются строящиеся в настоящее время африканские трансграничные газопроводы (среди прочих — Транссахарский газопровод и газопровод Нигерия-Марокко).[38]

[36] Trans-European Networks for Energy, 2020, доступ по ссылке: https://energy.ec.europa.eu/topics/infrastructure/trans-european-networks-energy_en.
[37] Keystone Pipeline System, доступ по ссылке: https://www.tcenergy.com/operations/oil-and-liquids/keystone-pipeline-system/.
[38] *Multi-Billion Dollar Opportunities in Cross-Border Cooperation for Oil and Natural Gas Projects in Southern Africa*, доступ по ссылке: https://energychamber.org/multi-billion-dollar-opportunities-in-cross-border-cooperation-for-oil-and-natural-gas-projects-in-southern-africa/.

В ближайшие десятилетия цифровая трансформация будет направлена на то, чтобы сделать энергетические системы более взаимосвязанными, эффективными, надежными и устойчивыми, в том числе с использованием искусственного интеллекта (ИИ).[39] Достижения в области цифровых технологий и услуг в последние годы ускорили цифровую трансформацию энергетики, особенно в электрических сетях.[40]

В то же время цифровизация несет с собой существенные дополнительные риски, такие как рост зависимости от поставок электроэнергии. Сегодня все секторы КВИ зависят от стабильного снабжения электроэнергией. Например, глубокая взаимозависимость систем электроснабжения и связи подчеркивает необходимость повышения их устойчивости.[41]

Более того, защита критической электроэнергетической инфраструктуры имеет важное значение для информационной безопасности. Хотя атаки с использованием ИКТ на энергетическую инфраструктуру могут нанести физический ущерб, обратное также верно: физическое повреждение электрической инфраструктуры может нарушить работу связанных с ИКТ систем.

3.3 Изменения в ландшафте безопасности

3.3.1. Использование новых и перспективных технологий в террористических целях

Отмечается тенденция использования террористами новых и перспективных технологий как для осуществления атак, так и для обеспечения террористической деятельности (финансирования, пропаганды и т.д.). Технологический ландшафт стремительно меняется, в связи с чем возникает проблема своевременности применения технологических достижений со стороны субъектов энергетической инфраструктуры, а также и их возможного использования в террористических целях. Это включает в себя выбор в качестве цели объектов, сетей, процессов и других критически важных объектов энергетического сектора.

Эксперты определили следующие новые технологии как потенциальные средства, которые террористы могут использовать для осуществления нападений на энергетическую инфраструктуру:

- Искусственный интеллект и машинное обучение (в частности, нейронные сети) могут использоваться террористами для различных целей: от распознавания объектов и людей на камерах видеонаблюдения на этапах планирования атаки до выбора инструментов для взлома информации и управления системами КВЭИ. Дополнительную информацию можно найти в отчете «Алгоритмы и терроризм»: Злоумышленное использование искусственного интеллекта в террористических целях, опубликованное ЮНИКРИ и Контртеррористическим центром ООН (КТЦ

[39] *Digitalization of the energy system,* доступ по ссылке: https://energy.ec.europa.eu/topics/energy-systems-integration/digitalisation-energy-system_en.

[40] *Digitalisation*, International Energy Agency, доступ по ссылке: https://www.iea.org/energy-system/decarbonisation-enablers/digitalisation.

[41] *Digitalisation – Essential for Energy System Transformation. But What About Communications?*, 12 June 2023, доступ по ссылке: https://www.techuk.org/resource/digitalisation-essential-for-energy-system-transformation-but-what-about-communications-guest-blog-by-grid-scientific-limited.html.

ООН) (Глобальная программа по борьбе с терроризмом в области кибербезопасности и новых технологий).[42]

- Дистанционно управляемые системы, такие как беспилотные авиационные системы (БАС), беспилотные наземные аппараты (БНА) или дистанционно управляемые подземные аппараты (ДУПА), все чаще используются против объектов энергетической инфраструктуры, включая подземные и подводные нефте- и газопроводы.
- Технология 3D-печати, которая, например, используется для производства компонентов самодельных взрывных устройств (СВУ) или для сборки БАС или ДУПА.
- ИКТ, такие как:
    - Виртуальные частные сети (VPN) и прокси-сервисы, которые могут скрывать местоположение пользователей и маскировать информацию об IP-адресе.
    - Так называемый «Dark Web», который предлагает скрытую и в значительной степени необнаружимую сеть для террористических группировок, таких как ИГИЛ (ДАИШ) и их филиалов. Эта платформа позволяет им обмениваться конфиденциальной информацией, планировать атаки на КВЭИ и хранить учебные материалы.[43]. Дополнительную информацию можно найти в отчете «Взгляд в глубину: использование террористами и насильственными экстремистами Dark Web и Cybercrime-as-a-Service (киберпреступности как услуги) в целях осуществления кибератак», опубликованном ЮНИКРИ и КТЦ/КТУ ООН (в рамках Глобальной программы по борьбе с терроризмом в области кибербезопасности и новых технологий).[44]

Что еще более важно, в последние годы террористические атаки на энергетическую инфраструктуру стали более изощренными, часто сочетая физические нападения с атаками с использованием ИКТ в отношении систем управления и других технологий на базе ИКТ. Возможный сценарий включает в себя обычное нападение на физический объект КВИ с использованием бомб в сочетании с атакой типа «распределенный отказ в обслуживании» (DDoS), которая временно нарушает сетевой трафик объекта. Подобные комбинированные атаки могут подорвать усилия по реагированию на чрезвычайные ситуации, потенциально увеличить число жертв и вызвать массовую панику среди населения.

3.3.2. Террористические атаки с использованием БАС

За последнее десятилетие быстрое развитие БАС и их использование в террористических целях существенно изменили обстановку в сфере безопасности. Возможности дистанционного управления БАС в сочетании с их доступностью на коммерческих рынках и простотой сборки сделали их существенной угрозой. Успешные масштабные нападения с использованием БАС на нефтяные

42 UNOCT/UNCCT – UNICRI report *Algorithms and Terrorism: The Malicious use of artificial intelligence for terrorist purposes*, доступ по ссылке: malicious-use-of-ai-uncct-unicri-report-hd.pdf.

43 *Law enforcement capabilities framework for new technologies in countering terrorism*, UNOCT, UNCCT, INTERPOL, доступ по ссылке: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_law_enforecement_capabilities_web2.pdf.

44 UNOCT/UNCCT – UNICRI доклад *Beneath the Surface: Terrorist and Violent Extremist use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attack*, dw_beneath_the_surface_update.pdf (un.org).

объекты в Саудовской Аравии, например, в Абкайк-Хураисе в 2019 году и Джидде в 2022 году, подчеркнули уязвимость подобных объектов к подобным атакам в любой точке света.[45.]

В Делийской декларации Контртеррористического комитета Совета Безопасности ООН[46] о противодействии использованию новых и перспективных технологий в террористических целях с обеспокоенностью отмечается «растущее во всем мире злоупотребление террористами беспилотными летательными системами в целях совершения нападений на критически важную инфраструктуру и налета на них» (стр. 7). Кроме того, в декабре 2023 года были приняты необязательные руководящие принципы в отношении угроз, создаваемых использованием БАС в террористических целях, известные как «Руководящие принципы Абу-Даби», подготовленные в соответствии с Делийской декларацией, в которой Комитет постановил разработать набор необязательных руководящих принципов для оказания помощи государствам-членам в противодействии угрозе, создаваемой использованием новых и перспективных технологий в террористических целях.

Аналогичным образом Совет Безопасности ООН путем принятия резолюции 2370 (2017)[47] «решительно осуждает непрекращающийся поток оружия, включая стрелковое оружие и легкие вооружения (СОЛВ), военной техники, БАС и их компонентов и компонентов СВУ, которые попадают к ИГИЛ (известному также как ДАИШ), «Аль-Каиде», их подразделениям и связанным с ними группам, незаконным вооруженным группам и преступным элементам и циркулируют между ними, и рекомендует государствам-членам предотвращать и пресекать деятельность сетей по закупке такого оружия, систем и компонентов, циркулирующих между ИГИЛ (известным также как ДАИШ), «Аль-Каидой» и связанными с ними лицами, группами, предприятиями и организациями». Глобальная программа по противодействию использованию оружия террористами КТУ ООН совместно с ИДКТК и Институтом ООН по исследованию проблем разоружения (ЮНИДИР) разработала Технические руководящие принципы для содействия выполнению этой резолюции, всесторонне охватывающие превентивные и ответные меры по противодействию использованию террористами СОЛВ, СВУ и БАС[48], и содействовала их применению в 43 странах.

Организация Объединенных Наций активно разрабатывает инструменты для оказания помощи государствам-членам в борьбе с этой угрозой. Ярким примером таких усилий является Глобальная программа по борьбе с терроризмом с использованием автономных и дистанционно управляемых систем (Программа AROS),[49] созданная в 2021 году.[50] В рамках программы AROS КТУ ООН и ее партнеры по реализации оказывают поддержку государствам-членам в разработке правовой базы, в которой приоритет отдается защите прав человека, международному гуманитарному праву и

45 Доступ по ссылке: https://apnews.com/article/d20f80188e3543bfb36d512df7777cd4.

46 Делийская декларация Контртеррористического комитета Совета Безопасности ООН. Доступ по ссылке: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Dec/english_pocket_sized_delhi_declaration.final_.pdf.

47 S/RES/2370 (2017). Доступ по ссылке: S/RES/2370(2017).

48 *Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons, 2022*, доступ по ссылке: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/cted_guidelines_2370.pdf.

49 https://www.un.org/counterterrorism/autonomous-and-remotely-operated-systems.

50 Доступ по ссылке: https://www.un.org/counterterrorism/autonomous-and-remotely-operated-systems.

гендерному равенству, обеспечивая при этом, чтобы меры по борьбе с терроризмом не препятствовали законному использованию БАС и не тормозили технический прогресс.

Кроме того, Глобальная программа ООН по защите уязвимых целей от террористических угроз опубликовала техническое руководство под названием «Защита уязвимых целей от террористических атак с использованием беспилотных летательных систем». В этом руководстве изложены лучшие практики защиты от террористических атак с использованием БАС. В нем подчеркивается, что «БАС предоставляют террористическим группам ряд явных преимуществ в рамках их стратегий атак, и самое главное — большую возможность обойти традиционные меры физической защиты, основанные на нескольких уровнях безопасности (например, в виде укрепленных периметров мест проведения мероприятий, предназначенных для предотвращения атак с использованием транспортных средств, вооруженной охраны или барьеров для досмотра посетителей)».[51]

Кроме того, в 2022 году Рабочая группа по пограничному контролю и правоприменению в целях противодействия терроризму Глобального договора ООН по координации контртеррористической деятельности опубликовала Технические руководящие принципы для содействия осуществлению резолюции 2370 (2017) Совета Безопасности и связанных с ней международных стандартов и передовой практики по предотвращению приобретения оружия террористами, которые были реализованы ИДКТК в качестве Председателя Рабочей группы совместно с ЮНИДИР и КТЦ/КТУ ООН в тесном сотрудничестве и взаимодействии с членами Рабочей группы. Технические руководящие принципы предлагают подход, который может помочь государствам-членам прекратить поставки СОЛВ и связанных с ними боеприпасов, СВУ и их компонентов, а также БАС и их компонентов террористам.

Значительное увеличение количества форм-факторов, возможностей, простоты доступа и простоты эксплуатации БАС при низкой стоимости делает их предпочтительным оружием для будущих террористов.[52] Дальность и возможности применения БАС влияют на то, как они могут быть использованы в террористических атаках на объекты энергетики-[53]. Микро-БПЛА (беспилотные летательные аппараты) используются для нападения на КВЭИ с близкого расстояния. Напротив, средние БПЛА с большой дальностью полета могут преодолеть десятки километров, прежде чем нанести удар по объекту.

Таким образом, БАС могут быть использованы террористами для атаки на КВЭИ следующими способами:

---

[51] *Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS),* 2022, доступ по ссылке: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf

[52] Thomas G. Pledger, *The Role of Drones in Future Terrorist Attacks*, доступ по ссылке: https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf.

[53] В зависимости от массы БПЛА и, соответственно, заряда аккумуляторной батареи и транспортных возможностей БАС можно разделить на четыре группы:

- Микро – вес не превышает 10 кг, могут находиться в воздухе не более часа.
- Малые – весят до 50 кг и способны выполнять работу до 5 часов без перерыва.
- Средние – вес достигает одной тонны, время непрерывной работы до 15 часов.
- Тяжелые — весят более тонны, могут работать более 24 часов, а некоторые способны совершать межконтинентальные перелеты.

- Бомбардировка объектов энергетики: подобные атаки могут осуществляться путем подрыва террористами небольших БПЛА (например, FPV-дронов) или сброса взрывных устройств с БПЛА.
- разведка объектов с использованием фото- и видеотехники, других технических средств наблюдения и сбора информации (местонахождение его критически важных элементов и уязвимых мест, элементов физической защиты и сил безопасности и т.п.).

Более того, террористы могут использовать БАС для совершения атак с применением ИКТ на цели, не являющиеся БАС. При таком сценарии БПЛА может использоваться как «информационное оружие» для доставки вредоносного ПО против других систем, таких как критически важная информационная инфраструктура. С развитием технологии 5G как нового стандарта широкополосных сотовых сетей «коммуникационная полезная нагрузка» БАС может потенциально стать более простым в использовании инструментом для нарушения частной беспроводной связи.[54] Атаки с использованием БАС также могут быть частью скоординированной атаки и сочетаться с атаками, использующими ИКТ, системы обнаружения целей в воздухе или системы наблюдения за КВЭИ.

Вставка 3
«Роевые атаки» БАС на КВЭИ

«Роевые атаки» представляют собой применение нескольких летающих платформ БАС, объединенных в единую сетевую систему, обладающую автономностью по связи, ведению разведки и нанесения ударов по вражеским целям. Так называемые «роевые атаки» позволяют террористам проводить несколько атак с использованием БАС практически одновременно, мгновенно усиливая эффект их применения.

Эти «рои» могут состоять из низкотехнологичных дронов, но их цель — подавить оборонительные возможности КВЭИ. В качестве технологий обеспечения эффективности роя дронов могут использоваться беспроводные сети Bluetooth. Эти сети Bluetooth представляют собой маломощные локальные сети, которые самоорганизуются и обеспечивают обмен информацией в режиме реального времени. Способность «роев» к самоорганизации и самокоординации будет продолжать совершенствоваться с ростом вычислительной мощности, что одновременно будет способствовать повышению способности дронов к наведению на цель.[55]

3.3.3. Быстро меняющаяся среда угроз, характеризующаяся ростом угроз использования ИКТ против КВЭИ в противоправных целях

Повышение роли ИКТ в автоматизации производства энергии и энергетического перехода приводит к тому, что КВЭИ становится все более уязвимой для террористических атак, использующих эти технологии. В отличие от физических атак, при таком виде атак террористам не нужен физический доступ или близость к объекту инфраструктуры. Интернет и ИКТ в целом предоставили террористам новые инструменты и возможности, позволяющие им не только вербовать, финансировать и

[54] *Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS),* 2022, доступ по ссылке: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf

[55] Thomas G. Pledger, *The Role of Drones in Future Terrorist Attacks*, доступ по ссылке: https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf.

планировать террористическую деятельность, но и совершать атаки на КВИ, включая объекты энергетики. Если сравнивать с другими секторами КВИ, то на энергетическую инфраструктуру приходится более трети всех компьютерных атак.[56]

В мае 2023 года датская КВЭИ подверглась самой масштабной атаке с использованием ИКТ за всю свою историю. В результате скоординированной атаки были скомпрометированы более 20 компаний, эксплуатирующих объекты датской энергетической инфраструктуры. В результате злоумышленники получили доступ к некоторым системам управления производством компаний, и нескольким компаниям пришлось перейти на изолированный режим работы.[57]

Установление авторства остается серьезной проблемой в случае атак с использованием ИКТ. Определение источника и лиц, ответственных за эти атаки, является исключительно сложной задачей из-за легкости анонимизации в сети Интернет. Примечательно, что потенциальные последствия атак с использованием ИКТ могут быть столь же серьезными, как и последствия физических атак, или даже более серьезными, независимо от мотива. Хотя террористические группы, возможно, и не берут на себя ответственность за атаки на КВЭИ с использованием ИКТ, растущая доступность ИКТ-технологий способствовала росту и эскалации угроз в этой области.

Атаки на КВЭИ, связанные с ИКТ, могут включать:

- Распределенные атаки типа «отказ в обслуживании» (DDoS): они могут нарушить сетевые соединения и основные ресурсы, вызывая сбои в работе систем и нарушая работу информационных и коммуникационных систем.
- Атаки с использованием программ-вымогателей: могут быть реализованы посредством фишинга. Программы-вымогатели, воздействующие на сеть, могут блокировать системы и нарушать повседневную деятельность операторов КВИ, что может повлиять на их работу. Например, в 2019 году масштабная атака с использованием вирусов-вымогателей была направлена на системы информационных технологий Национального топливного общества Анголы (Sonangol).[58] Злоумышленники получили доступ к данным более чем семи тысяч компьютеров, включая конфиденциальную и инсайдерскую информацию о компании и ее клиентах.
- Несанкционированное использование точек доступа для удаленного обслуживания: эти точки доступа, намеренно созданные как внешние входы в информационные и коммуникационные сети, часто оказываются недостаточно защищенными.

Более того, энергетическая инфраструктура требует отраслевого подхода, выходящего за рамки стандартных мер информационной безопасности, применяемых к системам информационных технологий. Это связано с уникальными особенностями и дополнительными уязвимостями информационных систем в энергетическом секторе.

---

56 *Energy sector faces 39% of critical infrastructure attacks*, Security, доступ по ссылке: https://www.securitymagazine.com/articles/99915-energy-sector-faces-39-of-critical-infrastructure-attacks.

57 *The attack against Danish, critical infrastructure,* 2023, доступ по ссылке: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf.

58 Доступ по ссылке: https://businesselitesafrica.com/2019/06/07/sonangol-suffers-attempted-cyber-attack/?v=f9308c5d0596#:~:text=The%20National%20Fuel%20Society%20of,company%20explained%20in%20a%20statement.

Таблица 3

Таблица ОБСЕ в отношении уязвимостей энергетической инфраструктуры к атакам с использованием ИКТ

Объект	Описание возможных уязвимостей и направлений атак
Программное обеспечение	Приложения или системное программное обеспечение могут иметь случайно или преднамеренно внесенные уязвимости, которые можно использовать для подмены цели, для которой было разработано программное обеспечение.
Аппаратное обеспечение	Уязвимости могут быть обнаружены в аппаратном обеспечении, включая микропроцессоры, микроконтроллеры, печатные платы, блоки питания, периферийные устройства, такие как принтеры или сканеры, устройства хранения данных и коммуникационное оборудование, такое как сетевые карты. Вмешательство в работу таких компонентов может изменить предполагаемую функциональность компонента или создать возможности для внедрения вредоносного ПО.
Стыки между оборудованием и программным обеспечением	Примером такого стыка может служить перепрограммируемая постоянная память компьютера (прошивка), которую можно несанкционированно и тайно перепрограммировать.
Каналы связи	Злоумышленники могут по-разному использовать каналы связи между системой или сетью и внешним миром. Они могут выдавать себя за авторизованных пользователей, глушить каналы, чтобы лишить доступа законных пользователей, или прослушивать, чтобы собирать секретную или конфиденциальную информацию.
Конфигурация	Большинство систем предоставляют множество вариантов конфигурации, которые пользователи могут устанавливать в зависимости от собственных предпочтений в вопросах безопасности и удобства. Поскольку удобство часто ценится больше, чем безопасность, многие системы на практике настроены небезопасно.
Пользователи и операторы	Авторизованные пользователи и операторы системы или сети могут быть обмануты или подвергнуты шантажу в целях выполнения требований злоумышленника, или они могут продать свои услуги.
Провайдеры услуг	Зачастую при использовании компьютерных установок задействуются третьи лица, которые предоставляют компьютерные услуги, такие как техническое обслуживание или подключение к Интернету. Злоумышленник может убедить провайдера услуг предпринять какие-то особые действия от его имени, например, установить атакующее программное обеспечение на целевой компьютер.

Источник: ОБСЕ Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства, доступ по ссылке: https://www.osce.org/files/f/documents/4/b/103500.pdf.

Энергетический сектор, особенно электроэнергетический и газовый подсекторы, демонстрирует уникальную взаимозависимость между физической инфраструктурой и системами информационных технологий (ИТ). Такая конвергенция создает уязвимости, которыми могут воспользоваться злоумышленники. Эти уязвимости охватывают различные риски, включая манипулирование системами операционных технологий (ОТ) с целью нарушения работы критически важного оборудования. Учитывая, что операторы КВЭИ могут полагаться на данные систем безопасности и мониторинга транспорта, используемых для регулирования потоков электроэнергии или газа, без дополнительной ручной проверки, манипуляции с системами ОТ могут привести к опасным перерасходам, потенциально повреждающим оборудование.

Уязвимость энергетического сектора еще больше усугубляется из угрозы инсайдерских атак с использованием ИКТ. Уполномоченный персонал, включая сотрудников и подрядчиков, представляет значительную угрозу из-за имеющихся привилегий доступа к критически важным информационным системам. Этот доступ может быть использован не по назначению, как непреднамеренно, так и преднамеренно (например, в случае радикализованных лиц).[59]

Вставка 4

Уязвимости, связанные с использованием интеллектуальных устройств в эксплуатации КВЭИ и автоматизированных систем управления технологическим процессом (SCADA)

SCADA — это компьютерная система, используемая в промышленности и КВИ для мониторинга и управления чувствительными процессами и физическими функциями. Системы управления могут использоваться для мониторинга простых процессов или для управления более сложными процессами в интеллектуальной электрической сети или на атомной электростанции. В процессе своего развития SCADA претерпела значительную эволюцию от обычной изолированной среды до тесно взаимосвязанной сети.

Исходя из статистики атак с использованием ИКТ, в более чем 50 процентах случаев объектом атак становятся системы SCADA[60]. Известно, что интеллектуальные устройства и SCADA позволят получить доступ к КВЭИ, что позволяет практически любому человеку получить доступ и взаимодействовать с инфраструктурой.

Согласно проведенному тщательному анализу уязвимостей SCADA, наиболее распространенными атаками на систему безопасности SCADA являются:

- Атака типа «отказ в обслуживании» (DoS) перегружает целевой объект большим объемом трафика. Напротив, распределенный отказ в обслуживании (DDoS) — это тип DoS, при котором несколько взломанных компьютеров одновременно атакуют целевой объект.
- Атаки с целью повреждения памяти происходят, когда ячейка памяти изменяется из-за ошибок программирования.
- Атаки с целью повышения привилегий происходят, когда злоумышленник получает несанкционированный доступ к учетной записи пользователя с административными привилегиями для повышения уровня доступа.
- Атаки с целью повышения уровня доступа происходят, когда злоумышленник получает прямой несанкционированный доступ к системе SCADA с привилегиями.
- Произвольное и удаленное выполнение кода — это атака, являющаяся результатом связанных атак и уязвимостей SCADA, таких как переполнение буфера.
- Проведение разведки позволяет злоумышленнику собирать информацию о топологии сети SCADA и значениях данных, функциях устройств или конфиденциальной информации, хранящейся на контроллерах автоматизации.
- Атаки с использованием кода функции сброса происходят, когда незащищенные протоколы связи SCADA не имеют надлежащей аутентификации и авторизации. Злоумышленник может изменить исходное состояние устройства SCADA, сбросив код функции этого устройства в несогласованное состояние, что приведет к сбою в работе.
- Атака путем внедрения SQL-кода представляет собой атаку путем внедрения кода, которая раскрывает приложения, работающие с данными.

Источник: Manar Alanazi, Abdun Mahmood, Mohammad Jabed Morshed Chowdhury, SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues, Computers & Security, Volume 125, 2023, 103028, ISSN 0167-4048, DOI: https://doi.org/10.1016/j.cose.2022.103028 https://www.sciencedirect.com/science/article/pii/S0167404822004205.

[59] Более подробная информация доступна по ссылке: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

[60] *Energy sector faces 39% of critical infrastructure attacks*, Security, доступ по ссылке: https://www.securitymagazine.com/articles/99915-energy-sector-faces-39-of-critical-infrastructure-attacks.

4. Национальные подходы к снижению связанных с терроризмом рисков для КВЭИ: роль участников и передовой опыт

Большинство стран предусмотрели меры защиты своих энергетических объектов, постепенно принимая национальные стратегии, правила и инструкции, охватывающие как национальный энергетический сектор, так и определенные подсекторы.

4.1. Нормативно-правовая база: национальная структура безопасности, национальное законодательство/регулирование, требования и стандарты в области защиты КВЭИ

4.1.1. Защита КВЭИ в рамках национальной безопасности

За последнее десятилетие многие государства-члены переключили свое внимание с непосредственно защиты критически важных объектов, отдав приоритет их устойчивости. Такой подход направлен на повышение способности минимизировать последствия и продолжительность разрушительных событий как в физической, так и в ИКТ-среде. Акцент сместился с исключительно предотвращения атак на быстрое восстановление работоспособности, при этом признается, что достижение 100-процентной безопасности не может быть гарантировано.

Согласно Руководству по внедрению принципов устойчивой инфраструктуры, опубликованному Управлением ООН по снижению риска бедствий (UNDRR), «устойчивость инфраструктуры — это своевременное и эффективное предотвращение, поглощение, восстановление, адаптация и трансформация основных структур и функций национальной инфраструктуры, которые подверглись воздействию текущих и потенциальных будущих опасностей».[61] Обеспечение устойчивости на всех этапах сбоев должно осуществляться посредством совместного управления рисками и неопределенностью, оценки множественных опасностей и методов, учитывающих системный характер национальной инфраструктуры.

[61] *Handbook for Implementing the Principles for Resilient Infrastructure*, UNDRR, 2023, доступ по ссылке: https://www.undrr.org/media/87213.

На практике это означает, что защита КВЭИ должна включать в себя предкризисные меры, направленные на устойчивость и способность выдерживать или противостоять стрессу. В нем также признается, что сбои в работе КВИ иногда неизбежны и их невозможно полностью избежать. Поэтому крайне важно повышать поглощающие и адаптивные возможности, например, внедрять избыточность и разрабатывать эффективные стратегии восстановления.[62]

4.1.2. Защита КВЭИ как часть политики национальной безопасности

Определение комплекса мер, направленных на защиту КВЭИ от террористических актов, является приоритетной задачей для большинства органов государственной власти, особенно спецслужб и правоохранительных органов, а также частных заинтересованных сторон. Связь между национальной безопасностью и защитой критически важной инфраструктуры имеет жизненно важное значение для прогресса любого общества, защиты права на жизнь и его надлежащего социального и экономического функционирования.

При этом национальные подходы к определению приоритетов и координации мер защиты могут существенно различаться. Органы власти могут принять решение, следует ли включить защиту энергетического сектора в свою национальную стратегию, подчеркнув его важную роль в обеспечении национальной безопасности, или разработать специальную стратегию борьбы с терроризмом, которая помимо других секторов будет включать защиту энергетического сектора. В качестве альтернативы защита КВЭИ может быть рассмотрена в рамках более широкой политики защиты КВИ.

В некоторых странах защита энергетического сектора может быть обеспечена несколькими документами в зависимости от роли и значимости энергетического сектора в социальной и экономической жизни страны. Например, в:

- Стратегии национальной безопасности и ее приоритетах (см. 4.1.3)
- Контртеррористической стратегии (см. 4.1.4)
- Стратегии защиты КВИ (см. 4.1.5)

4.1.3. Защита КВЭИ как один из приоритетов национальной безопасности

Совет Безопасности ООН и Генеральная Ассамблея заявили, что любые меры, принимаемые для предотвращения и борьбы с терроризмом, должны соответствовать обязательствам государств-членов по международному праву, в частности международному праву в области прав человека, международному беженскому праву и международному гуманитарному праву, и подчеркнули, что уважение прав человека, основных свобод и верховенства права являются взаимодополняющими и

[62] Christer Pursiainena, Eero Kytömaa, *From European critical infrastructure protection to the resilience of European critical entities: what does it mean?* Sustainable and Resilient Infrastructure, 2023, VOL. 8, Pages 85–101, https://doi.org/10.1080/23789689.2022.2128562 at: https://www.tandfonline.com/doi/epdf/10.1080/23789689.2022.2128562?needAccess=true.

взаимоукрепляющими с эффективными мерами по борьбе с терроризмом.[63] Следовательно, любые меры, направленные на защиту КВИ от террористических актов, должны разрабатываться и осуществляться в соответствии с международным правом в области прав человека, международным правом беженцев и международным гуманитарным правом.

Как отмечалось ранее, некоторые государства-члены включают защиту КВЭИ в число своих приоритетов национальной безопасности для содействия согласованным и скоординированным усилиям. Хотя в настоящее время это не основной метод организации защиты КВЭИ, он по-прежнему применяется в ряде стран, например, в Азербайджане[64], Бразилии[65], Чешской Республике[66], России[67] и других странах.

- Растущая взаимозависимость между секторами КВИ в сочетании с возможностью каскадных эффектов в случае аварий или атак требуют широкого подхода для эффективной координации совместной деятельности субъектов различных секторов по предотвращению, реагированию и восстановлению. Такой подход позволяет систематизировать и координировать межведомственную деятельность, а также избежать дублирования функций. Надежная структура национальной безопасности для защиты КВЭИ должна:
    - Определить государственные органы, ответственные за регулирование деятельности по защите КВЭИ, включая координацию партнерства с частным сектором.
    - Установить измеримые стратегические цели, национальные программы и сроки достижения этих целей.
    - Обеспечить основу для эффективного предотвращения и управления инцидентами посредством гармонизации задач в различных областях политики безопасности.

В то же время разработка надежной структуры национальной безопасности не обязательно снижает необходимость принятия мер защиты, специфичных для энергетического сектора, особенно если эти меры доказали свою эффективность или соответствуют обязательным международным нормативным актам. Учитывая сохраняющиеся террористические угрозы для КВЭИ, крайне важно принять стратегический подход, который предполагает наращивание потенциала и предвидит значительное увеличение как объема, так и разнообразия угроз.

63 Глобальная контртеррористическая стратегия (A/RES/77/298).
64 Национальная стратегия Азербайджана, доступ по ссылке: https://www.migration.gov.az/content/pdf/b5f3b29fd98276567dd7f0fd0ff2a58b.pdf.
65 Política Nacional de Defesa, доступ по ссылке: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf.
66 Стратегия безопасности Чешской Республики, 2023, доступ по ссылке: https://mzv.gov.cz/file/5119429/MZV_BS_A4_brochure_WEB_ENG.pdf.
67 Стратегия национальной безопасности Российской Федерации, 2024, доступ оп ссылке: http://www.kremlin.ru/acts/bank/47046.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 1

Законодательство Бразилии в области национальной обороны в части защиты КВЭИ

Обновленная политика в области национальной обороны и стратегия национальной обороны Бразилии включают в качестве национальной цели защиту стратегической инфраструктуры, включая объекты энергетики.[68]

Согласно этим документам, первоочередной целью национальной обороны является «гарантия суверенитета, национального наследия и территориальной целостности», что включает в себя необходимость обеспечения безопасности, среди прочего, следующих секторов экономики Бразилии:

- Производство и распределение электроэнергии.
- Производство и распределение топлива.

Более того, восьмая цель национальной обороны — «усиление влияния Бразилии в странах-участницах и интеграция в международные процессы принятия решений» — также включает в себя в качестве дополнительной цели защиту вышеупомянутых секторов в рамках усилий по наращиванию национального потенциала.

Источник: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf.

4.1.4. Защита КВЭИ в рамках политики борьбы с терроризмом

Защита КВЭИ чаще предусматривается в рамках политики по борьбе с терроризмом, нежели чем в рамках национальной безопасности. Национальные стратегии борьбы с терроризмом, включающие защиту от террористических актов в качестве одного из приоритетов, часто предусматривают широкую базу для предотвращения совершения террористических преступлений и обеспечивают синергию между разведывательными и правоохранительными органами, но редко определяют конкретные меры борьбы с терроризмом в энергетическом секторе, учитывающие особенности этого сектора.

[68] Política Nacional de Defesa, доступ по ссылке: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 2

Национальная система Ганы предупреждения и противодействия насильственному экстремизму и терроризму (NAFPCVET)

Документ основан на комплексном подходе и дает определения объектов инфраструктуры, включая объекты энергетики.

В Гане в рамках Национальной системы борьбы с терроризмом защита важнейших объектов энергетики требует четко определенного межведомственного подхода к предотвращению и борьбе с террористическими угрозами. В рамках программы особое внимание уделяется обеспечению систематической координации между министерствами, ведомствами и агентствами, а также организациями гражданского общества (ОГО).

Система NAFPCVET четко определяет государственные министерства и национальные агентства Ганы, которые должны участвовать в обеспечении защите КВЭИ, а также типы национальных документов, которые должны быть подготовлены.

Защита прибрежных нефтяных объектов от террористических атак является ярким примером межведомственного взаимодействия. В то время как Министерство энергетики Ганы отвечает за обеспечение безопасности добычи нефти, поставок нефтепродуктов и распределения нефтегазовых активов в стране, агентства по безопасности на море, такие как Управление морского судоходства Ганы (GMA), Военно-морские силы Ганы и другие ведомства, отвечающие за безопасность на море, также должны принимать активное участие в ситуациях, когда критически важная инфраструктура нефтегазовой отрасли попадает в сферу безопасности на море. Более того, в документе упоминается важность «внедрения стратегии морской безопасности для обеспечения надлежащей защиты этих (энергетических) национальных активов».[69]

Источник: Национальная система Ганы предупреждения и противодействия насильственному экстремизму и терроризму, 29 января 2020, доступ по ссылке: https://www.peacecouncil.gov.gh/storage/2019/09/NAFPCVET-Document-29-Jan-2020.pdf.

4.1.5. Обеспечение защиты КВЭИ через реализацию специализированных политик защиты КВИ

Наиболее распространенным вариантом институционализации обеспечения защиты энергетической инфраструктуры является проведение специализированной политики защиты КВИ. Согласно последним исследованиям, энергетический сектор чаще всего упоминается странами мира в своих стратегиях защиты КВИ (96%).[70]

Защита КВЭИ может быть неотъемлемой частью стратегии или политики государства в области защиты КВИ. Такая стратегия или политика должна:

[69] Национальная система Ганы предупреждения и противодействия насильственному экстремизму и терроризму, 29 января 2020, доступ по ссылке: https://www.peacecouncil.gov.gh/storage/2019/09/NAFPCVET-Document-29-Jan-2020.pdf.

[70] Valentin Weber, Maria Pericàs Riera, Emma Laumann, *Mapping the World's Critical Infrastructure Sectors*, 2023, доступ по ссылке: https://dgap.org/en/research/publications/mapping-worlds-critical-infrastructure-sectors.

- Включать методологию определения конкретных объектов энергетического сектора в качестве критически важных.
- Описывать дополнительные правила, учитывающие уникальные особенности энергетического сектора, такие как специальные стандарты обмена информацией или требования по обеспечению безопасности.
- Обеспечивать высококачественные планы реагирования на чрезвычайные ситуации и восстановления как для действующих, так и для вновь возводимых объектов.

4.1.6. Определение участников обеспечения безопасности КВЭИ

Для обеспечения инклюзивного подхода и участия всех участников обеспечения безопасности КВЭИ государствам-членам необходимо принять четкие правила определения и классификации участников, которые будут разделять ответственность за обеспечение защиты КВЭИ от террористических атак.

Таблица 4

Роль различных участников в реализации политики защиты КВЭИ

Правительство	Под правительством понимаются должностные лица, которые разрабатывают и инициируют изменения в национальной стратегии/политике обеспечения защиты КВЭИ, разрабатывают правовые основы защиты КВЭИ на национальном уровне и выделяют необходимое финансирование на контртеррористическую деятельность.
Регулирующие органы энергетического сектора	Регулирующие органы энергетического сектора реализуют политику защиты КВЭИ, определенную правительством, разрабатывают требования к протоколам безопасности, управлению рисками, планированию действий в чрезвычайных ситуациях и непредвиденных обстоятельствах, а также инструкции по мерам противодействия терроризму, которые должны быть реализованы на объектах энергетики. Обычно критерии отнесения объектов энергетики к критически важным определяются регулирующими органами.
Владельцы КВЭИ	Владельцы энергетической инфраструктуры принимают и повышают стандарты защиты, разрабатывают планы по противодействию терроризму для конкретных объектов и требуют от операторов КВЭИ оценивать потенциальные террористические угрозы.
Подрядчики КВЭИ	Подрядчики обязаны выполнять свою работу в соответствии с национальными стандартами и правилами. Они разрабатывают и внедряют инструменты для соблюдения требований и стандартов безопасности регулирующих органов энергетического сектора.
Операторы КВЭИ	Операторы КВЭИ управляют, обслуживают и восстанавливают инфраструктуру в соответствии со стандартами, кодексами и правилами, согласованными правительством и регулирующими органами энергетического сектора, используя технологии и решения, предоставляемые подрядчиками. Операторы собирают данные об угрозах и уязвимостях для совершенствования управления рисками. В рамках ГЧП владельцы и операторы обмениваются знаниями и опытом по защите объектов энергетики.

Также важна роль гражданского общества, включая профсоюзы, местные сообщества, экспертные и научные организации, в решении вопросов безопасности в энергетическом секторе. Хотя организации гражданского общества могут не иметь такого же уровня ответственности, как другие участники, они могут вносить вклад в принятие решений как на государственном, так и на оперативном уровнях. Они представляют интересы и ценности своих членов по этическим, культурным и религиозным вопросам и могут разрабатывать ответственные практики, которые повышают защиту энергетической инфраструктуры.

4.1.7. Критерии отнесения отдельных объектов энергетики к критически важным

Еще один важный вопрос касается критериев отнесения отдельных объектов энергетики к критически важным, поскольку это влечет за собой принятие в отношении них дополнительных мер безопасности. Государства-члены используют разные критерии для отнесения объектов энергетики к критически важным. Во многих случаях национальные определения включают один или оба из следующих элементов: они подчеркивают цель энергетической инфраструктуры, связывая ее критичность с выполнением важнейших социальных и экономических функций, и определяют последствия нарушения или разрушения, описывая критичность с точки зрения предполагаемых последствий прерывания обслуживания.

Таблица 5

Национальные подходы к отнесению объектов к критически важной энергетической инфраструктуре

Аргентина[71]	К объектам КВЭИ относятся плотины, подстанции, линии электропередач, хранилища топлива, нефтепроводы, газопроводы.
Бельгия[72]	Сектор энергетики включает в себя следующие подсекторы КВИ: 1. Электроэнергетика, включающая инфраструктуру и установки, обеспечивающие производство и транспортировку электроэнергии с целью ее поставки. 2. Производство нефти, включая добычу, переработку, хранение и транспортировку нефти по трубопроводам. 3. Производство газа, включая добычу, переработку, хранение, транспортировку по газопроводам и терминалы сжиженного природного газа.
Бразилия[73]	К КВЭИ относятся объекты, которые обеспечивают: • Производство и распределение электроэнергии • Производство и распределение топлива • Производство ядерной энергии

71 Subsecretaría de protección civil y abordaje integral de emergencias y catástrofes (1/2015), доступ по ссылке: http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242082/norma.htm.

72 Act of 1 July 2011 on the security and protection of critical infrastructure, доступ по ссылке: https://crisiscentrum.be/sites/default/files/documents/files/2021-03/PDFsam_15_2.pdf.

73 Estratégia Nacional de Defesa, доступ по ссылке: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf.

Хорватия[74]	КВИ энергетического сектора включает в себя системы производства, в том числе водохранилища и плотины, передачи, хранения, транспортировки энергии и распределения энергии.

Чешская Республика[75]	К чешской КВЭИ относятся:
	• Объект производства электроэнергии
	• Система передачи электроэнергии
	• Система распределения электроэнергии
	  ○ Газотранспортная система (транзитный газопровод высокого давления с номинальным диаметром не менее 700 мм или национальный газопровод высокого давления с номинальным диаметром 700 мм и менее и компрессорная станция или перекачивающая станция)
	• Система газораспределения (газопровод высокого или среднего давления и передаточно-регулирующая станция)
	• Газохранилище (подземное хранилище газа объемом не менее 50 млн. м3)
	• Система перекачки нефти и нефтепродуктов
	  ○ Транзитный нефтепровод номинальным диаметром не менее 500 мм, включая входы
	  ○ Национальный нефтепровод номинальным диаметром не менее 500 мм, включая входы
	  ○ Насосная станция
	  ○ Терминальное оборудование для перекачки нефти
	  ○ Начало и конец удвоения и ответвления нефтепровода – устройство запуска очистных устройств
	• Система распределения нефти и нефтепродуктов (трубопровод номинальным диаметром не менее 200 мм и насосная станция).
	• Хранение и добыча нефти и топлива (хранилище или комплекс хранилищ объемом не менее 40000 м3 и нефтеперерабатывающий завод мощностью фракционной перегонки не менее 500000 тонн в год).
	• Центры технического управления в энергетическом секторе также относятся к КВИ.

Германия[76]	К критической энергетической инфраструктуре относятся: • Электроснабжение: генерация, передача, распределение и торговля • Поставка газа: добыча, транспортировка, распределение и торговля • Поставка топлива/печного топлива: добыча, производство, транспортировка, распределение • Централизованное теплоснабжение: генерация и распределение

[74] Zakon o kritičnim infrastrukturama NN 56/13, 114/22, 2022, доступ по ссылке: *https://www.zakon.hr/z/591/Zakon-o-kritičnim-infrastrukturama.*

[75] Czech Governmental Order No 432/20,10 Coll of 22 December 2010 on the Criteria for the Identification of a Critical Infrastructure Element, доступ по ссылке: https://www.govcert.cz/download/kii-vis/preklady/Order_432_2010_EN_v1.0_final.pdf.

[76] KRITIS-Sektor definition Energie, https://www.openkritis.de/it-sicherheitsgesetz/sektor_energie.html.

Гана[77]	К КВЭИ относятся причалы, резервуары для хранения, нефтеперерабатывающие заводы, завод СПГ, инфраструктуру узловой передачи, электростанции, нефтехимический завод, завод по смешиванию смазочных материалов, а также инфраструктура передачи и хранения для стран, не имеющих выхода к морю.
Казахстан[78]	К стратегически важным объектам отраслей экономики, уязвимым в террористическом отношении, относятся объекты энергетики, которые соответствуют следующим критериям: • Газораспределительные станции, обеспечивающие товарным газом организации, осуществляющие производство тепловой энергии и удовлетворяющие критериям настоящего подпункта. • Энергопроизводящие организации, вырабатывающие электрическую (более 50 МВт) и (или) тепловую энергию, котельные, вырабатывающие тепловую энергию в зоне централизованного теплоснабжения (более 100 Гкал) (ГРЭС, ГЭС, ГТЭС, ТЭЦ и котельные). • Объекты, на которых осуществляется переработка нефти и (или) газа, хранение нефти и (или) газа в резервуарах, добыча и переработка урана. • Предприятия химической промышленности.
Румыния[79]	Подсекторы КВИ энергетического сектора: • Электроэнергия, включая ядерно-электрические мощности и объекты по производству, хранению/складированию, распределению и транспортным сетям. • Нефть и нефтепродукты: мощности и сооружения для добычи/производства, переработки, обработки, хранения/складирования, распределения и транспортировки по трубопроводам, терминалы. • Природный газ и продукты его переработки: мощности и сооружения для добычи/производства, переработки, обработки, хранения/складирования, распределения и транспортировки по трубопроводам, терминалы. • Минеральные ресурсы
Россия[80]	К объектам энергетического комплекса относятся объекты энергетики, нарушение или прекращение функционирования которых приведет к утрате управляемости экономикой Российской Федерации, субъекта Российской Федерации, административно-территориальной единицы, необратимым негативным изменениям (разрушению) либо существенному снижению безопасности и жизнедеятельности населения.

77 *Strategic Environmental Assessment on the Development of a Petroleum Hub in Ghana*.

78 Постановление Правительства Республики Казахстан «Об утверждении Правил и критериев отнесения объектов к объектам, уязвимым в террористическом отношении».

79 Order of the Minister of Economy, Commerce and Business Environment no. 1.178 of 6 June 2011 https://cncpic.mai.gov.ro/en/sectoare/energetic.

80 Федеральный закон от 21 июля 2011 г. N 256-ФЗ "О безопасности объектов топливно-энергетического комплекса", доступ по ссылке: https://base.garant.ru/12188188/.

Словения[81]	Нарушение энергетической системы на территории Республики Словения: • Восстановление которой занимает более семи дней. • Нарушение электроснабжения на три дня для более чем 100 000 человек. • Перерыв в поставках нефтепродуктов и природного газа более чем на неделю затронул более 100 000 человек и нанес ущерб в размере 10 000 000 евро в день.
Словакия[82]	К критически важным объектам энергетики относятся производство атомной энергии, передача электроэнергии, транспортировка и распределение природного газа, транспортировка и переработка нефти, производство тепла и добыча важного сырья.
Турция[83]	Совокупность энергетической сети, активов, систем и сооружений, неспособность которых выполнять свои функции полностью или частично может отрицательно повлиять на устойчивость общественного порядка или предоставление общественных услуг.
Великобритания[84]	Национальные активы, имеющие важное значение для функционирования общества, например, связанные с энергоснабжением. Сектор энергоснабжения состоит из добычи нефти и газа, переработки нефти и газа и электроэнергии.
США[85]	Энергетическая инфраструктура включает в себя электроэнергетические системы, системы природного газа и жидкого топлива, связанные с генерацией, передачей и распределением электроэнергии, а также аварийные и резервные системы электроснабжения. Трубопроводы, транспортирующие природный газ и жидкое топливо рассматриваются как часть транспортной инфраструктуры, поскольку технические стандарты безопасности и проектирования трубопроводов регулируются Управлением по безопасности трубопроводов и опасных материалов. «Критическая» часть энергетической инфраструктуры означает систему или актив основной энергетической системы (физической или виртуальной), неработоспособность или разрушение которой негативно повлияет на: • Национальную безопасность • Экономическую безопасность • Общественное здравоохранение или безопасность или любое сочетание этих видов безопасности.
Япония[86]	Энергетический сектор КВИ включает: • Услуги по электроснабжению • Услуги по газоснабжению • Нефтяная промышленность

81 *Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastructure državnega pomena v Republiki Sloveniji*, 2012.
82 Slovak Act No. 45/2011 Coll. on critical infrastructure, available at: https://www.aspi.sk/products/lawText/1/73766/1/2.
83 Enerji sektöründe kullanilan endüstriyel kontrol sistemlerinde bilişim güvenliği yönetmeliği, 2017, доступ по ссылке: https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm.
84 UK's Sector Security and Resilience Plans.
85 *Community Resilience Planning Guide for Buildings and Infrastructure System*, доступ по ссылке: https://crsreports.congress.gov/product/pdf/R/R47666.
86 Доступ по ссылке: https://sg.nec.com/en_SG/pdf/brochures/PublicSafety/SocialValueCreationReport_en_Vol.1.pdf.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 3

Критерии отнесения к критически важным объектов топливно-энергетического комплекса в Российской Федерации

Для отнесения объектов энергетической инфраструктуры к критически важным Минэнерго России использует как качественные, так и количественные показатели. Кроме того, объекты энергетики могут быть отнесены к критически важным на федеральном (национальном), региональном и административном уровнях.

		Качественные показатели	Количественные показатели
1.	**Федеральный уровень**	Объекты, нарушение или прекращение функционирования которых приведет к потере управления экономикой на территории 2 и более субъектов Российской Федерации, ее необратимому негативному изменению (разрушению).	Объекты, на которых в результате чрезвычайной ситуации количество людей, погибших и (или) получивших ущерб здоровью, составляет свыше 500 человек.
		Объекты, нарушение или прекращение функционирования которых приведет к существенному снижению безопасности жизнедеятельности населения 2 и более субъектов Российской Федерации.	Объекты, на которых в результате чрезвычайной ситуации размер ущерба окружающей природной среде и материальных потерь (далее - размер материального ущерба) составляет свыше 1,2 миллиардов рублей.
2.	**Региональный уровень**	Объекты, нарушение или прекращение функционирования которых приведет к потере управления экономикой на территории одного субъекта Российской Федерации, ее необратимому негативному изменению (разрушению).	Объекты, на которых в результате чрезвычайной ситуации количество людей, погибших и (или) получивших ущерб здоровью, составляет свыше 50 человек, но не более 500 человек.
		Объекты, нарушение или прекращение функционирования которых приведет к существенному снижению безопасности жизнедеятельности населения одного субъекта Российской Федерации.	Объекты, на которых в результате чрезвычайной ситуации размер материального ущерба составляет свыше 12 миллионов рублей, но не более 1,2 миллиардов рублей.
3.	**Муниципальный уровень**	Объекты, нарушение или прекращение функционирования которых приведет к потере управления экономикой административно-территориальной единицы субъекта Российской Федерации, ее необратимому негативному изменению.	Объекты, на которых в результате чрезвычайной ситуации количество людей, погибших и (или) получивших ущерб здоровью, составляет не более 50 человек.
		Объекты, нарушение или прекращение функционирования которых приведет к существенному снижению безопасности жизнедеятельности населения административно-территориальной единицы субъекта Российской Федерации.	Объекты, на которых в результате чрезвычайной ситуации размер материального ущерба составляет не более 12 миллионов рублей, а также данная чрезвычайная ситуация не может быть отнесена к чрезвычайной ситуации локального характера.

Источник: Приказ Министерства энергетики РФ от 15 сентября 2022 г. № 957, доступ по ссылке: https://minjust.consultant.ru/files/33257.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 4

Субъекты обеспечения безопасности КВЭИ в Турции

Согласно Государственному закону Турции № 4628, регулирующими органами КВЭИ являются:

- Департамент рынка электроэнергии
- Департамент рынка природного газа
- Департамент рынка нефти
- Департамент рынка сжиженных углеводородных газов
- Департамент тарифов
- Департамент аудита
- Департамент экспроприации
- Правовой департамент
- Департамент информационных технологий
- Департамент стратегического планирования
- Департамент кадров и вспомогательных служб
- Советник офиса по связям с общественностью и прессой
- Специальное бюро при Комиссии
- Специальное бюро при Президенте

Следующие организации определяются как «ответственные компании» (или владельцы КВЭИ) и считаются ответственными за КВЭИ:

- Владельцы лицензий на передачу электроэнергии.
- Владельцы лицензий на распределение электроэнергии.
- Владельцы объектов электрогенерации, имеющих временную акцептацию и установленную мощность 100 МВт и более.
- Владельцы лицензий на транспортировку природного газа, осуществляющие транспортировку по трубопроводу.
- Владельцы лицензий на распределение природного газа обязаны создать центр управления отгрузкой.
- Владельцы лицензий на хранение природного газа (СПГ, подземное хранение).
- Владельцы лицензий на транспортировку сырой нефти.
- Владельцы лицензий на нефтепереработку.

Помимо прочих обязанностей, указанные ответственные компании обязаны:

- Подготовить перечень рисков для мониторинга информационного процесса и обеспечения безопасности промышленных систем управления, используемых в КВЭИ.
- Подготовьте план устранения последствий, в котором четко изложены действия по снижению риска.
- Предоставить регулирующему органу форму принятия на баланс системы, в которой описываются соответствующие процессы, а также работа, которая была выполнена для обеспечения информационной безопасности и исходной информации.

Источник: The Regulation on Information Security of Industrial Systems Used in the Energy Sector, 13 July 2017, доступ по ссылке: https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm.

4.1.8. Стандарты, протоколы и правила в сфере защиты КВЭИ. Примеры типовых регламентов, используемых в странах мира

Операторы сложных высокотехнологичных объектов энергетики, таких как трубопроводы, нефтеперерабатывающие заводы и хранилища, обязаны разрабатывать и соблюдать протоколы безопасности и специальные правила в соответствии с национальным и международным законодательством. Общие требования безопасности для объектов энергетики обычно разрабатываются законодательными органами на национальном уровне и оформляются в виде национальных законов.

Эти законы должны соответствовать международным требованиям и рекомендациям, применимым к данному конкретному типу учреждения. Например, протоколы портовых терминалов СПГ должны строго соответствовать требованиям Международной конвенции по охране человеческой жизни на море (ИМО СОЛАС)[87] и Международного кодекса по охране судов и портовых сооружений (ИСПС),[88] а также мерам по повышению безопасности на море и национальным требованиям.

В целях обеспечения высокого уровня безопасности многие государства-члены разрабатывают требования (стандарты) по проектированию, строительству, эксплуатации и обслуживанию различных типов энергетической инфраструктуры. Соблюдение стандартов помогает снизить риски и способствует надлежащей работе энергетической инфраструктуры. Например, в США, где КВЭИ соединяет или проложена в зданиях, к некоторым компонентам инфраструктуры могут применяться строительные нормы и стандарты. Например, электрооборудование должно соответствовать строительным нормам и стандартам, поскольку эти компоненты часто являются частью конструкции здания.[89]

С 2019 года Министерство общественной безопасности Китайской Народной Республики стандартизировало профилактические меры по защите энергетических объектов и выпустило 12 отраслевых стандартов безопасности по борьбе с терроризмом, связанных с энергетической инфраструктурой, которые регулируют деятельность нефтяных и газовых месторождений, нефтеперерабатывающей и химической промышленности, предприятий по сбыту нефтепродуктов и природного газа, инжиниринговых услуг, транспортных и нефте- и газопроводных предприятий, а также электросетей, предприятий тепловой энергетики, гидроэнергетики, ветроэнергетики, солнечной энергетики и других предприятий.[90]

Во многих случаях протоколы и стандарты безопасности для КВЭИ включают:

- Методология определения категории риска объекта, например, правила категоризации. Данная процедура предполагает дифференциацию требований безопасности для конкретных объектов в зависимости от степени потенциальной опасности и возможных последствий противоправных действий или вмешательств.

---

87 Доступ по ссылке: International Convention for the Safety of Life at Sea (SOLAS), 1974.
88 Доступ по ссылке: The International Ship and Port Facility (ISPS) Code.
89 *Infrastructure Codes, Standards, and Regulations: Frequently Asked Questions*, 2023, доступ по ссылке: https://sgp.fas.org/crs/misc/R47666.pdf.
90 По информации Региональной антитеррористической структуры ШОС.

- Правила и структура плана безопасности объекта, которые помогают разрабатывать меры безопасности.
- Перечень необходимого оборудования, как физического, так и информационного, а также соответствующие финансовые ресурсы, которые необходимо выделить в бюджете учреждения.
- Критерии нарушений безопасности, о которых необходимо сообщать в ответственный национальный орган.
- При необходимости индивидуальные требования безопасности для каждого типа объекта. Например, элементы объекта энергетики, такие как буровые площадки при разведке, могут потребовать иных мер защиты по сравнению с трубопроводами средней протяженности из-за различий в местоположении, рассредоточении и доступности.

В то же время введение стандартов эффективности регулирования часто не решает внутренних проблем из-за медлительности бюрократических процессов. Традиционные модели регулирования рассматриваются отраслевыми экспертами как антитеза инноваций, наблюдаемых в частном секторе и среди тех, кто создает, эксплуатирует и использует инфраструктуру ИКТ.[91]

Во многих государствах-членах протоколы безопасности применяются не только к энергетическим объектам, но и к прилегающим территориям, определяемым как «зона/район безопасности». К транспорту и лицам, въезжающим или перемещающимся в этих зонах, обычно применяются особые правила.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 5

Зоны безопасности вокруг критически важных нефтяных объектов в Танзании

Согласно пункту 203 Закона Танзании о нефти (2015 г.), Управление по регулированию добычи нефти в Танзании (PURA) отвечает за регулирование зон безопасности вокруг критически важных нефтяных объектов. Зоны безопасности также могут быть созданы перед размещением объектов или вокруг заброшенных или оставленных объектов.

Операторы нефтяных объектов обязаны создавать такие зоны под контролем PURA. PURA определяет размеры этих зон вокруг нефтехранилищ, заводов, нефтеперерабатывающих заводов и трубопроводов и устанавливает для них дополнительные требования безопасности, такие как правила допуска лиц и транзитной доступности. В случае аварий и чрезвычайных ситуаций эти зоны безопасности могут быть расширены, а меры досмотра усилены.

Если зоны безопасности пересекают международные границы, PURA должна проконсультироваться с Министерством энергетики Танзании.

Источник: https://www.ewura.go.tz/wp-content/uploads/2020/04/The-Petroleum-Act-2015-1.pdf.

[91] Melkunaite, Laura & Giroux, Jennifer. (2013). *Information Sharing for Critical Energy Infrastructure Protection: Finding value & overcoming challenges*. NATO Energy Security Centre of Excellence. URL: https://www.researchgate.net/publication/281584950_Information_Sharing_for_Critical_Energy_Infrastructure_Protection_Finding_value_overcoming_challenges.

Инструмент 1

Сертификат безопасности («паспорт безопасности») критически важных объектов энергетики как часть управления рисками в Азербайджане, Казахстане и Российской Федерации

«Паспорт безопасности» энергетической инфраструктуры обычно отражает характеристики объектов, возможные социально-экономические последствия незаконного вмешательства (например, террористического акта), категорию объекта, состояние его системы физической защиты и пожарной безопасности. Кроме того, паспорт безопасности критического энергетического объекта содержит меры по обеспечению безопасности и антитеррористической защищенности с учетом его специфики, местонахождения и масштабов.

В Азербайджанской Республике паспорт безопасности объекта является основным документом, отражающим данные, удовлетворяющие критериям безопасности объекта.[92] Владелец или оператор объекта должен представить декларацию безопасности на утверждение компетентным органам исполнительной власти. Утверждение декларации безопасности объекта является основанием для включения объекта в Государственный реестр.

В Республике Казахстан паспорт безопасности объекта является инструментом повышения антитеррористической защищенности объектов, уязвимых к таким угрозам.[93] Он включает в себя меры по предупреждению террористических актов в зависимости от типа энергетического объекта.

В Российской Федерации паспорт безопасности критически важных энергетических объектов формируется на основе двухкомпонентной оценки: категоризации объекта согласно оценке риска и достаточности реализованных мер безопасности. Сюда входят инженерно-технический контроль, протоколы физической защиты и меры по борьбе с терроризмом, соответствующие установленным правительством требованиям безопасности.[94]

Инструмент 2

Сведения о КВЭИ

Сведения о критически важной энергетической инфраструктуре (CEII) включают конкретную инженерную информацию, информацию об уязвимостях или подробную информацию о проекте предлагаемой или существующей КВИ (физической или виртуальной), которая:

- Относится к производству, генерации, передаче или распределению энергии.
- Представляет интерес для лица, планирующего нападение на КВЭИ.
- Предоставляет стратегическую информацию за пределами местонахождения КВЭИ.

92 Правовое обеспечение безопасности объектов топливно-энергетического комплекса: опыт СНГ, 2022, доступ по ссылке: https://gubkin.ru/faculty/faculty-of-complex-safety-of-the-fuel-and-energy-complex/kafedry-i-podrazdeleniya/knb/files/metod_materialy/prav_obespech_obj_tek.pdf.

93 Об утверждении типового паспорта антитеррористической защищенности объектов, уязвимых в террористическом отношении, 2023, доступ оп ссылке: https://adilet.zan.kz/rus/docs/V2300032950.

94 Постановление Правительства РФ от 10 ноября 2022 г. N 2034 "Об утверждении Правил разработки и формы паспорта безопасности критически важного объекта", доступ по ссылке: https://base.garant.ru/405693779/.

Обычно регулирующие органы КВЭИ устанавливают специальные правила и стандарты обработки конфиденциальной информации, известные как CEII. Операторы CEII могут снизить риски физической и информационной безопасности, предоставляя правительству и отрасли сведения об уязвимостях, угрозах, местоположении или конструкции. Эти сведения важны для планирования и реагирования на чрезвычайные ситуации в сфере энергетики. Однако могут быть и исключения. Например, в США для предотвращения публичного раскрытия информации CEII существует освобождение от обязательного раскрытия в соответствии с Законом о свободе информации.[95]

4.1.9. Учет прав человека при обеспечении безопасности КВЭИ

Террористические атаки на КВЭИ имеют глубокие и прямые последствия для прав человека. Учитывая потенциальное воздействие на население и роль, которую такая инфраструктура играет в поддержании или обеспечении жизненно важных общественных функций, нападения на КВЭИ могут иметь отрицательные последствия для широкого диапазона прав человека, включая право на жизнь (статья 3 Всеобщей декларации прав человека и статья 6 МПГПП), безопасность личности, право на здоровье и благоприятную окружающую среду, право на образование, а также другие аспекты права, отвечающие достаточному уровню жизни.

Надлежащее функционирование КВЭИ имеет жизненно важное значение для предоставления адекватных услуг населению, а также для поощрения и защиты его прав человека, поскольку нарушение работы такой инфраструктуры в результате террористической атаки может нанести катастрофический ущерб местным сообществам. Например, это может включать в себя массовые травмы, гибель людей и вынужденное перемещение, что имеет отрицательные последствия для права на здоровье (статья 12 Международного пакта об экономических, социальных и культурных правах) и других правах человека. Аналогичным образом, нарушение работы или разрушение нефтегазовой инфраструктуры также может иметь серьезные экологические последствия для сообществ, включая загрязнение воды, воздуха и другие формы загрязнения. Наконец, важно признать различное воздействие терроризма и мер по борьбе с терроризмом на различные слои населения, а именно на женщин и девочек, мужчин и мальчиков.[96]

Более того, такие нападения могут дестабилизировать деятельность правительств, подорвать гражданское общество, поставить под угрозу мир и безопасность, а также социально-экономическое развитие, что существенно повлияет на осуществление прав человека.

Обязанность государств защищать права человека подразумевает обязательство принимать необходимые и адекватные меры для предотвращения, пресечения и уголовного преследования действий, которые ставят под угрозу права лиц, находящихся под их юрисдикцией, включая терроризм. Поэтому уважение прав человека и международного права должно стать основой разработки правовых рамок и политики по противодействию террористическим угрозам для КВЭИ. Согласно IV компоненту Глобальной контртеррористической стратегии ООН, меры по борьбе с

95 Источник: US Federal Energy Regulatory Commission: https://www.ferc.gov/ceii.
96 См. *UN Women 2023 Report on Energy*.

терроризмом должны соответствовать международному праву, в частности международному праву в области прав человека, международному гуманитарному праву и праву беженцев. Государствам-членам следует руководствоваться, в частности, Глобальной контртеррористической стратегией ООН (ГКС) с тем, чтобы гарантировать, что уважение прав человека является не конкурирующими, а взаимодополняющими и взаимоподкрепляющими целями в борьбе с терроризмом, принимая во внимание также гендерные и возрастные аспекты.

Разработка и совершенствование мер по обеспечению защиты КВЭИ от террористических актов не должны осуществляться за счет чрезмерного ограничения прав граждан или ухудшения условий труда. В случае террористического акта в отношении граждан, достигающего уровня чрезвычайного положения, угрожающего жизни нации и существование которого было официально объявлено, государства могут принять меры, освобождающие их от обязательств по международному праву в области прав человека, в той мере, в какой это строго вытекает из требований ситуации, и при соблюдении определенных условий.[97] Должны быть предусмотрены адекватные гарантии, включая надзор для недопущения злоупотреблений, а меры отступления должны быть отменены после восстановления нормального положения, учитывая их исключительный и временный характер. Помимо ситуации с объявлением чрезвычайного положения, государства могут ограничивать осуществление определенных прав при условии, что эти ограничения соответствуют принципам законности, необходимости, соразмерности и недискриминации. Государствам-членам рекомендуется проводить регулярные оценки воздействия мер, принимаемых в ответ на террористические акты против КВИ, на права человека, чтобы способствовать тому, чтобы такие меры подкреплялись фактической обстановкой и были соразмерными.

4.2. Институциональные рамки/механизмы противодействия террористическим угрозам в отношении КВЭИ

Необходимым условием эффективной координации обеспечения защиты КВИ и недопущения дублирования функций является обеспечение инклюзивного участия всех субъектов, включая государственные и негосударственные. К последним относятся, в частности, частные охранные предприятия, которые обычно непосредственно осуществляют охрану критической инфраструктуры.

[97] Международный пакт о гражданских и политических правах (принятый 16 декабря 1966 г., вступивший в силу 23 марта 1976 г.) предусматривает в статье 4: “1. Во время чрезвычайного положения в государстве, при котором жизнь нации находится под угрозой и о наличии которого официально объявляется, участвующие в настоящем Пакте Государства могут принимать меры в отступление от своих обязательств по настоящему Пакту только в такой степени, в какой это требуется остротой положения, при условии, что такие меры не являются несовместимыми с их другими обязательствами по международному праву и не влекут за собой дискриминации исключительно на основе расы, цвета кожи, пола, языка, религии или социального происхождения. 2. Это положение не может служить основанием для каких-либо отступлений от статей 6, 7, 8 (пункты 1 и 2), 11, 15, 16 и 18. 3. Любое участвующее в настоящем Пакте Государство, использующее право отступления, должно немедленно информировать другие Государства, участвующие в настоящем Пакте, через посредство Генерального секретаря Организации Объединенных Наций о положениях, от которых оно отступило, и о причинах, побудивших к такому решению. Также должно быть сделано сообщение через того же посредника о той дате, когда оно прекращает такое отступление”.

4.2.1. Общегосударственный (межведомственный) подход к защите от КВЭИ

Обеспечение защиты КВЭИ неизбежно предполагает участие различных государственных органов и учреждений на разных уровнях управления — от национального до местного. Таким образом, координация этих усилий имеет основополагающее значение и обычно определяется в стратегии национальной безопасности страны или политике борьбы с терроризмом.

Отсутствие механизмов координации может создать значительные проблемы. Например, в определенной стране может проводиться сбор различных служб безопасности для проведения анализа связанных с терроризмом разведданных для оценки угроз КВЭИ. С одной стороны это способствует позитивной конкуренции и взаимодополняемости, а с другой, может привести к дублированию и фрагментации усилий, если нет четкой структуры реагирования. Кроме того, отсутствие стандартизированных процедур и различия в терминологии могут помешать достижению всестороннего понимания и реализации эффективных мер.

Как указывается в Руководстве ОБСЕ по передовой практике в области защиты неядерной критической энергетической инфраструктуры, государственные органы могут иметь разные подходы к координации. При этом некоторые органы власти «являются сторонниками рыночного подхода, в то время как другие твердо верят в законодательную роль государства». Эти различия могут стать серьезной проблемой, в том числе при взаимодействии с субъектами из частного сектора.[98]

Последовательный общегосударственный (межведомственный) подход к обеспечению защиты КВЭИ зарекомендовал себя в качестве положительной практики, способствующей укреплению эффективной межведомственной координации на национальном уровне. При таком подходе приоритет должен отдаваться эффективной координации между всеми субъектами, включая министерства (например, отвечающие за энергетический сектор, безопасность, внутренние дела и оборону), региональные органы и регулирующие органы, сотрудничающие на стратегическом, тактическом и оперативном уровнях.

4.2.2. Формы межведомственной координации для укрепления и поддержания безопасности КВЭИ

Некоторые формы межведомственной координации для укрепления и поддержания безопасности КВЭИ включают в себя:

- Горизонтальная координация: Сотрудничество между ведомствами одного уровня. Например, министерства транспорта и энергетики могли бы совместно проводить оценку рисков КВЭИ в рамках своего горизонтального сотрудничества.

[98] Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства, Вена, 2013, доступ по ссылке: www.osce.org/atu/103500?download=true.

- Вертикальная координация: Взаимодействие между различными уровнями власти. Например, орган безопасности национального уровня может издать общие рекомендации по защите от КВЭИ для местных органов власти. Эти рекомендации затем послужат основой для разработки каждым органом более конкретных стандартов безопасности для своих объектов.

Для содействия координации между ведомствами, участвующими в защите КВЭИ, многие государства-члены законодательно устанавливают специальные механизмы управления, которые позволяют государственным органам, операторам энергетической инфраструктуры и местным органам власти обмениваться информацией. Эти механизмы часто включают в себя комбинацию политических инструментов - от регулирования до механизмов стимулирования - для обеспечения реализации мер по контртеррористической защите энергетической инфраструктуры.

Анализ практического примера 6

Межведомственный координационный подход Туркменистана к антитеррористической защите инфраструктуры по производству природного газа

Министерство внутренних дел Туркменистана совместно с Министерством обороны и другими соответствующими ведомствами осуществляет охрану важнейших объектов энергетики, а также оперативно-розыскную деятельность по выявлению и пресечению противоправных действий, направленных на нарушение их функционирования. В рамках усилий по защите КВЭИ правительство провозгласило принцип неделимости сложившихся систем магистрального трубопроводного транспорта, а также транспортных систем, которые будут образовываться в перспективе. Оно также считает тесное межведомственное сотрудничество необходимым условием для защиты трубопроводов, расположенных во внутренних и приграничных районах Туркменистана.

Источник: https://turkmenistan.gov.tm/ru/post/19819/garantii-nadezhnosti-i-bezopasnosti.

4.2.3. Взаимодействие правоохранительных органов и органов национальной безопасности в контексте защиты энергетической инфраструктуры

В современных условиях обеспечения безопасности защита энергетической инфраструктуры от террористических атак является сложной, многоаспектной задачей, требующей совместных усилий органов национальной безопасности и правоохранительных органов. Поскольку в этих органы могут использоваться разные подходы и методы, тесное сотрудничество и регулярное взаимодействие имеют основополагающее значение. Национальная законодательная база также должна позволять этим ведомствам обмениваться соответствующими разведывательными данными и информацией, соблюдая при этом международное право, включая международное право в области прав человека.

Партнерское сотрудничество между правоохранительными органами и органами национальной безопасности могло бы основываться на общих задачах, четко определенных функциях и взаимных обязательствах по предоставлению необходимых ресурсов. Такая координация могла бы включать:

- Совместное и взаимодополняющее стратегическое и оперативное планирование
- Совместные оценки рисков и угроз
- Периодический обмен информацией
- Создание институциональной платформы для обмена информацией в чрезвычайных ситуациях
- Совместные учения
- Совместные операции, например, осуществление сбора информации с участием сотрудников разных ведомств

4.2.3.1. Межведомственный обмен информацией

Хорошо налаженная система связи часто помогает соответствующим ведомствам получить новые сведения о террористических угрозах объектам энергетики. Обмен информацией может быть как ситуативным (информация о конкретном событии, факты), так и аналитическим (оценки, прогнозы, анализ опыта) и, в случае КВЭИ, обычно охватывает три уровня:[99]

- Стратегическое планирование и инвестирование для принятия эффективных решений по управлению рисками
- Ситуационная осведомленность, как для обычных операций, так и во время кризисов или инцидентов, включая сообщения о подозрительной активности, анализ инцидентов и рекомендуемые действия по защите
- Оперативное и тактическое планирование и исполнение

В этом контексте ключевым моментом является наращивание потенциала соответствующих ведомств для адекватного обмена информацией и принятия мер на ее основе. Например, в некоторых государствах-членах контртеррористические центры или специализированные органы безопасности организуют семинары, на которых специалисты из разных министерств и ведомств делятся передовым опытом по обмену аналитической информацией и особенностями, связанными с защитой КВЭИ, например, как оснастить энергетические объекты инженерно-техническими средствами и системами безопасности; как организовать физическую безопасность, методы досмотра посетителей, транспортных средств и багажа; конкретные террористические угрозы (организационная структура, методы действия, тактика и т. д.); как реагировать на опасность возникновения пожара, токсичные и опасные вещества, меры по предотвращению и реагированию на чрезвычайные ситуации; как идентифицировать взрывные устройства и как реагировать на их обнаружение (классификация, процедуры, меры безопасности и т. д.).

[99] Melkunaite L., Giroux J. (2013) *Information Sharing for Critical Energy Infrastructure Protection: Finding value & overcoming challenges*, доступ по ссылке: https://www.researchgate.net/publication/281584950_Information_Sharing_for_Critical_Energy_Infrastructure_Protection_Finding_value_overcoming_challenges.

Учет гендерных и возрастных особенностей при планировании, сборе, анализе и распространении разведывательных данных является еще одним способом выявления признаков нестабильности, которые могли быть упущены из виду, и позволяет сформировать комплексное представление о социальном контексте и динамике. Это, в свою очередь, помогает предвидеть возможные неблагоприятные последствия сбора и распространения разведывательной информации для гражданских, политических прав и прав человека лиц, которых это касается.

4.2.4. Институциональная архитектура для координации защиты КВЭИ

Что касается обеспечения подотчетности, то передовая практика подчеркивает важность определения для координации защиты КВЭИ министерств или департаментов, имеющих достаточные для этого ресурсы. Во многих странах для этого обычно задействовано специализированное подразделение в Министерстве внутренних дел, специализированные группы в Вооруженных силах или специальное агентство по противодействию террористическим угрозам в отношении КВЭИ.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 7

Департамент охраны стратегических трубопроводов МВД Грузии (SPPD)

SPPD входит в состав Министерства внутренних дел Грузии, в его задачи входит охрана терминала Супса, нефтепровода Баку-Тбилиси-Джейхан и Южнокавказского газопровода Баку-Тбилиси-Эрзурум, а также соответствующей инфраструктуры. К функциям SPPD относятся:

- Обеспечение защиты и безопасности: Обеспечение безопасности терминала Супса, нефтепровода Баку-Тбилиси-Джейхан и Южнокавказского газопровода Баку-Тбилиси-Эрзурум, а также связанной с ними инфраструктуры путем реализации комплексных мер.
- Оценка рисков и сбор оперативной информации: Оценка рисков, сбор и анализ информации, связанной с безопасностью охраняемых объектов, и ведение разведки.
- Меры по реализации функций: Координация и сотрудничество с другими ведомствами для принятия соответствующих мер в отношении правонарушителей с целью обеспечения безопасности охраняемых объектов.
- Дополнительная ответственность: Осуществление других функций и задач, определенных «Законом Грузии о полиции» и другими соответствующими нормами.

Источник: https://police.ge/en/ministry/structure-and-offices/strategiuli-milsadenebis-datsvis-departamenti?sub=9658

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 8

Нефтяная полиция Ирака

Нефтяная полиция — специальный орган безопасности, созданный в Ираке в 2007 году для защиты КВЭИ. Нефтяная полиция является частью Министерства нефти и охраняет нефтяные месторождения Ирака, в основном в Басре и на юге Ирака, охватывая 4300 миль газо- и нефтепроводов. Силы нефтяной полиции хорошо оснащены и включают мобильные моторизованные подразделения, которые развернуты вокруг нефтяных месторождений и электростанций в Салах-эд-Дине и Киркуке, а также на нефтяных месторождениях Аль-Кайяра и Наджма недалеко от города Мосул.[100]

Нефтяная полиция Ирака для обеспечения мер защиты координирует свои действия с иракской федеральной полицией и силами совместных операций, техническими группами Министерства нефти и Корпусом гражданской обороны.

Обязанности нефтяной полиции включают:

- Защита нефтегазовой инфраструктуры от вооруженных нападений и диверсий
- Предотвращение контрабанды нефти и нефтепродуктов за рубеж
- Противодействие иным противоправным действиям, в том числе хищению нефтепродуктов путем врезки в нефтепровод

4.2.5. Государственно-частное сотрудничество

При разработке политики защиты объектов энергетики от террористических угроз крайне важно привлекать все заинтересованные стороны, поскольку многие энергетические объекты эксплуатируются частным сектором. Учитывая, что основная ответственность за защиту активов и систем КВЭИ лежит на их владельцах и операторах, создание эффективных ГЧП имеет решающее значение для обеспечения адекватного уровня защиты.

Кроме того, промышленные предприятия и связанные с ними организации обладают бесценным опытом в части знания конкретных функциональных возможностей объектов КВЭИ. Эти знания касаются в том числе взаимосвязи с другой инфраструктурой, присущих уязвимостей и особых требований к техническому обслуживанию и ремонту.

В зависимости от правовой базы собственниками и эксплуатантами объектов КВЭИ не всегда могут быть одни и те же лица, а потенциальными операторами могут быть частные компании, государственные организации или смешанные государственно-частные консорциумы. В этом процессе могут участвовать и иностранные компании, особенно в странах транзита. Эти организации в силу своего права собственности или функций эксплуатанта обязаны проводить тщательную оценку рисков и угроз. Эти оценки должны учитывать как текущие, так и возникающие угрозы

[100] *Understanding the security bureaucracy in Iraq: agencies and their tasks*, July 2020, ORSAM Report, доступ по ссылке: https://orsam.org.tr/d_hbanaliz/understanding-the-security-bureaucracy-in-iraq-agencies-and-their-tasks.pdf

и соответствовать требованиям безопасности, политике и рекомендациям, установленным государственными органами и соответствующими отраслевыми ассоциациями.

Частные организации, участвующие в ГЧП, должны соблюдать процедуры комплексной проверки, предусмотренные национальным законодательством стран, в которых они осуществляют свою деятельность.

4.2.6. Факторы, способствующие укреплению ГЧП в области защиты КВЭИ

ГЧП могут существенно различаться по форме: от неформального сотрудничества до более формальных соглашений. Уровень формальности часто отражает степень контроля, которую государственные органы желают сохранить, а также правовой и культурный контекст. Проектно-ориентированные ГЧП часто считаются более эффективными, чем ГЧП, ориентированные на процесс благодаря четко определенным целям, срокам и бюджетам.[101]

Однако ряд проблем может отрицательно повлиять на эффективность ГЧП в области защиты КВЭИ. К числу таких проблем относятся различия в ожиданиях между частным и государственным секторами, отсутствие доверия между сотрудничающими сторонами и нечеткое распределение задач. Эксперты часто отмечают значительные различия в организационной культуре и бюрократических процессах между государственными и частными структурами.

Напротив, передовая практика подчеркивает важность содействия инклюзивному процессу. Этот процесс должен включать многогранный подход, включающий выявление и классификацию угроз для КВЭИ; создание надежных механизмов коммуникации и координации; содействие эффективному сотрудничеству между государственными и частными субъектами; последовательное внедрение согласованных защитных мер и определение четких и недвусмысленных обязанностей для всех субъектов ГЧП. Расставив приоритеты по этим ключевым элементам, субъекты могут разработать надежную и эффективную модель ГЧП для защиты КВЭИ.

Механизмы, используемые для развития сотрудничества между государственным и частным секторами в сфере защиты КВЭИ, различаются в зависимости от страны. Хотя это и не исчерпывающий список, общие элементы часто включают в себя:

- Взаимное предоставление информации, мониторинг и обмен передовой практикой (см. 4.2.6.1)
- Совместное управление рисками и координация при разработке планов реагирования на чрезвычайные ситуации (см. 4.2.6.2)
- Сотрудничество в разработке правил безопасности (см. 4.2.6.3)
- Совместные учения и тренировки по безопасности (см. 4.2.6.4)

[101] Проектно-ориентированные ГЧП сосредоточены на четко определенной задаче в рамках безопасности энергетической инфраструктуры. Эти партнерства имеют ограничение по времени, характеризуются срочностью и решают такие важные вопросы, как разработка конкретных правил взаимодействия для решения конкретной проблемы.

4.2.6.1. Взаимное предоставление информации, мониторинг и обмен передовой практикой в рамках ГЧП

Взаимное предоставление информации является одним из важнейших аспектов государственно-частного сотрудничества в сфере защиты КВЭИ. Следует поощрять совместный подход, способствующий обмену данными, знаниями и опытом между субъектами энергетической инфраструктуры. В подготовленном UNDRR Руководстве по внедрению принципов устойчивой инфраструктуры указывается, что «организации с общими взаимозависимостями должны иметь возможность обмениваться данными стандартизированным образом и вырабатывать общие идеи о том, как справляться с общими угрозами».[102] Такой обмен информацией способствует созданию среды обучения, позволяя заинтересованным сторонам получать ценную информацию о прошлых нарушениях безопасности и разрабатывать единую стратегию реагирования на распространенные террористические угрозы.

Эмпирические наблюдения показывают, что эффективный обмен информацией между государственным и частным секторами в сфере защиты КВЭИ основывается на трех принципах:

- Развитие доверия: укрепление доверия между всеми субъектами со стороны ведущих ведомств.
- Реализация мер безопасности: обеспечение защиты конфиденциальной информации, распространение которой поощряется или является обязательным в рамках соглашений о защите КВЭИ.
- Разработка правовой базы: создание эффективной правовой архитектуры для облегчения сотрудничества.

Еще одной причиной укрепления ГЧП и создания соответствующей структуры сотрудничества является то, что отделы безопасности энергетических компаний часто оказываются непосредственно вовлеченными в сбор информации о потенциальной незаконной деятельности в отношении объектов энергетики, или могут быть обязаны по закону готовить и передавать данные об инцидентах, связанных с безопасностью, правоохранительным органам или государственным службам безопасности.

[102] *Handbook for Implementing the Principles for Resilient Infrastructure*, 2020, доступ по ссылке: https://www.undrr.org/media/87213/download?startDownload=20240612.

Вставка 5

ГЧП в обмене информацией для защиты энергетической инфраструктуры

Для многих стран ГЧП стали ключевым инструментом создания структуры обмена информацией об угрозах и уязвимостях, влияющих на национальную инфраструктуру, а также для координации действий между государственными и частными субъектами. Во многих случаях обмен информацией, совместные учения и совместная оценка рисков позволяют преодолеть распыление ответственности и координировать работу.

Хотя и частный, и государственный секторы поддерживают эти партнерства, разработка и внедрение эффективных механизмов обмена информацией на практике оказываются сложными из-за культурных различий между двумя секторами. В то время как некоторые ГЧП смогли установить эффективные отношения по обмену информацией и наладить координационные связи, другим сложно развивать такие партнерства из-за опасений относительно ненадлежащего раскрытия информации и других несоответствий между ожиданиями и приоритетами частных и государственных субъектов.

Например, отсутствие прозрачности и информации о партнерской стороне существенно затрудняет, если не делает невозможным, понимание должностными лицами коренных причин и возможных каскадных взаимозависимостей между затронутыми критически важными секторами и влиянием на национальную безопасность и экономику.

Что касается обмена информацией и мониторинга, то различные субъекты обычно выполняют следующие задачи:

- **Правительство:**
  - Разрабатывает государственную политику мониторинга КВЭИ и регулирования обмена информацией, особенно конфиденциальной информации.
- **Регулирующие органы:**
  - Обеспечивают соблюдение государственных норм, касающихся мониторинга и проверки энергетической инфраструктуры на предмет соответствия.
  - Организуют семинары и консультации с представителями энергетической отрасли для выработки требований.
- **Владельцы:**
  - Запрашивают проведение мониторинга и проверки критически важных объектов энергетической инфраструктуры и обеспечивают совершенствование операторами навыков сбора данных и предотвращения сбоев.
- **Операторы:**
  - Внедряют системы мониторинга, собирают достоверные данные, проводят анализ и внедряют передовую практику, рекомендованную регулирующими органами.

4.2.6.2. Совместное управление рисками и координация при разработке планов реагирования на чрезвычайные ситуации

Структура управления рисками, разработанная для ГЧП в части защиты КВЭИ, в приоритет ставит универсализм использования. Для достижения этой цели структура разработана с высокой степенью гибкости, что позволяет каждому субъекту адаптировать свои стратегии управления рисками для устранения конкретных угроз в своей сфере ответственности. Такая адаптивность обеспечивает комплексный и детализированный подход к снижению рисков в рамках ГЧП.

Распространенным подходом является создание специализированных постоянных рабочих групп, в состав которых входят представители широкого спектра субъектов ведущего энергетического сектора, включая как участников отрасли, так и регулирующие органы. Например, обеспечение информационной безопасности на объектах нефтегазовой отрасли представляет собой уникальную задачу, связанную с угрозами со стороны третьих лиц.[103] Эффективная оценка рисков в этом контексте требует тесного сотрудничества с частными компаниями,[104] чего можно добиться посредством создания постоянной рабочей группы с участием многих субъектов.

Для достижения оптимальной эффективности защиты КВЭИ ГЧП должны охватывать весь цикл управления рисками. Это включает в себя привлечение частных компаний к мониторингу и контролю процессов для предоставления актуального обзора комплекса угроз. Такой комплексный подход расширяет рамки ГЧП за пределы подготовительной фазы и включает в себя усилия по управлению кризисами и восстановлению.

Кроме того, ГЧП имеют важное значение для разработки эффективного плана управления кризисными ситуациями, включая террористические акты, направленные в отношении энергетической инфраструктуры. Эти планы должны охватывать как государственные, так и частные субъекты и быть сосредоточены на (1) защите гражданского населения и (2) обеспечении непрерывности бизнеса.

4.2.6.3. Сотрудничество в разработке правил безопасности

Разработка общенациональных требований и стандартов безопасности в энергетическом секторе, аналогичных требованиям других важнейших отраслей промышленности, требует совместного и инклюзивного подхода. Эти совместные усилия требуют активного участия владельцев КВЭИ, операторов и поставщиков. Такой подход имеет первостепенное значение для достижения оптимального баланса между общественной безопасностью и сохранением жизнеспособности энергетической отрасли. Стандарты безопасности должны эффективно снижать риски, не создавая при этом чрезмерного бремени для прибыльности отрасли, не препятствуя своевременной реализации или не ставя под угрозу техническую осуществимость этих мер.

В рамках этого инклюзивного подхода субъекты из частного сектора могли бы предлагать изменения в существующие стандарты безопасности или правительственные рекомендации, например, в отношении трубопроводов в зонах безопасности, в рамках прозрачного и консенсусного ГЧП.

---

[103] Риск третьих лиц — это любой риск, привносимый в организацию внешними сторонами в ее цепочке поставок.

[104] https://www3.weforum.org/docs/WEF_Advancing_Supply_Chain_Security_in_Oil_and_Gas_2021.pdf.

Хорошим примером является Комиссия по регулированию добычи нефти в Нигерии. Как национальный регулирующий орган энергетической инфраструктуры, Комиссия с 2021 года проводит специальные форумы и семинары, посвященные поощрению сотрудничества в разработке правил для их эффективного внедрения и устойчивого соблюдения всеми субъектами.[105]

4.2.6.4. Совместные учения и тренировки по безопасности в рамках ГЧП

Мероприятия по защите КВЭИ по своей сути многогранны, что требует координации и оперативного сотрудничества между частными службами безопасности и их коллегами из государственных ведомств, включая правоохранительные органы Учитывая транснациональный и трансграничный характер многих объектов КВЭИ (часто расположенных вблизи сухопутных или морских границ), такой подход к сотрудничеству особенно важен. Участие в совместных учениях и тренировках способствует формированию бесценного опыта в реализации дополнительных мер безопасности, обеспечивая комплексную и эффективную защиту от террористических угроз.

Например, после ряда атак БАС на нефтеперерабатывающие заводы в Саудовской Аравии в 2021 году военно-морские силы Саудовской Аравии провели комплексные учения с нефтяными компаниями в целях предотвращения атак беспилотников и ракет в отношении «жизненно важных нефтяных объектов».[106]

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 9

Индонезийское ГЧП в защите энергетических объектов от террористических атак

Военно-морские силы Индонезии совместно с элитными силами страны, Национальными вооруженными силами Индонезии и Национальной полицией провели серию учений с индонезийской нефтегазовой компанией с целью повышения защиты энергетической инфраструктуры от террористических атак.[107]

В ноябре 2023 года элитные силы ВМС Индонезии приняли участие в учениях по освобождению захваченного танкера-нефтепродуктовоза «Санга-Санга» в водах Баликпапана, Восточный Калимантан. По сценарию учений, проведенных в водах Баликпапана, танкер «Санга-Санга», собиравшийся войти в залив Баликпапан, подвергся нападению со стороны 20 вооруженных похитителей, использовавших два быстроходных катера и приблизившихся с левого борта судна. Также была имитирована террористическая деятельность вблизи морской нефтяной платформы в Сепингане.

Учения по реагированию на нарушения безопасности на море были проведены оперативно с привлечением 274 человек из антитеррористического отряда «Денджака» при поддержке различных подразделений ВМС Индонезии. В ходе проведенной ВМС Индонезии операции против захватчиков на танкере и морской платформе все угрозы были нейтрализованы.

105 Доступ по ссылке: https://leadership.ng/stakeholders-engagement-and-anticipated-oil-gas-industry-turnaround/.
106 Доступ по ссылке: https://www.worldoil.com/news/2021/3/22/aramco-and-saudi-navy-start-exercises-to-thwart-drone-and-missile-attacks.
107 Например: https://www.pertamina.com/en/news-room/news-release/strengthening-security-of-national-vital-object-pertamina-indonesian-navy-conducts-emergency-drill.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 10

Канадская ресурсная инфраструктура Nexus (CRIRN)

Проект CRIRN - это специальный проект, реализуемый Отделом безопасности энергетической инфраструктуры Министерства природных ресурсов Канады (NRCan) — ведущим федеральным департаментом по безопасности КВЭИ. NRCan руководствуется тремя стратегическими целями, определенных в Национальной стратегии по критической инфраструктуре:

- Создание партнерств для поддержки и повышения устойчивости КВИ
- Внедрение комплексного подхода к управлению рисками
- Содействие своевременному обмену и защите информации при передаче между партнерами и заинтересованными субъектами.

Целью CRIRN является содействие развитию государственно-частного партнерства по обеспечению защиты КВЭИ в Канаде, а также укрепление связей между субъектами в сфере технологий, безопасности и энергетики.[108] CRIRN находится на стыке взаимодействия канадской контрразведывательной службы, служб безопасности и разведки, а также научно-исследовательских институтов. Проект опирается на опыт и доверительные отношения в целях предоставления владельцам и операторам энергетического сектора знаний и навыков для преобразования информации в действия.

Источник: https://natural-resources.canada.ca/sites/nrcan/files/science-and-data/science-research/cyber-security/eisd-booklet-en.pdf.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 11

ГЧП в защите КВЭИ в Алжире

В 2023 году правительство Алжира приступило к реализации плана по борьбе с терроризмом для защиты нефтегазовых объектов от потенциальных террористических актов, уделив особое внимание ГЧП. Этот план включал в себя прием на работу более 20000 сотрудников службы безопасности для обеспечения безопасности КВЭИ по всей стране. Дополнительно на разработку систем безопасности нефтегазовой инфраструктуры было выделено 400 млн долларов США. В результате крупнейшая алжирская нефтегазовая компания приняла новую стратегию безопасности, сотрудничая с властями в целях защиты жизненно важных энергетических объектов страны. Для дальнейшего обсуждения вопросов укрепления потенциала по борьбе с терроризмом посредством ГЧП в июле 2023 года была проведена специальная встреча с топ-менеджерами алжирского нефтегазового сектора, Министерства энергетики и горнодобывающей промышленности и сил государственной безопасности.

Источник: https://english.aawsat.com/home/article/4102616/algeria-allocates-400-mln-protect-oil-facilities-against-terrorism.

[108] Energy infrastructure security division, доступ по ссылке: https://natural-resources.canada.ca/sites/nrcan/files/science-and-data/science-research/cyber-security/eisd-booklet-en.pdf.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 12

Координация и сотрудничество между государственным и частным секторами в области защиты морской энергетической инфраструктуры в Индии

Обеспечение безопасности морских энергетических объектов требует комплексного и многостороннего подхода. В Индии эти совместные усилия возглавляются Координационным комитетом по безопасности на шельфе (OSCC), созданным в 1978 году. Выступая в качестве высшего органа по надзору и оценке безопасности на море, OSCC собирается два раза в год под председательством генерального директора Береговой охраны Индии. В его состав входят представители самых разных заинтересованных сторон, включая ВМС Индии, ВВС, Береговую охрану, Бюро разведки, Министерство иностранных дел, индийские полицейские силы и Индийскую нефтегазовую компанию.

В дальнейшем данная деятельность была дополнена «Группой советников по вопросам обороны и безопасности на море при правительстве Индии» (FODAG), созданной в 1983 году и переименованной в 2002 году. Являясь членом OSCC, FODAG выступает в качестве центрального агентства по взаимодействию с ONGC и другими компаниями по разведке и добыче нефти. Его основная функция — консультирование правительства Индии по вопросам безопасности и обороны на шельфе, касающимся объектов в морских зонах Индии.

Региональные комитеты по чрезвычайным ситуациям (РКЧС) обеспечивают дополнительный уровень координации. Под председательством начальников штабов Западного и Восточного военно-морских командований ВМС Индии эти комитеты также собираются дважды в год. Их состав аналогичен составу OSCC, но включает представителей частных компаний, работающих в секторе добычи нефти и газа.

Помимо патрулирования в целях сдерживания, важнейшим аспектом стратегии безопасности Индии на шельфе является регулярное проведение учений на случай непредвиденных обстоятельств. Кульминацией данных мероприятий являются проводимые дважды в год крупномасштабные учения под кодовым названием PRASTHAN, которые предоставляют платформу для отработки ответных действий на различные потенциальные угрозы. Реализуемые в ходе учений PRASTHAN сценарии включают в себя отработку действий по противодействию захвату судов, порядок обезвреживания бомб, ликвидацию пожаров, повреждений конструкций, разливов нефти, медицинскую эвакуацию и оказание помощи поврежденным судам. Стоит отметить, что в учениях 2023 года приняли участие представители ВМС Индии, ВВС, береговой охраны, сил безопасности индийской нефтегазовой компании, Генерального директората судоходства, полиции Махараштры, таможни, Департамента рыболовства, Управления порта Мумбаи, Управления порта Джамму и других соответствующих государственных и центральных гражданских агентств. Такое межведомственное участие обеспечивает всестороннюю и реалистичную оценку готовности к различным непредвиденным обстоятельствам, что позволяет совершенствовать установленный стандартный порядок действий.

В 2023 году учения проводились на платформе Greatdrill Chaaya. В ходе учений отрабатывались действия по ликвидации последствий непредвиденных обстоятельств, таких как пожар на нефтяной платформе, разлив нефти в пределах обозначенной зоны, чрезвычайные ситуации в полете, опасные сценарии утечки газа, оказание помощи судну, потерпевшему аварию в морской зоне, а также медицинская эвакуация экипажа платформы. В рамках учений были созданы реалистичные условия для оценки готовности всех заинтересованных сторон к решению этих непредвиденных обстоятельств и укреплению стандартных операционных процедур.

Источник: https://maritimeindia.org/physical-protection-of-indias-critical-maritime-infrastructure-part-2-maritime-energy-sector/.

4.3. Операционные рамки и техническая готовность в защите КВЭИ

За последние годы государства-члены активно адаптировали свои операционные рамки к защите КВЭИ. В большинстве случаев такие рамки включают структурированный набор рекомендаций, принципов и передовой практики, которые регулируют деятельность по защите энергетической инфраструктуры как государственного, так и частного сектора.

4.3.1. Управление рисками: угрозы, риски и уязвимости в защите энергетической инфраструктуры

13 февраля 2017 года Совет Безопасности в своей резолюции 2341 призвал 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» (пункт 2).

На основе структурированного подхода к управлению рисками все необходимые аспекты должны быть объединены и описаны в комплексной структуре, призванной помочь организациям эффективно и действенно управлять рисками. Содержание структуры управления рисками будет зависеть от размера и сложности организации/предприятия/объекта, подверженности его рискам, правовых требований и уже внедренных элементов управления рисками или систем управления.

В целом связанные за защитой КВИ процедуры управления рисками включают:

- Оценку рисков (см. 4.3.2)
- Оценку уязвимостей (см. 4.3.4)
- Оценку угроз (см. 4.3.5)

В этом случае важным является также и оценка последствий. Она включает в себя оценку потенциальных последствий атаки на КВЭИ, включая экономические, экологические и социальные последствия. Хотя оценка последствий имеет важное значение для всестороннего понимания общего риска, в настоящем Руководстве она подробно не рассматривается.

Важно отметить, что некоторые методологии включают оценки угроз, последствий и уязвимости как неотъемлемые части общей оценки риска.

Общая цель методологий оценки рисков — предоставить структуру, которая с учетом национальных приоритетов и требований конкретного сектора КВЭИ позволит эффективно распределять ресурсы защиты с целью снижения уязвимости и минимизации последствий атак.

4.3.2. Оценка рисков

Оценка риска является основополагающим шагом в обеспечении эффективного управления рисками КВЭИ, включая контроль и снижение рисков, и имеет важное значение для разработки успешных стратегий защиты КВЭИ. Несмотря на то, что существуют устоявшиеся методики, их применение для защиты от КВЭИ требует значительного опыта и технических знаний.

Особенно важны межсекторальные оценки рисков. Эти оценки охватывают энергетический сектор, а также такие взаимозависимые сектора, как финансы, информация и транспорт, выявляя критические взаимозависимости и взаимосвязи. Часто в сочетании с методами управления рисками в цепочке поставок этот подход способствует последовательной оценке и постоянному обновлению сложных макроуровневых рисков в цепочке поставок. Это позволяет владельцам КВЭИ, операторам и государственным органам эффективно расставлять приоритеты в управлении рисками.

Оценки рисков, характерные для энергетического сектора, помогают определить объекты КВЭИ, расставить приоритеты в обеспечении защиты ресурсов, таких как финансы, персонал и информация. Эти оценки также дают информацию для принятия решений о принятии мер по смягчению последствий и оперативной тактике, обеспечивая точную оценку уязвимости КВЭИ к террористическим угрозам. Это имеет решающее значение для разработки стратегий защиты КВЭИ от террористических атак и минимизации возможных потерь.

При оценке рисков, специфичных для конкретного объекта, акцент делается на уникальных уязвимостях и угрозах, связанных с каждым отдельным объектом КВЭИ, что позволяет провести более подробный анализ.

За последнее десятилетие были разработаны различные методики оценки рисков и уязвимостей в защите энергетической инфраструктуры. Примерами служат теория сетей, матрицы рейтингов и методы системной динамики.[109]

Кроме того, наличие различных подходов к управлению рисками привело к разработке широко используемых во всем мире методологий. Яркими примерами являются стандарты Международной организации по стандартизации (ИСО) по управлению рисками, которые предоставляют комплексные рамки и рекомендации по оценке и управлению рисками в различных контекстах, включая защиту КВЭИ.[110]

[109] Yao, Xijun & Wei, Hsi-Hsien & Shohet, Igal & Skibniewski, Miroslaw. (2020). *Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation*. Applied Sciences. 10. 7162. 10.3390/app10207162. https://www.researchgate.net/publication/346227204_Assessment_of_Terrorism_Risk_to_Critical_Infrastructures_The_Case_of_a_Power-Supply_Substation.

[110] Более подробная информация представлена по ссылке: https://www.iso.org/iso-31000-risk-management.html.

Инструмент 3

Пример методики анализа риска: модель BCK

Модель «Байесовская сеть — Последствия — Знания» (BCK), специально разработанная для оценки рисков террористических атак на резервуары для хранения сжиженного природного газа (СПГ), предложенная исследователями Жунчэнь Чжу, Сяофэн Ху, Ипин Байем и Синь Ли из Народного университета общественной безопасности Китая и Китайского университета горного дела и технологий (Жунчэнь Чжу и др., 202X), предлагает комплексный подход, включающий следующие ключевые элементы:

- Многомерная идентификация факторов риска: Модель BCK подчеркивает важность выявления факторов риска с многогранной точки зрения, учитывая потенциальные межсекторальные взаимозависимости, которые могут усугубить последствия атаки.
- Построение графической модели и анализ условных зависимостей: Модель использует графические модели, такие как байесовские сети, для визуального представления взаимосвязей между различными переменными и их условными зависимостями. Это способствует более точному пониманию того, как различные факторы влияют на вероятность и серьезность атаки.
- Дерево событий и теория нечетких множеств для оценки последствий: Модель BCK, основанная на анализе факторов риска, использует для оценки потенциальных последствий террористической атаки деревья событий и теорию нечетких множеств. Деревья событий обеспечивают структурированную основу для изучения различных сценариев атак и их соответствующих результатов. Теория нечетких множеств позволяет учитывать неопределенность и неоднозначность при оценке рисков.
- График знаний для хранения и визуализации знаний о рисках: Ключевым нововведением модели BCK является применение графика знаний. Этот график знаний служит центральным хранилищем знаний о рисках, включая выявленные узлы из графических моделей и оцененные последствия различных сценариев атак. Граф знаний не только облегчает хранение и извлечение информации о рисках, но и обеспечивает наглядное представление различных факторов риска и их взаимосвязей.

Источник: https://www.sciencedirect.com/science/article/abs/pii/S0925753521000370

4.3.3. Обзор и мониторинг показателей риска

Управление рисками КВЭИ должно основываться на индикаторах риска, которые обычно подразделяются на различные группы. Выявленные риски и их потенциальные последствия можно классифицировать как по общим критериям, применимым ко всем КВИ (таким как количество пострадавших и экономические последствия), так и по критериям, характерным для энергетики (таким как экологические и социальные последствия). Процесс оценки рисков включает ранжирование КВИ и моделирование взаимозависимостей путем выявления потенциальных цепочек рисков. Некоторые подходы к управлению рисками также описывают основные причины уязвимостей, связанных с потенциалом, компетентностью и функционированием КВИ.

Например, риски безопасности, связанные с трубопроводами, могут быть более серьезными, чем риски безопасности стационарных нефтеперерабатывающих заводов или НПЗ. Это связано с тем, что трубопроводы проложены на тысячи километров через различные районы, каждый из которых имеет разную плотность населения, природную среду, активы и близлежащие уязвимые центры.[111]

Другим важным аспектом является взаимозависимость между объектами энергетики и другими секторами, которую можно разделить на такие типы, как физическая, информационная, географическая и иногда логическая.[112]

Тактика и методы террора постоянно меняются, как и функционирование объектов энергетики. Например, новое оборудование или системы управления могут снизить определенные уязвимости, но также создать новые.

В этой связи в рамках управления рисками важно:

- Регулярно проверять индикаторы и сценарии угроз.
- Актуализировать перечень объектов энергетики, отнесенных к категории «критически важных» в соответствии с установленными критериями
- Переоценивать возможности риска
- Пересматривать и обновлять документацию по управлению рисками с тем, чтобы отразить изменения в контексте риска и выявить новые риски.

4.3.4. Оценка уязвимостей

Как упоминалось ранее, эффективная защита КВЭИ, основанная на подходе управления рисками, должна включать в качестве неотъемлемого компонента оценку уязвимостей. Уязвимость можно проанализировать, смоделировав, как различные компоненты инфраструктуры реагируют на угрозы, и оценив общий риск для инфраструктуры. Это включает в себя оценку последствий атаки на каждый компонент, понимание взаимодействия между компонентами и оценку совокупного воздействия как прямого, так и косвенного ущерба на общую функциональность инфраструктуры.[113.]

Оценка уязвимости может включать определение критических элементов и установление процедур защиты. Что касается КВЭИ, определенные элементы можно определить как критически важные с точки зрения функционирования инфраструктуры и более уязвимые с точки зрения прямых физических атак. Такая оценка может быть частью анализа «технологической карты», который включает оценку защит и блокировок, предназначенных для реагирования на чрезвычайные ситуации, а также выявление критических элементов (или «слабых мест»), нарушение работы которых обязательно приведет к прерыванию технологического процесса.

---

111 Donya Fakhravar, Nima Khakzad, Genserik Reniers, Valerio Cozzani, *Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network*, Process Safety and Environmental Protection, Volume 111, 2017, Pages 714-725, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2017.08.036, доступ по ссылке: https://www.sciencedirect.com/science/article/abs/pii/S0957582017302914.

112 According to relevant research of Petit F., Verner D., Brannengan D. et al. (2015), *Analysis of Critical Infrastructure Dependencies and Interdependencies*, logical dependency is attributable to human decisions and actions and is not the result of physical or cyber processes. Доступ по ссылке: https://publications.anl.gov/anlpubs/2015/06/111906.pdf.

113 См. выше.

К критическим элементам объекта энергетической инфраструктуры могут относиться:

- Конструктивные и технологические компоненты: к ним относятся основные конструкции объекта, административные здания, инженерные сооружения и системы связи. Например, на газозаправочной станции — это производственная зона с газовыми компрессорами, склад заправленных баллонов, вспомогательные зоны с газохранилищами, гаражи и т.д.
- Системные элементы: компоненты или устройства в потенциально опасных установках.
- Места хранения: места хранения оружия, боеприпасов и их составных частей, если они находятся на территории объекта.[114]
- Места хранения опасных материалов: зоны, содержащие ядовитые и/или легковоспламеняющиеся вещества.
- Другие уязвимые системы: любые другие системы, элементы или коммуникации, классифицированные по результатам оценки уязвимости как уязвимые к физическим атакам.

Результаты любой оценки уязвимости должны использоваться для разработки и внедрения планов минимизации последствий и реагирования на чрезвычайные ситуации на КВЭИ в координации с национальными или местными планами и рекомендациями.

Вставка 6

Оценка уязвимости в цикле управления рисками

Оценка уязвимости, как часть оценки рисков и общего управления рисками, представляет собой комплексное исследование, которое включает:

- Назначение и особенности: Изучение назначения, функциональных характеристик, местоположения и масштаба объекта энергетики.
- Меры защиты: Оценка ресурсов и мер физической защиты и безопасности, включая внутренние протоколы безопасности и процедуры контроля доступа.
- Критические и уязвимые зоны: Выявление критических элементов, потенциально опасных зон и уязвимых участков на объекте.
- Террористические угрозы: Оценка потенциальных террористических угроз, характерных для объекта энергетики.
- Террористические методы и последствия: Анализ возможных методов, которые террористы могут использовать для совершения атак, и ожидаемых последствий таких действий.
- Назначение и особенности: Назначение, функциональные характеристики, местоположение и масштаб объекта энергетики.
- Меры защиты: Имеющиеся ресурсы и меры физической защиты и безопасности, включая внутренние протоколы безопасности и процедуры контроля доступа.
- Критические и уязвимые зоны: Выявление критических элементов, потенциально опасных зон и уязвимых участков на объекте.
- Террористические угрозы: Потенциальные террористические угрозы, характерные для объекта энергетики.
- Террористические методы и последствия: Возможные методы, которые террористы могут использовать для совершения атак, и ожидаемые последствия таких действий.

[114] Во многих государствах службы безопасности критически важных энергетических объектов имеют на вооружении нелетальное (электрошокеры, газовые пистолеты) или летальное оружие (пистолеты, автоматические винтовки и т. д.).

Инструмент 4

Управление информацией о физической безопасности (PSIM)

PSIM — это инструмент 3D-визуализации для проектирования систем физической защиты энергетической инфраструктуры. Подходит для крупных систем, таких как, например, объекты нефтегазовой инфраструктуры, имеющие значительное количество интегрированных подсистем физической, эксплуатационной и информационной безопасности. Его можно использовать в качестве инструмента компьютерного моделирования для имитации возможных атак на стационарные объекты нефтегазовой отрасли (заводы, хранилища, нефтеперерабатывающие заводы и т. д.). При таком подходе учитываются такие факторы, как численность и оснащение нападающих, их снаряжение и транспорт. PSIM помогает улучшить эксплуатационные показатели и выбрать экономически эффективные методы.

Рекомендуется использовать методы моделирования на основе оценки рисков и рассматривать все возможные сценарии террористических атак на объект энергетики. Поэтому крайне важно проанализировать уязвимость объекта, чтобы выявить критические элементы и уязвимые зоны. Атаки на эти объекты могут повлечь за собой серьезные последствия для персонала, самого объекта и окружающей среды, вплоть до полного прекращения функционирования объекта.

Источник: Инструмент PSIM «Система физической защиты компании Итерация», доступ по ссылке: https://iter.ru/en/TERATION_PHYSICAL_PROTECTION_SYSTEM.pdf.

4.3.5. Оценка угроз

Подготовка сценариев угроз или атак должна быть частью процесса оценки угроз. Например, компьютерное моделирование возможных террористических атак на объекты КВИ включает анализ возможностей злоумышленников, например, террористов, и их доступа к новым технологиям. Моделирование также позволяет определить типы потенциальных атак и оценить уровень их сложности. Оценка угроз включает в себя выявление различных типов угроз, оценку их потенциального воздействия на объект и определение наиболее эффективных стратегий смягчения последствий на основе текущих возможностей и потребностей в ресурсах.

В сфере защиты КВЭИ моделирование угроз является ключевым методом комплексной оценки рисков безопасности. Этот метод, основанный на принципах оценки рисков, помогает выявить потенциальные уязвимости в различных сценариях безопасности, которые могут быть использованы в террористических целях. Благодаря проактивному применению моделирования угроз можно минимизировать потенциальные последствия атак на персонал, сами объекты и окружающую среду.

Однако важно осознавать очевидное разнообразие категорий инфраструктуры. Объекты одной категории могут иметь разные функциональные возможности и эксплуатационные условия, что приводит к различиям в их профилях уязвимости. Поэтому необходима единая методология анализа уязвимостей. Эта методология должна быть специально адаптирована для реагирования на уникальные сценарии, связанные с террористическими угрозами, в целях обеспечения комплексной и целенаправленной защиты от потенциальных атак.

Инструмент 5

Моделирование атак в соответствии с выявленными рисками

При разработке сценариев террористических угроз для КВЭИ можно использовать структурированный подход к моделированию потенциальных атак. Этот подход можно разбить на следующие этапы.[115]

1. Определение мотивации и типа атаки: на этом этапе определяются наиболее вероятные мотивы террористических атак на объекты КВЭИ и наиболее вероятный тип атаки.
2. Определение цели нападения: на основании выявленных мотивов в качестве потенциальных целей определяются конкретные здания или уязвимые элементы в пределах КВЭИ.
3. Методы разведки: на этом этапе анализируются методы, которые террористы могут использовать для сбора информации об объекте атаки, например, о системе безопасности, техническом оборудовании, каналах связи, месте хранения легковоспламеняющихся материалов и т.д.
4. Изучение методологии атаки: изучаются и анализируются возможные средства и методы, которые террористы могли бы использовать для совершения атаки.
5. Выявление преступника: на этом этапе основное внимание уделяется выявлению потенциальных участников нападения, включая как внешних субъектов, так и потенциальных инсайдеров.
6. Оценка ресурсов: оцениваются возможные финансовые затраты и ресурсы, необходимые для атаки.
7. Подготовка и приобретение: на этом этапе анализируются методы, используемые террористами для подготовки к нападению, включая обучение участников, а также приобретение или изготовление средств нападения.
8. Скрытая связь: рассматриваются методы установления и поддержания скрытой связи между злоумышленниками.
9. Временное и пространственное планирование: на этом этапе выбирается конкретная дата, время и место совершения нападения.
10. Отход и уничтожение улик: рассматриваются стратегии отхода после совершения нападения и устранения улик, связанных с планированием и исполнением нападения.
11. Информационная поддержка: анализируются методы распространения информации в поддержку целей нападения.

[115] Жадиков Р.С., Бекжанов М.А. Организация системы антитеррористической защиты объектов, уязвимых в террористическом отношении: науч.-практ. пособие. Алматы. Академия Комитета национальной безопасности Республики Казахстан, 2018. 104 стр.

4.3.6. Меры пресечения и реагирования в целях обеспечения защиты КВЭИ

Меры пресечения и реагирования в целях обеспечения защиты КВЭИ от террористических атак должны основываться на комплексном подходе и включать определенные меры и инструменты, соразмерные выявленным рискам, с целью:

- обеспечения физической защиты объектов энергетики (см. 4.3.6.1)
- обеспечения информационной безопасности объектов энергетики (см. 4.3.6.3)
- минимизации последствий межсекторальной взаимосвязанности (см. 4.3.6.4)
- разработки планов реагирования и действий в чрезвычайных ситуациях (см. 4.3.6.5, 4.6.5.6, 4.3.6.7)

4.3.6.1. Меры физической защиты

Меры физической защиты следует выбирать на основе ранее проведенных оценок рисков и выявленных остаточных уязвимостей. Конкретные меры, применяемые к объекту, определяют спектр используемого оборудования. Физическая защита КВЭИ предусматривает как охрану периметра, так и внутреннюю охрану. Охрана периметра направлена на предотвращение несанкционированного проникновения на территорию объекта, в то время как внутренняя охрана направлена на контроль ситуации внутри периметра объекта. Внутренняя охрана действует как резервная защита периметра в случае успешного проникновения и направлена на пресечение противоправных действий со стороны персонала КВЭИ.

Таблица 6

Меры физической защиты от террористических атак на КВЭИ

Меры	Оборудование	Примечания
Охрана периметра		
Ограждение периметра зоны КВЭИ	Заборы, стены	Зона КВЭИ должна быть четко обозначена для недопущения несанкционированного проникновения.
Инженерная защита	Укрепленные сооружения, взрывозащитные стены, колючая проволока	Конструкция периметра КВЭИ должна исключать возможность несанкционированного проникновения на территорию объекта.
Наблюдение	Камеры видеонаблюдения, датчики проникновения, охранное освещение, тепловые датчики, лазерное ограждение	Используемое оборудование должно обеспечивать круглосуточное обнаружение несанкционированного проникновения с немедленным уведомлением центрального поста охраны КВЭИ и подразделения полиции/национальной гвардии, отвечающего за резервную защиту КВЭИ.

Меры	Оборудование	Примечания
Контроль на входе	Пост охраны, оборудованный системой видеонаблюдения, шлагбаумами, системой контроля доступа, рентгеновскими сканерами, ручными металлоискателями, системами обнаружения следов взрывчатых веществ, собаками для обнаружения взрывчатых веществ и т.д.	КПП должен обеспечивать безопасный проход персонала и проезд транспортных средств.

Меры	Оборудование	Примечания
Внутренняя охрана		
Патрулирование внутри периметра	Вооруженная пешая охрана или морской патруль (в случае охраны морской инфраструктуры)[116]	Физическое присутствие патрулирующих охранников в пределах периметра позволяет быстро прибыть на место происшествия.
Наблюдение	Камеры видеонаблюдения, охранное освещение, БАС, объемные детекторы и т.д.	Оборудование для внутренней охраны должно охватывать все зоны и помещения объекта КВЭИ. БАС могут дублировать камеры видеонаблюдения на случай их преднамеренного или случайного выхода из строя.
Связь	Средства стационарной, мобильной и радиосвязи, кнопки тревоги	Все сотрудники службы безопасности должны быть обеспечены как минимум двумя средствами связи. Используемые средства связи должны дублировать друг друга на случай, если одно из них будет подавлено.

В случае изменения уровня безопасности и оценки рисков необходимо обновить меры безопасности. Например, при прокладывании новых дорог, ведущих к объекту КВЭИ, их необходимо будет оборудовать противотаранными устройствами (барьерами) для противодействия потенциальным террористическим атакам с использованием транспортных средств.

Более того, государства-члены все чаще внедряют так называемые подходы «конструктивной безопасности» (security-by-design) в качестве инструмента обеспечения физической безопасности на этапах проектирования и строительства (реконструкции) зданий, в которых размещаются важнейшие объекты энергетики.

[116] Например, в Индии физическая безопасность морской нефтегазовой инфраструктуры обеспечивается посредством постоянного патрулирования одним вооруженным патрулем «Судов немедленной поддержки», укомплектованным военнослужащими.

Новые технологии также помогают решать серьезные проблемы, связанные с нефте- и газопроводами. Например, распределенные акустические датчики (РАД), которые используют оптоволоконные кабели для обнаружения сейсмоакустических колебаний грунта на расстоянии нескольких десятков километров вдоль кабеля.[117]

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 13

Меры обеспечения физической безопасности на проекте Восточноафриканского нефтепровода (EACOP) в Уганде

Нефтяное управление Уганды (PAU) в консультации с соответствующими государственными службами безопасности выявило основные угрозы безопасности строящегося в настоящее время проекта Восточноафриканского нефтепровода.[118] К таким угрозам относятся диверсии и террористические акты, а также другие ситуации чрезвычайного характера. Поэтому для решения этих проблем была разработана стратегия безопасности. Для контроля за проникновением по всей длине трубопровода протяженностью 1443 км будет использоваться оптоволоконный кабель. Кроме того, на энергетических объектах EACOP в Уганде будут реализованы и другие меры, такие как:

- Развертывание кинологической группы и отряда по разминированию.
- Размещение сотрудников службы безопасности для контроля доступа и установка трех арочных металлоискателей для проверки лиц, имеющих доступ на территорию.
- Развертывание пожарной машины и пожарной бригады.
- Привлечение более 50 сотрудников службы безопасности, в том числе для обеспечения круглосуточного дежурства.
- Привлечение не менее 10 сотрудников для регулирования движения транспортных средств на объектах.
- Ограждение периметра мест проведения мероприятий с помощью предупреждающих лент.

Источник: Отчет о воздействии проекта строительства Восточноафриканского нефтепровода на окружающую среду и социальную сферу, Уганда, 2019 г., доступ по ссылке: https://www.eia.nl/projectdocumenten/00009498.pdf.

4.3.6.2. Меры в отношении БАС

Защита объектов энергетики от атак БАС представляет собой сложную задачу из-за сложности контроля воздушного пространства вокруг этих объектов. Частое соседство энергетической инфраструктуры с транспортными коридорами еще больше усложняет эту проблему, поскольку позволяет террористам развертывать БАС с относительно близкого расстояния.

[117] Например, Houjia X, Yuantao L., Taotao Z., Fengyi L, et al, *An overview of the oil and gas pipeline safety in China*, Journal of Industrial Safety, 2024, доступ по ссылке: https://www.sciencedirect.com/science/article/pii/S2950276424000035. Также доступ по ссылке: https://en.t8-sensor.ru/pipelines.

[118] Проект Восточноафриканского нефтепровода, доступ по ссылке: https://eacop.com/overview.

В большинстве случаев стандартная процедура противодействия атакам БАС в отношении КВЭИ включает следующие шаги:

- Мониторинг воздушного пространства над охраняемым объектом и прилегающей к нему территории.
- Информирование операторов об обнаруженных целях.
- Использование инструментов для обнаружения БАС в случае подозрительной активности.
- Определение типа БАС и его отличие от ложных целей, таких как птицы.
- Выдача целеуказания средствам нейтрализации потенциальной угрозы.
- Нейтрализация потенциальной угрозы.

Совокупность этих факторов обусловливает необходимость внедрения комплексной системы наблюдения за окружающим воздушным и наземным пространством. Для обеспечения эффективного круглосуточного и всепогодного контроля наиболее надежным методом наблюдения является сочетание радиолокационных и радиотехнических средств, дополненных оптическими методами наблюдения. Радиолокационные датчики необходимы для точного определения местоположения наблюдаемого объекта и определения целеуказания для сдерживания или нейтрализации угрозы. Возможны различные варианты размещения радиолокационных датчиков в зависимости от конфигурации охраняемого объекта и требуемой зоны обзора.

Частный сектор все чаще разрабатывает БАС, специально предназначенные для мониторинга нефтяных и газовых трубопроводов. Например, некоторые из этих БАС сочетают в себе преимущества конструкции самолета и вертолета (гибридная аэродинамика), включают воздушный мониторинг (например, с помощью удаленного лазерного сканера и видеокамеры высокого разрешения, установленной на БАС), а также обрабатывают данные с помощью самообучающихся систем.

Вставка 7

Методы обнаружения атаки БАС на энергетическую инфраструктуру

Основными и наиболее эффективными методами обнаружения БАС являются:

- Радиолокационное обнаружение, при котором радар определяет координаты, параметры движения и характеристики БАС путем анализа излучаемых и отраженных радиоволн.
- Системы радиообнаружения сканируют сигналы БАС и могут использоваться для определения их местоположения и траектории.
- Оптическое обнаружение с использованием высокотехнологичных оптоэлектронных датчиков.
- Акустическое обнаружение, позволяющее обнаруживать БПЛА с помощью сверхчувствительных шумовых микрофонов.

4.3.6.3. Меры по обеспечению безопасности энергетической инфраструктуры

Меры по обеспечению информационной безопасности энергетической инфраструктуры должны включать в себя:

Аппаратные и программные средства защиты:

- К ним относятся брандмауэры, антивирусные программы, системы обнаружения/предотвращения вторжений (IDS/IPS) и другие инструменты безопасности для защиты от несанкционированного доступа и основанных на ИКТ угроз.

Политика информационной безопасности означает:

- Установление и обеспечение соблюдения правил и прав доступа к ресурсам и базам данных, как правило, на основе принципа служебной необходимости. Это подразумевает управление доступа на основе ролей (RBAC) и регулярный аудит для обеспечения соответствия.

Разделение информационных систем:

- Этот процесс также известен как сегментация сети и подразумевает разделение сети на более мелкие изолированные сегменты, чтобы предотвратить влияние сбоя или нарушения безопасности в одном сегменте на всю систему.

Анализ инцидентов информационной безопасности и обмен информацией:

- Регулярный анализ инцидентов, связанных с ИКТ, для понимания и устранения уязвимостей. Обмен информацией об угрозах и уязвимостях с другими субъектами (например, другими энергетическими компаниями, государственными учреждениями и организациями по информационной безопасности) имеет решающее значение для обеспечения коллективной защиты.

Внедрение системы анонимных сообщений:

- Применение системы анонимных сообщений может помочь выявить внутренние угрозы со стороны сотрудников или инсайдеров, которые могут иметь злой умысел.

Проверка цифровой подписи и комплексная аутентификация:

- Для предотвращения несанкционированных действий решающее значение имеет обеспечение подлинности и целостности команд и сообщений с помощью цифровых подписей и надежных методов аутентификации (например, многофакторной аутентификации).

Регулярное обучение по вопросам безопасности:

- Обучение сотрудников основам информационной безопасности, позволяющее распознавать потенциальные угрозы и реагировать на них.

Регулярные обновления и исправления:

- Обеспечение регулярного обновления и внесение исправлений в оборудование и программное обеспечение для защиты от выявленных уязвимостей.

План реагирования на инциденты:

- Разработка и поддержка комплексного плана реагирования на инциденты для быстрого и эффективного реагирования на нарушения безопасности.

Физическая безопасность:

- Хотя основное внимание уделяется информационной безопасности, меры физической безопасности также имеют ключевое значение для защиты инфраструктуры от физических атак, которые могут поставить под угрозу информационную безопасность.

Еще одной эффективной организационной мерой является обязанность операторов КВЭИ оперативно информировать органы власти о каждом инциденте информационной безопасности. Во многих государствах-членах ЕС действуют оперативные центры по реагированию на инциденты информационной безопасности. Однако, учитывая уязвимость энергетического сектора к террористическим атакам с использованием ИКТ, некоторые страны создали специализированные центры и группы реагирования на инциденты компьютерной безопасности специально для операторов КВЭИ. Например, в Австралии с 2021 года операторы электросетей обязаны сообщать о каждом инциденте информационной безопасности на своих объектах, включая программы-вымогатели, фишинг и другие подобные угрозы.[119] Другой пример был представлен правительством Индонезии в 2022 году, когда оно создало базу данных инцидентов компьютерной безопасности для сбора информации об инцидентах, связанных с ИКТ, в секторах КВИ, включая энергетику.[120]

Некоторые государства-члены создали интегрированные системы безопасности данных для КВЭИ. Например, согласно Национальной политике Бразилии по защите критически важной инфраструктуры, Система данных о безопасности критически важной инфраструктуры содержит цифровые записи о состоянии безопасности критически важной инфраструктуры, включая энергетические объекты по всей территории страны. Эта система охватывает сбор, обработку, хранение и поиск информации.[121]

Инструмент 6

Лаборатория моделирования ИКТ-рисков на критически важных объектах нефтегазового комплекса (РГУ нефти и газа (НИУ) имени И.М. Губкина)

Лаборатория развернута на базе программно-аппаратного комплекса «AMPIRE» и использует «цифрового двойника» типичных информационных процессов в нефтегазовой компании для моделирования различных видов ИКТ-атак. Такие атаки могут осуществляться персоналом компании во время специализированных учебных занятий, при этом некоторые ИТ-специалисты выступают в роли «атакующих», а другие — в роли «защитников».

В ходе выполнения практических занятий в лаборатории обучающиеся получают следующие основные навыки:

- мониторинг и обнаружение компьютерных атак, направленных на элементы информационных систем нефтегазового предприятия;
- работа со специальным программным обеспечением для обнаружения и анализа событий информационной безопасности, включая вредоносные действия ИКТ;

[119] Доступ по ссылке: https://www.abc.net.au/news/2021-10-13/government-will-mandate-business-reporting-ransomware-attacks/100534890.
[120] Доступ по ссылке: https://www.thejakartapost.com/paper/2023/08/09/cybersecurity-strategy-for-indonesias-critical-infrastructure-protection.html.
[121] Política Nacional de Segurança de Infraestruturas Críticas, DECRETO Nº 9.573, DE 22 DE NOVEMBRO DE 2018, доступ по ссылке: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm.

- проведение расследований по локализации объектов атаки и внесение изменений в элементы информационной системы виртуального предприятия для нейтрализации выявленных угроз.

Лаборатория используется РГУ нефти и газа (НИУ) имени И.М. Губкина для подготовки как обучающихся по очной форме обучения, так и сотрудников предприятий, проходящих обучение в рамках программ дополнительного профессионального образования.

Источник: https://en.gubkin.ru/news/university-life/the-training-laboratory-to-study-computer-attack-detention-was-established-at-gubkin-university/.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 14

Рекомендации Комиссии ЕС 2019/553 по кибербезопасности в энергетическом секторе

Согласно Рекомендациям Комиссии ЕС 2019/553 операторы энергетических сетей должны:

a. Анализировать риски, связанные с объединением традиционных концепций и концепций Интернета вещей, а также учитывать внутренние и внешние интерфейсы и их уязвимости.
b. Принимать соответствующие меры против вредоносных атак, исходящих от большого количества злонамеренно контролируемых потребительских устройств или приложений.
c. Создать автоматизированную возможность мониторинга и анализа событий, связанных с безопасностью, в традиционных средах и средах Интернета вещей, таких как неудачные попытки входа в систему, срабатывание сигнализации об открытии шкафа или другие события.
d. Регулярно проводить специальный анализ рисков информационной безопасности для всех устаревших установок, особенно при соединении старых и новых технологий; поскольку устаревшие установки часто представляют собой очень большое количество активов, анализ рисков может проводиться по классам активов.
e. По возможности обновлять программное обеспечение и оборудование устаревших систем и систем Интернета вещей до последней версии. При этом операторам энергетических сетей следует рассмотреть дополнительные меры, такие как разделение системы или добавление внешних барьеров безопасности там, где исправление или обновление было бы достаточным, но невозможным, например, для неподдерживаемых продуктов.
f. Составлять тендеры с учетом требований информационной безопасности, то есть требовать предоставления информации о функциях безопасности, соблюдения существующих стандартов информационной безопасности, обеспечения постоянного оповещения, исправления и предложений по смягчению последствий в случае обнаружения уязвимостей, а также разъяснять ответственность поставщика в случае компьютерных атак с использованием ИКТ.
g. Взаимодействовать с поставщиками технологий для замены устаревших систем, когда это выгодно по соображениям безопасности, но при этом учитывать критически важные функциональные возможности системы.

Источник: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019H0553.

4.3.6.4. Меры по снижению взаимосвязанности

Как отмечалось ранее в Руководстве, развитие международных и региональных энергетических систем неизбежно создает взаимозависимости, которые приводят к появлению дополнительной уязвимости в энергетической инфраструктуре. Для минимизации этих взаимосвязанных уязвимостей можно рассмотреть следующие меры:

- Повышение осведомленности о взаимозависимостях: Содействие сотрудничеству внутри различных секторов и между ними, например, посредством проведения семинаров и межсекторальных встреч, на которых рассматриваются общие проблемы в различных отраслях.[122]
- Интеграция взаимозависимостей в структуры управления рисками: Включение концепции взаимозависимостей или каскадных эффектов в структуры управления рисками, например, в сценарии угроз. Такой подход способствует более тесному сотрудничеству между субъектами.
- Исключение зависимости от одного источника: Обеспечение наличия альтернатив и диверсификации для снижения зависимости от одного источника.
- Содействие проведению межсекторальных учений: Проведение межсекторальных учений для проверки эффективности возможностей реагирования на инциденты.

Кроме того, защита энергетической инфраструктуры должна рассматривать зависимости не как статичные отношения, а как динамические и быстро меняющиеся. Повышение осведомленности о взаимозависимости посредством межсекторального взаимодействия, например, обсуждения сценариев риска, может стимулировать дальнейшее сотрудничество между различными субъектами.

4.3.6.5. Планы по снижению последствий и реагированию на чрезвычайные ситуации

Меры по снижению последствий и реагированию на чрезвычайные ситуации являются важнейшими компонентами защиты энергетической инфраструктуры от терроризма и должны соответствовать международным обязательствам, включая международное право в области прав человека и международное гуманитарное право.

Комплексные планы реагирования на чрезвычайные ситуации имеют решающее значение и должны подробно описывать процедуры реагирования на инциденты, связанные с энергетической инфраструктурой. Во многих государствах-членах операторы критически важной энергетической инфраструктуры обязаны предвидеть, предотвращать и минимизировать потенциально опасные условия, связанные с их объектами. В планах действий в чрезвычайных ситуациях должны быть изложены действия по аварийному ремонту и восстановлению, установлены приоритеты, распределены обязанности, определены ресурсы и предусмотрены вопросы координации и связи в случае чрезвычайных ситуаций.

Как уже упоминалось в разделе 4.3.2, операторы КВЭИ должны использовать процессы оценки угроз и рисков для выявления потенциальных инцидентов, требующих экстренного реагирования. План

[122] Например, в ходе конференции «Российская энергетическая неделя» участники от секторов добычи ископаемого топлива и возобновляемой энергетики имеют возможность вместе обсудить общие вопросы. См. https://rusenergyweek.com/en/about/about-rew/.

действий в чрезвычайных ситуациях должен включать цепочку команд для реагирования на чрезвычайные ситуации, метод классификации инцидентов и общее описание системы управления инцидентами. Например, в Канаде операторы обязаны предоставлять сведения о мониторинге объектов энергетики в режиме реального времени, описывать учения и тренировки для проведения испытаний, а также излагать меры по информированию спасателей, медицинских учреждений, организаций и пользователей о местоположении объектов, потенциальных чрезвычайных ситуациях и процедурах безопасности.

Планы действий в чрезвычайных ситуациях также должны включать в себя списки персонала для оказания экстренной помощи, включая порядок дежурства и протоколы быстрой мобилизации. Кроме того, эти планы должны быть адаптированы к местным и географическим условиям, с учетом таких факторов, как специфика соседних территорий и транспортная доступность объекта. Они также должны включать инструменты и механизмы экстренной связи с зависящими от них учреждениями и секторами. Назначенный координатор, ответственный за реализацию и координацию пересмотра плана действий в чрезвычайных ситуациях, должен пройти предварительное обучение и быть готов к выполнению данных функций.

Активное партнерство между частным сектором и правоохранительными органами имеет решающее значение для эффективного реагирования на атаки. Например, в Казахстане руководители служб безопасности обязаны разработать алгоритмы первичного реагирования в целях:

немедленного информирования правоохранительных органов и органов национальной безопасности о террористических угрозах.

Своевременного сообщения о случаях кражи или незаконного приобретения оружия или оборудования, которые могут быть использованы для создания самодельных взрывных устройств.

Планы действий в чрезвычайных ситуациях должны быть интегрированы с планами, разработанными соответствующими национальными органами, чтобы избежать дублирования усилий и гарантировать выполнение всех требований. Их следует обновлять в соответствии с процедурами обзора управления рисками и оценки уязвимости. Проведение учений по реагированию на чрезвычайные ситуации и учений по управлению кризисными ситуациями с участием как операторов объектов, так и правоохранительных органов дает возможность апробирования процедур, выявления пробелов в координации, уточнения задач и обновления планов и протоколов управления кризисными ситуациями.

Системы раннего оповещения являются неотъемлемой частью планов реагирования на чрезвычайные ситуации и предназначены для оперативного информирования персонала и, при необходимости, местных сообществ. Например, в Кувейте нефтяная компания использует электронные сирены с двумя каналами связи (основным и резервным) на тридцати газовых скважинах. Данная мера по минимизации риска направлена на повышение защиты персонала и обеспечение своевременного оповещения в случае возникновения чрезвычайных ситуаций.[123]

[123] Доступ по ссылке: https://www.electronic-sirens.com/success-story-early-warning-system-kuwait-oil-company/.

Регулярные учебные занятия и учения по реагированию на чрезвычайные ситуации, проводимые совместно с местными сообществами, имеют важное значение для подготовки персонала к быстрому и эффективному реагированию на чрезвычайные ситуации. Эти учебные занятия также дают возможность обсудить волнующие общественность вопросы и обеспечить информированность жителей о порядке реагирования на чрезвычайные ситуации.[124]

В ответ на чрезвычайные ситуации, включая потенциальные террористические атаки, большинство нефтегазовых компаний создают оперативные центры для координации мер реагирования и минимизации последствий инцидентов. Например, многие компании предусматривают специальные центры реагирования, которые взаимодействуют с центральным диспетчерским центром компании. Такой централизованный подход обеспечивает комплексную координацию всех мер реагирования и обеспечивает полный контроль над аварийными операциями до тех пор, пока не будут завершены все восстановительные мероприятия, такие как рекультивация окружающей среды. Кроме того, уведомление направляется в соответствующие службы реагирования на чрезвычайные ситуации, а также региональные или местные органы власти, которые, при необходимости, выстраивают взаимодействие в вопросах эвакуации близлежащих населенных пунктов.

4.3.6.6. Меры по минимизации воздействия на окружающую среду

Планы восстановления энергетической инфраструктуры должны включать меры по минимизации воздействия на окружающую среду. Например, операторы трубопроводов обычно разрабатывают планы реагирования на разливы, чтобы свести к минимуму ущерб окружающей среде в случае утечки из трубопровода в результате атаки.

- Ярким примером является крупная российская нефтегазовая компания, которая проводит регулярные учения по реагированию на чрезвычайные ситуации (не реже одного раза в год) на нефтяных скважинах в Карском море, где окружающая среда особенно уязвима к потенциальным разливам нефти.[125] Такие комплексные учения включают в себя ликвидацию разливов нефти, тушение пеной и эвакуацию персонала.

[124] Например, https://dag-aif-ru.turbopages.org/turbo/dag.aif.ru/s/society/v_dagestane_na_neftegazovom_obekte_proshli_antiterroristicheskie_ucheniya.
[125] Например, https://www.gazprom.ru/about/subsidiaries/news/2021/october/article540502/.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 15

План протокола безопасности трубопроводов и восстановления после аварий в США

Целью Плана протоколов по обеспечению безопасности трубопроводов и восстановлению после инцидентов является разработка комплексного межведомственного подхода к противодействию рискам и минимизации последствий чрезвычайных ситуаций, связанных с инфраструктурой трубопроводов, с особым упором на действия, которые федеральное правительство США может предпринять для содействия защите, реагированию и восстановлению трубопроводов.

План представляет собой структуру и протоколы для поддержки восстановления инфраструктуры трубопровода, а также меры по предотвращению инцидентов безопасности и повышению устойчивости. Целью Плана является ликвидация последствий атаки, а также минимизация эксплуатационных последствий и сокращение времени, необходимого для восстановления после сбоя в инфраструктуре трубопроводной системы.

Источник: https://www.tsa.gov/sites/default/files/pipeline_sec_incident_recvr_protocol_plan.pdf.

4.3.6.7. Опыт планирования действий в чрезвычайных ситуациях

Во многих государствах-членах операторы КВЭИ по закону обязаны разрабатывать план действий в чрезвычайных ситуациях в рамках своей готовности к реагированию на ЧС. Эти планы обычно вступают в действие в случае инцидентов, связанных с травмами персонала, повреждением объектов или загрязнением окружающей среды. Путем классификации инцидента можно оповестить максимальное количество людей в кратчайшие сроки, что позволит им быстро принять соответствующие меры. Как правило, каждый тип инцидента требует индивидуального реагирования, включающего конкретные инструкции для соответствующих сотрудников, различные задачи и координацию с различными организационными службами.

Планы действий в чрезвычайных ситуациях содержат четкие инструкции для персонала и служб безопасности, подробно описывающие работу критически важных систем в период действия чрезвычайной ситуации, включая сценарии, связанные с террористической атакой на объект. В них также излагается порядок мобилизации персонала и оборудования для эффективного управления чрезвычайными ситуациями. Например, в Великобритании операторы объектов энергетики обязаны разрабатывать меры и планы действий на случай непредвиденных сбоев в поставках электроэнергии.[126] Таким образом, проведение испытаний является еще одним типичным требованием этих планов. Немецкое Федеральное сетевое агентство по электроэнергии, газу, телекоммуникациям, почте и железным дорогам (Bundesnetzagentur) регулярно проводит стресс-тесты национальной энергетической системы. Эти испытания направлены на подготовку к возможным перебоям в электроснабжении и обеспечение возможности принятия соответствующих мер в случае возникновения чрезвычайной ситуации.[127]

[126] UK's *Public summary of sector security and response plan*, 2018, доступ по ссылке: https://assets.publishing.service.gov.uk/media/5c8a7845ed915d5c1456006a/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf

[127] Доступ по ссылке: https://www.bmwk.de/Redaktion/EN/Pressemitteilungen/2022/09/20220905-power-system-stress-test.html.

План действий в чрезвычайных ситуациях нефтегазовой компании обычно охватывает широкий спектр сценариев, таких как травмы, требующие эвакуации и внешней медицинской помощи, отравление сероводородом (H2S) (как с индивидуальными, так и с массовыми жертвами), смертельные случаи, инциденты с падением персонала за борт и серьезные травмы в результате отказа оборудования. Кроме того, в этих планах часто указываются критерии классификации серьезности ущерба нефтегазовому объекту и оценки возможных экологических последствий в зависимости от типа разлива и характера сбрасываемых жидкостей.[128]

План предусматривает назначение контактного лица в компании для координации усилий по реагированию, подробно описывает пошаговые действия персонала, определяет преемственность руководства и обеспечивает четкие каналы связи для эффективного принятия решений на случай чрезвычайных ситуаций.

Обычно планы действий в чрезвычайных ситуациях для энергетической инфраструктуры включают:

- Правила и процедуры оповещения о чрезвычайных ситуациях: Подробные инструкции по оповещению соответствующих сторон в случае возникновения чрезвычайной ситуации.
- Непосредственные обязанности персонала: Четкое распределение задач и координационных обязанностей между сотрудниками.
- Работа систем охранной сигнализации: Процедуры активации и управления системами сигнализации для оповещения персонала и прибывших спасателей.
- Эксплуатация резервных систем: Инструкции по обеспечению правильной работы резервных систем для поддержания функционирования в чрезвычайной ситуации.
- Инструкции по эвакуации: Подробные планы безопасной эвакуации персонала с объекта.
- Меры по переходу на безопасный режим работы: Процедуры приведения объекта в стабильное и безопасное эксплуатационное состояние.
- Альтернативные аварийные объекты: Определение дополнительных мест или объектов, которые могут быть использованы в случае компрометации основного объекта.

[128] Например, https://www.energean.com/media/1061/eisa-annex-13-contingency-plan.pdf.

5. Международные усилия по защите КВЭИ

Ввиду большой протяженности инфраструктуры транспортировки энергоносителей сотрудничество между странами, по территориям которых проходит трансграничный КВЭИ, имеет решающее значение для эффективной защиты от террористических атак. На повышение уязвимости может сказаться разделение обязанностей по обеспечению безопасности между несколькими юрисдикциями. Поэтому страны должны работать сообща для оценки террористических угроз и разработки комплексных планов по их смягчению, соответствующих правам человека.

5.1. Трансграничная энергетическая инфраструктура

5.1.1. Трансграничный каскадный эффект

Глобализация энергетического сектора достигла продвинутой стадии, и сбои, вызванные террористическими атаками на хранилища или трубопроводы, могут иметь широкомасштабные последствия. Подобные сбои могут спровоцировать цепную реакцию с серьезными последствиями для энергетических секторов других стран, а также для общества и окружающей среды.

Ярким примером каскадного эффекта трансграничного характера, вызванного нарушением работы энергетической инфраструктуры, является отключение электроэнергии в энергосистеме Центральной Азии в январе 2022 года.[129] В результате крупной аварии на единой энергосистеме Средней Азии на юге Казахстана, в Узбекистане и Кыргызстане произошли масштабные отключения электроэнергии. Миллионы людей по всей Центральной Азии остались без электричества. Отключение электроэнергии привело к приостановке работы аэропортов и метрополитенов в Казахстане и Узбекистане. Крупнейшие операторы мобильной связи в Казахстане, Кыргызстане и Узбекистане сообщили о потерях связи, в то время как больницам пришлось полагаться на генераторы для поддержания работы основного оборудования.

Еще один случай нарушения работы трансграничной энергетической инфраструктуры произошел в июне 2024 года. Масштабное отключение электроэнергии привело к отключениям электроэнергии по всему Балканскому региону. Отключения электроэнергии начались в Черногории, а затем затронули Боснию и Герцеговину, некоторые районы Хорватии, включая Далмацию, и северную Албанию.[130]

Эти примеры, наряду с продолжающимся ростом целостности и взаимосвязанности энергетической инфраструктуры на глобальном уровне, подчеркивают важность дальнейшего развития международного сотрудничества в борьбе с терроризмом, включая гармонизацию законодательства и сотрудничества в правовой сфере.

[129] Доступ по ссылке: https://www.reuters.com/world/asia-pacific/power-blackout-hits-kazakhstan-kyrgyzstan-uzbekistan-2022-01-25/#:~:text=ALMATY%2C%20Jan%2025%20(Reuters)%20-,use%20to%20cover%20unexpected%20shortages.

[130] Доступ по ссылке: https://balkaninsight.com/2024/06/21/major-power-blackout-hits-albania-bosnia-croatia-montenegro/.

5.1.2. Необходимость трансграничного сотрудничества в защите КВЭИ

Транснациональный характер терроризма обусловливает необходимость усиления трансграничного сотрудничества в целях защиты КВЭИ. Для решения этих задач многие государства-члены разработали правовые и организационные основы, предусматривающие двусторонние и многосторонние соглашения, межправительственные комиссии и рабочие группы. Такое сотрудничество имеет жизненно важное значение для международных усилий, направленных на противодействие терроризму в отношении объектов энергетики.

Например, на фоне роста угроз морской энергетической инфраструктуре важное значение для защиты транспортных коридоров, используемых нефтяными и газовыми танкерами, приобретают совместные международные инициативы. К ним относится регулярный мониторинг, обмен информацией о возникающих угрозах и координация мер реагирования. Несмотря на эти усилия, операторы КВЭИ сталкиваются со значительными проблемами в защите нефтяных и СПГ танкеров, а также связанной с ними портовой инфраструктуры. В международных водах танкерам приходится проходить по протяженным и опасным маршрутам, где зачастую присутствует недостаточное количество кораблей охраны.

5.1.3. Примеры международных организаций, работающих в сфере защиты энергетической инфраструктуры от террористических атак

Важно отметить, что не существует специализированных международных организаций, занимающихся исключительно защитой нефтегазовой инфраструктуры от террористических атак. Как правило, такая деятельность подпадает под более широкие полномочия различных организаций. Например:

- Глобальная программа ООН по защите уязвимых целей от террористических угроз в рамках своего мандата, вытекающего из Глобальной контртеррористической стратегии, направлена на оказание поддержки государствам-членам в укреплении защиты КВИ, включая КВЭИ. Данная программа реализуется КТУ ООН совместно с ИДКТК, ЮНИКР, Альянсом цивилизаций ООН и в консультации с Интерполом. В число инициатив Программы входит наращивание потенциала государств-членов-бенефициаров; разработка информационных продуктов, таких как технические руководства, содержащие передовую международную практику; объединение экспертов стран мира через специализированную Глобальную сеть по защите уязвимых целей и оказание помощи государствам-членам в устранении возникающих угроз уязвимым целям.
- Международная конвенция по охране человеческой жизни на море (СОЛАС) 1974 года (с изменениями), в частности Глава XI-2, и Международный кодекс по охране судов и портовых средств (ИСПС), а также Конвенция о борьбе с незаконными актами, направленными против безопасности морского судоходства (включая Протоколы 1988 и 2005 годов) содержат всеобъемлющие требования по обеспечению безопасности для правительств, портовых властей и судоходных компаний. В этих правилах подробно описаны конкретные меры безопасности для

международного судоходства, портовых сооружений и стационарных платформ на континентальном шельфе, включая требования к оценкам и планам безопасности судов, оценкам и планам безопасности портовых сооружений, а также функции сотрудников службы безопасности. В результате национальные правительства и операторы терминалов предприняли такие шаги, как усиление физической безопасности на портовых сооружениях и проведение патрулирования в открытом море с соблюдением требований Кодекса ОСПС и улучшением мер безопасности, о которых сообщили операторы танкеров.

- Решающую роль в поддержке внедрения этих правил играет Международная морская организация (ИМО). Являясь специализированным учреждением ООН, ИМО оказывает государствам-членам помощь в разработке и совершенствовании их национального управления морской безопасностью в соответствии с СОЛАС и Кодексом ОСПС. Это включает в себя оказание технической помощи в создании национальных комитетов по безопасности на море, реестров рисков и стратегий безопасности. ИМО также занимается вопросами безопасности морской энергетической инфраструктуры и разрабатывает требования к реагированию на чрезвычайные ситуации для нефтяных и газовых танкеров в случае совершения террористических и других противоправных действий.[131]

5.1.4. Примеры регионального сотрудничества в сфере защиты энергетической инфраструктуры от террористических атак

В связи с необходимостью защиты трансграничной энергетической инфраструктуры региональные организации играют решающую роль в содействии сотрудничеству между соседними странами. Наглядным примером такого взаимодействия являются «Рекомендации по противодействию терроризму на объектах топливно-энергетического комплекса», подготовленные Организацией Договора о коллективной безопасности (ОДКБ) в декабре 2022 года (см. Приложение 2). [132] В этом документе предлагаются рамки, позволяющие государствам-членам усилить меры безопасности против террористических атак, направленных на КВЭИ. В Рекомендациях изложены меры по борьбе с терроризмом, включая системы физической защиты, такие как контроль доступа и персонал службы безопасности, а также надежные протоколы информационной безопасности для защиты инфраструктуры от атак, связанных с ИКТ. Кроме того, в документе подчеркивается важность обучения персонала процедурам безопасности и проведения кампаний по повышению осведомленности общественности для повышения бдительности в отношении потенциальных угроз.

Другим ярким примером является Трансасеанский газопровод, который повышает связуемость газовой и СПГ систем стран Ассоциации государств Юго-Восточной Азии (АСЕАН) за счет трубопроводов и регазификационных терминалов. В 2021 году АСЕАН подписала и приняла Меморандум о взаимопонимании по проекту Трансасеанского газопровода, который включает положения о реализации «соответствующих мер по обеспечению безопасности и сохранности трубопроводов».[133]

---

131 Доступ по ссылке: https://www.imo.org/en/OurWork/Security/Pages/FAQ.aspx#Should_IMO_should_be_worried_about_the

132 См. стр. 36-46: https://paodkb.org/uploads/publication/file/45/sbornik_5_december_2022.pdf.

133 Меморандум о взаимопонимании по проекту Трансасеанского газопровода, 2021, доступ по ссылке: https://asean.org/wp-content/uploads/2021/08/ASEAN-MoU-on-the-Trans-ASEAN-Gas-Pipeline.pdf-

Учитывая, что перебои в подаче электроэнергии на КВЭИ могут поставить под угрозу доступность энергоснабжения, угрожать региональной стабильности и повлиять на мировые цены на энергоносители, важную роль в трансграничной защите КВЭИ играют региональные организации в сфере безопасности. Такие организации, как Региональная антитеррористическая структура Шанхайской организации сотрудничества, Антитеррористический центр СНГ, АСЕАН и Организация по безопасности и сотрудничеству в Европе (ОБСЕ), разработали широкий спектр программ, курсов и учений для скоординированного на международном уровне предотвращения и управления кризисами.

Например, за последнее десятилетие ОБСЕ организовала множество мероприятий, направленных на защиту энергетической инфраструктуры от террористических атак. В 2020 году ОБСЕ создала Виртуальный центр по защите критической энергетической инфраструктуры. Эта платформа обеспечивает сотрудничество лиц, принимающих решения в сфере энергетики, предлагая технические знания, устанавливая нормы и стандарты, а также содействуя политическому взаимодействию с тем, чтобы КВЭИ содействовала устойчивому развитию.[134]

Еще одним ярким примером региональной межгосударственной координации в сфере защиты КВЭИ являются Методические рекомендации Антитеррористического центра СНГ (2019 г.). Этот документ, который уже упоминался здесь, является примером совместных усилий по повышению безопасности КВЭИ.

Инструмент 7

Антитеррористический центр государств-участников СНГ (АТЦ СНГ), 2019. Методические рекомендации по организации взаимодействия между органами безопасности, специальными службами и правоохранительными органами государств-участников СНГ в обеспечении антитеррористической защиты критической энергетической инфраструктуры

Методические рекомендации содержат указания по подготовке и проведению как национальных, так и международных антитеррористических учений по защите объектов энергетической инфраструктуры. В документе изложены показатели, позволяющие отслеживать террористическую деятельность, направленную против энергетических и ядерных объектов. Помимо экономических и демографических показателей, он включает в себя комплексные количественные и качественные параметры, связанные с готовностью военных, правоохранительных и других специализированных ведомств к потенциальным атакам на межрегиональную энергетическую инфраструктуру. В частности, АТЦ СНГ поручено осуществлять мониторинг показателей, связанных с защитой субрегионального энергоснабжения, учитывая межрегиональную взаимозависимость в энергетическом секторе.

Источник: Материалы сбора руководящего состава органов безопасности и специальных служб государств-участников СНГ: Сборник материалов– М.: Издательство «Принт Торг», 2019. – 362 с.

[134] Ivo Walinga, *OSCE activities on Critical Energy Infrastructure Protection*, 2020, доступ по ссылке: https://www.energycharter.org/fileadmin/DocumentsMedia/Forums/2-3_-_Critical_Infrastructure_Mr_Walinga.pdf.

Инструмент 8

ОБСЕ Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства

В публикации представлены основы, который способствуют разработке и реализации соответствующих политик и институционального управления информационной безопасностью, связанной с КВЭИ, на основе совместного, комплексного (учитывающего все опасности) и основанного на рисках подхода, а также с упором на достижение готовности к реагированию на инциденты, общей устойчивости инфраструктуры и надежности энергоснабжения.

Целью руководства является оказание помощи странам в выявлении и противодействии террористическим угрозам с использованием ИКТ, освещение методологических вопросов, которые необходимо учитывать для защиты неядерных объектов КВЭИ, а также предложение рекомендаций по передовой практике для снижения потенциальных уязвимостей. Кроме того, в руководстве описаны меры, которые могут быть адаптированы, расширены и/или применены к другим угрозам и другим секторам. В публикации представлена мировая практика оценки рисков, физической безопасности, информационной безопасности, планирования действий в чрезвычайных ситуациях, государственно-частного партнерства, взаимодействия с общественностью и международного/трансграничного сотрудничества по защите неядерных объектов энергетики.

Источник: https://www.osce.org/files/f/documents/4/b/103500.pdf.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 16

Учения по безопасности в нефтегазовой сфере в рамках Азиатско-Тихоокеанского экономического сотрудничества (АТЭС)

После 10-й встречи министров энергетики АТЭС в Санкт-Петербурге (Россия) в июне 2012 года государства-члены поручили Азиатско-Тихоокеанскому центру энергетических исследований (APERC) проводить регулярные учения по безопасности в нефтегазовой отрасли (OGSE). Целью этих учений является укрепление регионального сотрудничества путем разработки комплексных мер реагирования, включая политику и институциональные рамки, для эффективного устранения перебоев в поставках нефти и газа и ущерба инфраструктуре.

Учения OGSE, стартовавшие в 2014 году, проводились в семи странах-участницах, и каждое из них включало уникальные, тщательно разработанные сценарии. Например, в ходе учений OGSE 2019 года в Чили был смоделирован взрыв на трубопроводе жидких продуктов Конкон-Майпу, приведший к серьезному сбою поставок нефтепродуктов, особенно затронувшему Сантьяго и его окрестности. Эти учения привели к положительным изменениям в процедурах оценки угроз и разработке планов реагирования на чрезвычайные ситуации для субъектов как государственного, так и частного секторов.

Последнее учение OGSE проводилось в Таиланде в сентябре 2023 года. Одним из сценариев предусматривался крупный пожар на нефтеперерабатывающем заводе в Таиланде, который потребовал скоординированных действий всех заинтересованных сторон для поддержания работоспособности энергозависимых секторов экономики.

Источник: https://aperc.or.jp/reports/ogsi.php.

5.2. Международная межведомственная координация и сотрудничество

Учитывая трансграничный характер энергетической инфраструктуры, международное сотрудничество имеет решающее значение для ее эффективной защиты от террористических угроз. Например, трубопровод, проходящий через несколько стран, регулируется разными режимами, что требует скоординированных усилий всех участвующих стран для обеспечения всеобъемлющей безопасности.

5.2.1. Факторы, обусловливающие необходимость международного сотрудничества в защите КВЭИ

Потенциальные сценарии, демонстрирующие необходимость интеграции международного сотрудничества в стратегии государств-членов в области КВИ, включают:

- Общая инфраструктура: когда в двух или более странах имеются объекты КВИ одного и того же типа, например, подводный газопровод Langeled между Норвегией и Великобританией или подводный газопровод Balticconnector между Финляндией и Эстонией.
- Зависимость от иностранных ресурсов: когда энергетическая инфраструктура одной страны зависит от продуктов, услуг или технологий, поставляемых другой страной, как это происходит с трубопроводом Баку-Тбилиси-Джейхан.
- Трансграничное воздействие: когда проблемы или сбои в энергетической инфраструктуре одной страны влияют на соседние страны, особенно те, которые имеют общую границу.

5.2.2. Формы и механизмы международного сотрудничества по защите энергетической инфраструктуры

Существующие формы и механизмы международного сотрудничества по защите КВЭИ значительно различаются. К распространенным формам межгосударственного сотрудничества, направленного на предотвращение, выявление и реагирование на террористические акты в отношении КВЭИ, относятся:

- Меры по обмену информацией и повышению осведомленности: Содействие обмену соответствующей информацией и повышение осведомленности о потенциальных угрозах.
- Сотрудничество в разведывательных операциях: Координация усилий по предупреждению, выявлению и пресечению террористической деятельности в энергетическом секторе.
- Совместные меры по борьбе с финансированием терроризма: Сотрудничество в целях предотвращения и пресечения финансирования, поставок и приобретения оружия и боеприпасов, используемых в террористических актах.
- Гармонизация законодательства: Согласование национальных законов о борьбе с терроризмом и обмен нормативной информацией и практикой, связанными с усилиями по борьбе с терроризмом.

- Обмен опытом: Обмен знаниями и опытом в области предотвращения, выявления и пресечения террористической деятельности в энергетическом секторе.
- Скоординированный обмен информацией о кризисных ситуациях: Совершенствование информирования и координации в случае возникновения кризисных ситуаций и экстренного реагирования на террористические атаки на трансграничную энергетическую инфраструктуру.
- Совместные программы обучения и образования: Разработка и участие в учебных программах, направленных на защиту КВЭИ.

Хотя эти формы международного сотрудничества не направлены исключительно на защиту объектов КВЭИ, они являются важнейшими компонентами мер государственного реагирования на террористические атаки на объекты энергетики.

Кроме того, государства-члены часто проводят совместное патрулирование в приграничных районах или морских районах вблизи нефтяных платформ и трубопроводов. Например, Азербайджан, Турция и Грузия координируют усилия по защите трубопровода Баку-Тбилиси-Джейхан. Аналогичным образом, Танзания и Замбия осуществляют двустороннее сотрудничество по повышению безопасности трубопровода от терроризма.[135]

Международное сотрудничество в законодательной сфере также имеет решающее значение для контртеррористической защиты КВЭИ. Гармонизация законодательства между странами может гарантировать, что связанные с терроризмом преступления будут рассматриваться единообразно и соответствовать международным стандартам борьбы с терроризмом. Такой подход помогает избежать ситуации, когда в определенных юрисдикциях та же атака на объект энергетики может не классифицироваться как акт терроризм.

Примером такой гармонизации является «Модельный закон о противодействии терроризму» Межпарламентской Ассамблеи СНГ. Целью данной инициативы является стандартизация законодательства в странах Содружества, в том числе касающихся безопасности энергетической инфраструктуры. Модельное законодательство предусматривает конкретные меры по защите объектов энергетики от террористических угроз, указанные в Модельном законе СНГ «О противодействии терроризму», в частности в статье 12.[136]

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 17

Комитет по защите нефтяной и критической инфраструктуры Совета сотрудничества стран Персидского залива (Бахрейн, Кувейт, Оман, Катар, Саудовская Аравия, Объединенные Арабские Эмираты)

Учитывая важность защиты национальных активов, в частности нефтяных месторождений, министры государств-членов Совета сотрудничества арабских государств Персидского залива (ССАГПЗ) создали Комитет по безопасности и защите объектов нефтедобычи и критической инфраструктуры, заседания которого проводятся ежегодно.

135 Доступ по ссылке: https://www.aa.com.tr/en/africa/zambia-tanzania-agree-to-enhance-security-on-jointly-owned-oil-pipeline/2941120.
136 Модельный закон СНГ «О противодействии терроризму», доступ по ссылке: https://www.cisatc.org/1289/9115/135/9126/9129/249.

Комитет координирует деятельность по борьбе с терроризмом по нескольким ключевым направлениям:

- Обучение и повышение квалификации: Разработка и проведение специализированных программ обучения для сотрудников служб безопасности с упором на защиту жизненно важной нефтяной инфраструктуры в контексте современных проблем безопасности.
- Образовательные ресурсы: Подготовка образовательных материалов и создание учебных заведений в государствах-членах ССАГПЗ.
- Обмен информацией: Содействие обмену научными и экспертными знаниями, связанными с защитой КВЭИ от противоправных действий.

В соответствии с целями комитета образовательные и учебные заведения в сфере национальной безопасности в государствах-членах ССАГПЗ проводят ежегодные групповые выездные экскурсии для сотрудников и студентов.

Источник: https://www.gcc-sg.org/en-us/CooperationAndAchievements/Achievements/SecurityCooperation/Achievements/Pages/Twelfteducationandsecuritytra.aspx.

5.3. Совместные учения и тренировки

Трансграничный характер террористических угроз требует широкого международного сотрудничества. Это предусматривает не только проведение совместных операций и патрулирования, но и обмен знаниями, накопленным опытом и программ обучения для сотрудников служб безопасности. Более того, международное сотрудничество выходит за рамки государственных органов и охватывает взаимное обучение неправительственных субъектов и представителей гражданского общества.

5.3.1. Международные учебные курсы

Для повышения способности агентств обеспечивать безопасность важнейших объектов энергетики важное значение имеют международные учебные курсы. Эти программы способствуют трансграничной передаче знаний, передаче агентствам экспертных знаний, необходимых для противодействия меняющимся угрозам и обеспечения глобальной энергетической безопасности. Обеспечивая обмен передовым опытом и передовыми технологиями, такие программы укрепляют энергетическую безопасность и снижают уязвимость. Они играют решающую роль в укреплении как национальных, так и международных возможностей энергетической безопасности, выступая в качестве составных элементов глобальной системы защиты КВЭИ от террористических угроз. Эти курсы подчеркивают коллективную ответственность стран за обмен знаниями и опытом во имя более безопасного энергетического будущего.[137]

[137] Ярким примером тому является курс «Физическая безопасность критической энергетической инфраструктуры» и экспертный семинар, организованный в 2024 году Флорентийской школой регулирования. Целью данного мероприятия была оценка текущих проблем в области физической защиты критически важной энергетической инфраструктуры и изучение стратегий по повышению такой защиты. Доступ по ссылке: https://fsr.eui.eu/event/the-physical-security-of-critical-energy-infrastructure/.

5.3.2. Совместные антитеррористические учения

Совместные антитеррористические учения имеют решающее значение для обмена практическим опытом и содействия прямому сотрудничеству между субъектами обеспечения безопасности КВЭИ. Такие учения помогают отработать совместные шаги реагирования на чрезвычайные ситуации и решить проблемы трансграничной координации. Как правило, совместные учения на объектах КВЭИ носят тактический характер и включают в себя моделирование противоправных действий, направленных против объектов энергетики, которые являются трансграничными или расположены вблизи государственных границ.

Подобные межгосударственные антитеррористические учения дают ряд преимуществ:

- Объективная оценка: они позволяют провести объективную оценку состояния антитеррористической безопасности на ключевых национальных объектах КВЭИ.
- Разработка механизмов: они помогают разрабатывать и совершенствовать механизмы координации действий спецподразделений и служб безопасности при проведении операций по реагированию на террористические угрозы.
- Повышение квалификации: они способствуют совершенствованию использования коллективных межгосударственных информационно-коммуникационных систем.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 18

Совместные антитеррористические учения АТЦ СНГ

В 2021 году были проведены совместные антитеррористические учения «Каспий-Антитеррор» с целью выявления признаков террористической активности и пресечения атак на объекты морской инфраструктуры и нефтегазовой отрасли. Эти учения проводились одновременно в восьми странах Содружества: Армения, Беларусь, Казахстан, Кыргызстан, Молдова, Россия, Таджикистан и Узбекистан.

В 2019 году в ходе учений «Арарат-Антитеррор» отрабатывались задачи на атомной электростанции с участием семи стран СНГ. Аналогичным образом, в 2016 году учения «Информационная безопасность-Антитеррор», в которых приняли участие девять стран Содружества, были сосредоточены на тепловой электростанции в учебных целях.

Эти учения подчеркнули важность сотрудничества между национальными властями и правоохранительными органами. Организованные АТЦ СНГ мероприятия позволили:

- Улучшить взаимодействие в выявлении и пресечении террористических актов на критически важных объектах энергетики
- Закрепить навыки использования информационных систем коллективного пользования органов безопасности стран СНГ
- Повысить уровень сотрудничества между оперативными подразделениями органов безопасности

Источник: https://eng.cisatc.org/1289/133/161/9077.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 19

Международные совместные учения «ADMM-Plus Maritime Security Field Training Exercise»

В совместных учениях 2019 года, организованных Сингапуром и Республикой Корея, участвовали силы безопасности из 18 стран, которые работали сообща над устранением угрозы террористического нападения со стороны моря на нефтяную вышку недалеко от Пусана. В сценарий было заложено условное нападение на катерах преступной группы на объект энергетики, в качестве которого выступало судно ROKS Cheonjabong, использованное вместо нефтяной вышки.

В ходе учений военно-морские силы провели различные учения по обеспечению безопасности на море, включая абордажные операции и защиту ключевых объектов. Были отработаны действия по Кодексу незапланированных столкновений в море (CUES, 2014) и обмен информацией для отслеживания представляющих интерес судов. Учения также включали в себя посадку вертолетов на палубу и пополнение запасов в море, что способствовало укреплению доверия и практического взаимодействия между участниками.

Достигнув вод восточного Сингапура, досмотровые группы военно-морских сил Брунея, Индии, Республики Корея и Сингапура имитировали досмотр подозрительного судна. Затем для установления контроля, перехвата судов противника, окружения ключевого объекта и спасения вынужденно оказавшейся в воде команды нефтяной вышки были задействованы корабли ADMM-Plus.

Источник: https://www.mindef.gov.sg/web/wcm/connect/mindef/14d67a7b-f7a4-473c-958b-0ae2093590a0/Infographic.pdf?MOD=AJPERES&CVID=mGI0R7G.

АНАЛИЗ ПРАКТИЧЕСКОГО ПРИМЕРА 20

Компьютерные командно-штабные учения «Eternity-2023»

В прошедших в Баку международных учениях «Eternity-2023» приняли участие сотрудники правоохранительных органов Азербайджана, Грузии и Турции. Основной целью было укрепление взаимного сотрудничества и обеспечение взаимодействия в противодействии террористическим угрозам стратегически важным объектам, включая КВЭИ трубопровода Баку-Тбилиси-Джейхан. Сценарием учений была предусмотрена организация обеспечения защиты нефтепровода БТД в условиях кризиса. Трехсторонние учения Азербайджана, Грузии и Турции проводятся в данных странах ежегодно в порядке очередности.

Источник: https://mod.gov.az/en/news/eternity-2023-computer-assisted-command-and-staff-exercises-held-in-baku-ended-video-49709.html.

5.4. Сетевое взаимодействие и обмен информацией в контексте защиты КВЭИ

5.4.1. Типы информации, которой можно обмениваться на межгосударственном уровне

Для эффективной безопасности КВЭИ решающее значение имеет расширение международного сотрудничества, обмена знаниями и информацией по такой инфраструктуре. Обмен информацией, связанной с защитой энергетической инфраструктуры, может осуществляться в связи с инцидентами и не без связи с инцидентами. Первый вариант подразумевает срочный и своевременный обмен информацией во время инцидентов, а второй касается стратегических аналитических данных.

Поскольку обеспечение безопасности КВЭИ часто координируется государственными органами, обмен информацией обычно происходит между правоохранительными органами, министерствами юстиции и ведомствами, а также специализированными организациями по безопасности. Однако обмен информацией должен быть также налажен между отечественными операторами энергетической инфраструктуры и субъектами из разных стран.

Типы информации, которой можно обмениваться на межгосударственном уровне для совершенствования контртеррористической деятельности и повышения контртеррористической защиты, включают:

- Передовой опыт по предотвращению и реагированию на террористические угрозы на различных типах объектов энергетики, в том числе методы и тактика проведения контртеррористических операций и планы реагирования для оказания немедленной поддержки жертвам.
- Правовая информация, включая электронные доказательства для расследования террористических атак на КВЭИ, с учетом гарантий справедливого судебного разбирательства и прав человека.
- Информация, связанная с финансированием террористических группировок.
- Различные виды оперативной информации.

Хотя этот список не является исчерпывающим, эти категории представляют собой ключевые области для обмена информацией в целях усиления мер по борьбе с терроризмом и защиты от терроризма.

5.4.2. Обмен оперативной информацией в целях предотвращения и пресечения терроризма на критически важных объектах энергетики

Международный обмен оперативной информацией направлен на повышение ситуационной осведомленности относительно значимых событий или деятельности международных террористических группировок. В части защиты КВЭИ обмен оперативной информацией может включать информацию о:

- Передвижение и деятельность транснациональных террористических группировок, причастных к нападениям на объекты энергетики.
- Лица и группы, подозреваемые в участии в террористической деятельности.
- Выявлены закономерности и методы как осуществленных, так и планируемых террористических атак на объекты энергетической инфраструктуры.
- Любая другая информация, представляющая взаимный интерес.

Расширение возможностей контртеррористической разведки, в том числе в энергетическом секторе, посредством обмена оперативными данными является одним из ключевых направлений деятельности Интерпола.[138] Интерпол занимает уникальное положение, предоставляя глобальную и нейтральную платформу для правоохранительных органов, объединяющую экспертов, правительства, промышленность, научные круги и частный сектор для оказания помощи странам-членам в борьбе с этими новыми угрозами.[139]

Учитывая решающую роль разведывательных служб в выявлении схем террористической деятельности, которые в отрыве от другой информации могут показаться незначительными, крайне важно получить комплексное представление о том, что международные террористические группировки планируют делать в отношении энергетической инфраструктуры. Крайне важно учитывать, в том числе с точки зрения прав человека, конфиденциальный характер предоставленных оперативных данных, включая то, как они были собраны и как их предполагается использовать.

5.4.3. Экспертные, исследовательские сетевые и международные комплексные программы по повышению потенциала

Разработка политики защиты КВЭИ должна подкрепляться экспертными и научными данными для повышения ее эффективности, поскольку она требует высокого уровня знаний в различных областях. Хотя защита важнейших объектов энергетики является приоритетом для многих стран, не все располагают необходимыми ресурсами и междисциплинарными навыками. Таким образом, обмен знаниями и экспертная поддержка в рамках международного сотрудничества имеют решающее значение.

Экспертная и исследовательская поддержка международного сотрудничества в области защиты КВЭИ важна по нескольким причинам:

- Выработка общего понимания террористических угроз, тенденций и развивающихся методов работы.
- Содействие научным исследованиям по тематики террористических атак в отношении КВЭИ.

[138] Защита критически важных инфраструктур от террористических атак: Сборник передовой практики, 2018, доступ оп ссылке: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf.

[139] Там же.

- Установление единой терминологии и определений, касающихся контртеррористической деятельности на объектах энергетической инфраструктуры.
- Обмен передовым опытом по выявлению подозрительной деятельности, связанной с терроризмом.

Ярким примером экспертной поддержки и обмена знаниями является деятельность негосударственной организации «Научно-исследовательский институт проблем безопасности СНГ», которая совместно с ведущими отраслевыми вузами Восточной Европы и Центральной Азии организовала ряд международных семинаров и конференций по вопросам безопасности нефтегазовой инфраструктуры.[140]

В некоторых случаях международное экспертное и научное сотрудничество может включать совместное обучение как важный компонент. Например, взаимодействие на уровне экспертов Кувейта и США в 2018-2019 годах включало комплексные учебные сессии, обмен данными и повышение осведомленности об угрозах терроризма для объектов нефтегазовой отрасли.[141]

5.4.4. Защита конфиденциальной информации

При обмене информацией и данными, являющимся важнейшим аспектом межгосударственного сотрудничества в области защиты энергетических объектов, возникают проблемы защиты конфиденциальной информации. Межгосударственный обмен информацией сопряжен с рисками, связанными с конфиденциальностью и безопасностью информации. Как случайное, так и преднамеренное раскрытие секретной оперативной информации может существенно подорвать эффективность разведывательных служб и других институтов.

Для обеспечения безопасного обмена информацией национальные агентства, правоохранительные органы и операторы КВЭИ должны быть уверены в том, что при обработке, хранении и обеспечении защиты их конфиденциальной информации исключена возможность ее несанкционированного раскрытия. Поэтому обмен информацией должен осуществляться в соответствии со стандартными механизмами и протоколами, предназначенными для эффективной защиты и обмена информацией о КВИ. Например, Центр обмена и анализа нефти и газа (ONG-ISAC) для обмена информацией использует протокол Traffic Light Protocol (TLP), что позволяет членам обмениваться информацией как анонимно, так и с указанием источника.[142] Только члены ONG-ISAC получают информацию, имеющую пометку TLP Green, Amber и Red; лица, не являющиеся членами, получают только информацию, имеющую пометку TLP Clear.[143]

[140] Доступ по ссылке: https://spi-cis.ru/deyatelnost/nauchnaya/.
[141] Доступ по ссылке https://nps.edu/web/eag/kuwait-energy-infrastructure.
[142] Протокол Traffic Light был создан для содействия более широкому обмену потенциально конфиденциальной информацией и более эффективного сотрудничества. Передача информации осуществляется от одного источника информации к одному или нескольким получателям. TLP — это набор из четырех меток, используемых для обозначения границ совместного использования, которые должны применяться получателями.
[143] Доступ по ссылке: https://ongisac.org/.

6. Защита инфраструктуры возобновляемых и нетрадиционных источников энергии

6.1. Террористические угрозы инфраструктуре возобновляемых источников энергии

6.1.1. Инфраструктура возобновляемых источников энергии как цель террористов

Поскольку современное общество все больше опирается на инфраструктуру возобновляемых источников энергии, эти объекты становятся все более привлекательными целями для террористических атак. Например, в 2023 году объект MGM Mega Solar Array в США был закрыт после инцидента, который посчитали террористическим актом. Злоумышленник врезался на своем автомобиле в трансформатор солнечного генератора, а затем поджег транспортное средство.[144]

Инфраструктура возобновляемых источников энергии часто состоит из крупных, географически разбросанных объектов, оснащенных передовыми технологиями. Например, ветряные электростанции могут иметь сотни турбин и охватывать огромные площади, составляющие сотни квадратных километров.

В частности, морские ветровые электростанции становятся все более привлекательными целями для правонарушителей. Их огромные размеры и удаленное расположение в открытом море создают многочисленные проблемы безопасности. Следовательно, эти объекты требуют постоянного наблюдения и комплексных систем обнаружения для отслеживания приближающихся надводных и подводных угроз.

6.1.2. Уязвимости инфраструктуры возобновляемой энергетики

Объекты возобновляемой энергетики все чаще контролируются и управляются с помощью удаленных инструментов и приложений, которые в значительной степени зависят от стабильности информационной инфраструктуры. Например, в последние годы сектор ветроэнергетики столкнулся с атаками с использованием ИКТ, которые повлияли на его способность контролировать и управлять ветряными турбинами. В марте 2022 года после одной из таких атак немецкому производителю ветряных турбин пришлось отключить свои ИТ-системы на нескольких объектах и в нескольких бизнес-подразделениях. Инцидент был своевременно обнаружен службой ИТ-безопасности, и меры

[144] Доступ по ссылке: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/fbi-joins-investigation-into-alleged-terror-attack-on-las-vegas-solar-plant-73776901.

реагирования были приняты незамедлительно. Власти и сотрудники экстренных служб провели масштабные расследования и судебно-медицинскую экспертизу.

Из-за высокой степени взаимозависимости систем возобновляемой энергии успешные террористические атаки могут привести к значительным сбоям и каскадным отказам. Подобные атаки могут затронуть не только компьютерные системы и физические компоненты ветроэнергетических установок, но и подорвать надежность всей электросети.

Подобно объектам традиционной энергетики, инфраструктура возобновляемой энергетики уязвима как для ИКТ-атак, так и для смешанных физических и ИКТ-атак. Например, подстанция может иметь две отдельные сети SCADA: одну для управления работой ветряных турбин, а другую для управления сбором и подачей электроэнергии в сеть. Такая сегментация может повысить уязвимость как к физическим, так и к ИКТ-атакам, способным нарушить или исказить каналы связи.

6.1.3. Меры защиты, специфичные для конкретного объекта

Меры физической и информационной безопасности для инфраструктуры возобновляемой энергетики часто напоминают те, которые применяются для традиционных объектов энергетики. Однако существуют очевидные исключения и нюансы, обусловленные спецификой данных объектов.

Хотя инфраструктура возобновляемой энергетики является важнейшим компонентом энергетических систем многих стран, она не всегда соответствует тем же строгим нормам и стандартам, что и традиционные объекты энергетики. Это несоответствие можно объяснить более низким воспринимаемым уровнем угрозы и меняющимся характером методов защиты на национальном уровне. Например, эксперты Sandia National Laboratories (США) отметили отсутствие стандартов для оборудования, связанного с информационными технологиями, требований безопасности при передаче данных и протоколов сертификации в секторе солнечной энергетики.[145]

Учитывая масштабы многих объектов возобновляемой энергетики, таких как солнечные электростанции, традиционные технологии наблюдения и обнаружения вторжений могут оказаться весьма дорогостоящими. Кроме того, применение традиционных средств обнаружения, таких как радары, имеет определенные проблемы: например, движение лопаток турбины может препятствовать прохождению радиолокационных лучей или создавать помехи для них, что ограничивает их эффективность.[146] Таким образом, использование ограждений, оборудованных датчиками обнаружения вторжений, по периметру объекта, как это было продемонстрировано на примере венгерского солнечного парка Tázlár, может стать эффективной и экономически выгодной мерой повышения физической безопасности.

Новые технологии также способствуют защите этих объектов. Например, инфракрасные датчики — это особый тип датчиков движения, использующих инфракрасное излучение. Их можно использовать для обеспечения наблюдения и обнаружения как неотъемлемой части системы физической безопасности морских ветряных электростанций. Кроме того, во многих случаях эти системы

[145] Johnson Jay, Roadmap for Photovoltaic Cyber Security, Report number: SAND2017-13262, 2017, доступ по ссылке: https://www.researchgate.net/publication/322568290_Roadmap_for_Photovoltaic_Cyber_Security.

[146] Доступ по ссылке: https://www.roc.noaa.gov/wsr88d/windfarm/turbinesimpacton.aspx.

обнаружения дополнены технологиями искусственного интеллекта, обеспечивающими автоматическое распознавание и классификацию угроз, интеллектуальную фильтрацию сигналов тревоги и автоматическое реагирование (создание снимков экрана, видео и т. д.).[147]

Вставка 8

Меры защиты ветряных электростанций от противоправной деятельности в области информационных и коммуникационных технологий

Согласно исследованиям атак на ветряные электростанции,[148] векторы доступа, которые террористы могут использовать для осуществления атак с использованием ИКТ, включают:

- Физический доступ к ветряным турбинам или коллекторным подстанциям.
- Удаленный доступ к информационным системам.
- Атаки на транзитные информационные и коммуникационные объекты, которые могут быть классифицированы как физические, информационные или комбинированные информационно-физические атаки в зависимости от метода воздействия.

Для минимизации этих рисков и защиты ветряных электростанций от противоправного использования ИКТ можно реализовать следующие меры:

- Меры физической защиты:
  - Оснастите каждую турбину надежными механизмами блокировки, многофакторной аутентификацией, датчиками движения, камерами видеонаблюдения и удаленными уведомлениями о тревоге.
- Меры информационной защиты:
  - Изоляция турбин: обеспечьте изоляцию турбин, когда связь между турбинами не требуется.
  - Усиление защиты системы: отключите ненужные интерфейсы удаленного управления.
  - Усовершенствованные политики и процедуры информационной безопасности: усовершенствуйте политики и процедуры для повышения общей безопасности.

Источник: Staggs, Jason & Ferlemann, David & Shenoi, Sujeet. (2017). Wind farm security: Attack surface, targets, scenarios and mitigation. International Journal of Critical Infrastructure Protection. 17. 10.1016/j.ijcip.2017.03.001. https://www.researchgate.net/publication/315590797_Wind_farm_security_Attack_surface_targets_scenarios_and_mitigation.

147 Например: https://hgh-infrared.com/offshore-windfarm-security.

148 Sarah G. Freeman, Matthew A. Kress-Weitenhagen, Jake P. Gentle, Megan J. Culler, Megan M. Egan, Remy V. Stolworthy Attack Surface of Wind Energy Technologies in the United States, 2024, доступ по ссылке: https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf?utm_medium=email&utm_source=govdelivery.

6.2. Защита инфраструктуры ядерной энергетики от террористических атак

Атаки на объекты ядерной энергетики входят в более широкий спектр рисков ядерного терроризма. Подобные атаки вызывают особую обеспокоенность, поскольку они могут оказать значительное устрашающее воздействие, что повышает их привлекательность для террористов.

В преамбуле к Международной конвенции о борьбе с актами ядерного терроризма (2005 г.) государства-члены признали, что «акты ядерного терроризма могут повлечь за собой самые серьезные последствия и могут представлять угрозу международному миру и безопасности». В преамбуле также подчеркивается настоятельная необходимость укрепления международного сотрудничества между государствами в целях разработки и реализации эффективных мер по предотвращению подобных актов терроризма, а также по преследованию и наказанию виновных.

Мотивы террористических атак на атомные электростанции зачастую обусловлены скорее возможностью катастрофических последствий, чем просто нарушением цепочки поставок.

6.2.1. Специфические террористические угрозы атомным электростанциям

Основная привлекательность объектов ядерной энергетики в качестве целей для террористов заключается в возможности выброса радиоактивности, достаточно большого, чтобы привести к значительным жертвам и загрязнению земель. Например, в 2016 году две атомные электростанции в Бельгии были заблокированы из-за подозрений в попытке ИГИЛ (ДАИШ) атаковать, проникнуть или устроить диверсию на объектах с целью получения ядерных и радиоактивных материалов.[149]

Основными международно-правовыми документами в области физической ядерной безопасности, принятыми под эгидой Международного агентства по атомной энергии (МАГАТЭ), являются Конвенция о физической защите ядерного материала (КФЗЯМ) и Поправка к ней 2005 года.[150] Эти документы стали важнейшими вехами в развитии международно-правовой базы физической ядерной безопасности, поскольку остаются единственными юридически обязывающими международными обязательствами в области физической защиты ядерных материалов и ядерных установок, используемых в мирных целях. КФЗЯМ и Поправка к ней устанавливают правовые обязательства сторон в отношении физической защиты ядерного материала, используемого в мирных целях.

В соответствии с международными стандартами защиты от физических атак, таких как взрывы и бомбардировки, операторы атомных электростанций в значительной степени усилили меры безопасности. Они разработали современные защитные барьеры, включая заграждения на въезде, множественные ограждения и конструкции, устойчивые к физическим воздействиям. Меры по

[149] Belgium evacuates nuclear plant staff after attacks / CBS news. Доступ по ссылке: https://www.cbsnews.com/news/belgium-attacks-evacuation-tihange-nuclear-plant-staff-isis-dirty-bomb.

[150] Конвенция о физической защите ядерного материала (КФЗЯМ) и Поправка к ней, доступ по ссылке: https://www.iaea.org/publications/documents/conventions/convention-physical-protection-nuclear-material-and-its-amendment.

борьбе с терроризмом на атомных электростанциях включают в себя создание специальных сил реагирования на чрезвычайные ситуации, биометрические и другие сложные системы контроля доступа, освещенные зоны обнаружения и различные средства обнаружения вторжений. К таким средствам относятся различные типы полей обнаружения, системы видеонаблюдения и устройства сигнализации/оповещения, а также пуленепробиваемые заграждения в критических зонах.

Несмотря на высокий уровень защиты от внешних атак, ядерные объекты остаются уязвимыми для инсайдерских угроз. Технологическая сложность объектов ядерной энергетики подчеркивает острую необходимость в глубоких знаниях принципов их работы и методов обеспечения безопасности. Террористам, скорее всего, понадобится инсайдерская информация, чтобы одновременно отключить управление реактором и несколько систем безопасности. Например, в 2024 году Королевская канадская конная полиция арестовала бывшего сотрудника Ontario Power Generation за то, что он якобы передал защищенную информацию об атомной электростанции террористической группировке или иностранному государству.[151]

Для предотвращения угроз многие государства-члены требуют от сотрудников атомных электростанций проходить проверку на наличие судимостей и выполнять различные тесты на безопасность. На некоторых объектах также действует «правило двух человек», которое запрещает сотрудникам работать одним в некоторых зонах повышенной безопасности атомной электростанции.

Ярким примером инсайдерской угрозы является ситуация, произошедшая в Бельгии на атомной электростанции «Дул» в 2014 году.[152] Злоумышленник проник в реактор № 4 на атомной электростанции Дул и повернул клапан, слив 65 000 литров масла, используемого для смазки турбин. Это действие вызвало значительное трение, что едва не привело к перегреву оборудования и привело к его остановке. Ущерб был настолько серьезным, что реактор был выведен из эксплуатации на пять месяцев.

Кроме того, атомные станции управляются с помощью систем информационного контроля, что делает их уязвимыми для ИКТ-атак. Показательным примером является произошедшая в 2019 году ситуация на АЭС «Куданкулам», где были обнаружены вредоносные действия в системах ИКТ. Позже выяснилось, что в журналах содержались данные со взломанного компьютера, принадлежащего сотруднику.[153]

Ядерные объекты, которые потенциально могут стать целями, включают не только реакторы по производству плутония, но и связанные с ними объекты по хранению отработанного топлива и его переработке. Эти места являются привлекательными целями для злоумышленников из-за хранящихся и используемых там опасных веществ.

Кроме того, транспортировка ядерных и других радиоактивных материалов также уязвима для террористических атак. По данным информационного бюллетеня ITDB, 52% всех зарегистрированных

[151] Доступ по ссылке: https://www.power-eng.com/news/ex-ontario-power-generation-employee-accused-of-sharing-information-with-foreign-entity-or-terrorist-group/#gref.

[152] Доступ по ссылке: https://www.brusselstimes.com/181163/enquiry-into-nuclear-plant-sabotage-comes-to-no-conclusion.

[153] Breach at Kudankulam nuclear plant may have gone undetected for over six months, доступ по ссылке: https://economictimes.indiatimes.com/news/politics-and-nation/breach-at-kudankulam-nuclear-plant-may-have-gone-undetected-for-over-six-months-group-ib/articleshow/79412969.cms?from=mdr.

краж с 1993 года произошли во время санкционированной перевозки радиоактивных материалов.[154] Поэтому решающее значение имеют международное сотрудничество и совместные учения по транспортировке ядерных и других радиоактивных материалов. Например, в 2015 году Марокко и Испания провели совместные командно-штабные и полевые учения («Ворота в Африку») по отработке террористических угроз при транспортировке радиоактивных материалов. Целью совместных учений была проверка национальных мер и возможностей в области ядерной безопасности с точки зрения предотвращения, обнаружения, защиты и реагирования на события во время перевозки радиоактивных материалов морским транспортом, а также обсуждение и отработка мер реагирования на террористические акты с использованием радиоактивных материалов.[155]

6.2.2. Практика защиты ядерных объектов

МАГАТЭ играет центральную роль в разработке международных стандартов и норм по защите атомных электростанций от физических и ИКТ-атак. Ключевые правовые основы международной защиты ядерных объектов от терроризма и других противоправных действий включают следующие документы:

- Конвенция о физической защите ядерного материала (с поправкой 2005 года)
- Международная конвенция о борьбе с актами ядерного терроризма
- Глобальная контртеррористическая стратегия ООН
- Резолюции Совета Безопасности ООН 1373 (2001), 1540 (2004) и 2325 (2016)
- Кодекс поведения по обеспечению безопасности и сохранности радиоактивных источников

Серия публикаций МАГАТЭ по физической ядерной безопасности служит дополнением к этим инструментам, предлагая передовой опыт, технические руководства, учебные пособия и другие ресурсы для оказания помощи государствам-членам. К другим важным инициативам МАГАТЭ относится Центр обучения и демонстрации в области физической ядерной безопасности (NSTDC), открытый в лабораториях МАГАТЭ в Зайберсдорфе в 2023 году. NSTDC посредством обучения, проведения исследований и разработок содействует укреплению возможностей стран по борьбе с ядерным терроризмом, решению специфических проблем и реализации сложных проектов в области ядерной безопасности, требующих специализированной технической инфраструктуры.[156]

В рамках своей Глобальной программы по противодействию использованию оружия террористами КТУ/КТЦ ООН оказывает поддержку усилиям государств-членов по противодействию ядерному терроризму через специальный портфель учебных мероприятий, в том числе по защите КВИ, и оказание технической помощи в осуществлении Международной конвенции о борьбе с актами ядерного терроризма (МКБАТ, 2005).[157]

[154] Доступ по ссылке: https://www.iaea.org/resources/databases/itdb.
[155] Более подробная информация: https://amssnur.org.ma/wp-content/uploads/2020/11/Gate-to-Africa-report.pdf.
[156] Более подробная информация: https://www.iaea.org/about/organizational-structure/department-of-nuclear-safety-and-security/division-of-nuclear-security/iaea-nuclear-security-training-and-demonstration-centre.
[157] Более подробная информация: https://www.un.org/counterterrorism/cct/chemical-biological-radiological-and-nuclear-terrorism.

Для предоставления странам-членам информации, касающейся их расследований террористических и преступных актов с использованием радиоактивных и ядерных материалов, Интерполом создана база данных Гейгера и базу данных по инцидентам и контрабанде (ITDB). (https://www.iaea.org/resources/databases/itdb). Это аналитическая платформа, которая собирает данные правоохранительных органов об инцидентах, связанных с радиоактивными или ядерными материалами. Она используется для анализа закономерностей и тенденций, рисков и угроз, маршрутов и методов, слабых мест и уязвимостей, а также дополняет публикации уведомлений Интерпола и двухмесячного дайджеста CBRNE.[158]

Международные усилия привели к разработке сложного набора строгих стандартов и требований, при этом многие государства-члены разрабатывают национальные инструменты и меры по обеспечению ядерной безопасности. Например, Управление по ядерному регулированию Японии обязывает местные органы власти разрабатывать планы эвакуации граждан, проживающих в радиусе 30 километров от атомной электростанции, в случае возникновения чрезвычайной ситуации. Это требование дополняет международные стандарты гражданской ядерной безопасности.

В некоторых государствах-членах создан специализированный государственный орган для координации защиты атомных электростанций и реализации общегосударственного подхода. Например, в 2015 году правительство Индии создало Совет по ядерной безопасности, который действует под руководством премьер-министра.[159]

Еще одной мерой защиты критически важных ядерных объектов является создание на государственном уровне специализированных сил безопасности или вооруженных групп быстрого реагирования. Например, в Великобритании Гражданская ядерная полиция представляет собой специализированное вооруженное формирование, отвечающее за оборону ядерных объектов, таких как Селлафилд и Даунрей. Кроме того, это подразделение имеет право производить задержания на неядерных объектах, таких как порты, аэропорты и железнодорожные станции.[160] Полиция также осуществляет патрулирование на расстоянии до трех миль от ядерных объектов и имеет право останавливать и обыскивать людей и транспортные средства.

158 https://www.interpol.int/Crimes/Terrorism/Radiological-and-Nuclear-terrorism/Our-response-to-radiological-and-nuclear-terrorism.
159 Nuclear security in India, 2015, доступ по ссылке: https://www.orfonline.org/wp-content/uploads/2015/02/NUCLEAR_SECURITY_IN_INDIA.pdf.
160 Доступ по ссылке: https://www.gov.uk/government/organisations/civil-nuclear-constabulary/about.

Приложение 1

Перечень передовых практик, включенных в руководство

Тематика	Международная передовая практика	Описание	Ссылка на страницу
Нормативно-правовая база	Включение защиты КВЭИ в политику национальной безопасности	Включение защиты КВЭИ в число приоритетов национальной безопасности для укрепления скоординированных усилий и межведомственного сотрудничества.	стр. 26-27
	Определение субъектов энергетического сектора, включая распределение соответствующих ролей и обязанностей	Национальные правила должны определить четкие критерии категоризации субъектов КВЭИ, их функции и зоны ответственности в области безопасности и защиты энергетической инфраструктуры	стр. 32
	Определение критериев критичности энергетической инфраструктуры	Правовые основы обеспечения критериев критичности энергетических объектов, площадок и активов, характерных для энергетического сектора, с использованием качественных и количественных показателей на государственном (федеральном), региональном (провинциальном) и местном (муниципальном) уровнях	стр. 32-34
	Особые требования к проектированию, строительству, эксплуатации и обслуживанию КВЭИ	В целях обеспечения высокого уровня безопасности органы, регулирующие деятельность КВЭИ, разрабатывают стандарты или строительные нормы для проектирования, строительства, эксплуатации и обслуживания различных типов энергетической инфраструктуры, включая электротехническое оборудование.	стр. 38
	Установление отраслевых стандартов безопасности в сфере борьбы с терроризмом	Национальное законодательство в сфере борьбы с терроризмом, предусматривающее стандарты безопасности, помимо прочего, для инфраструктуры энергетического сектора, в том числе для различных типов объектов энергетики	стр. 36, 38

Тематика	Международная передовая практика	Описание	Ссылка на страницу
Управление рисками	Сертификаты безопасности («паспорт безопасности») КВЭИ	«Паспорт безопасности» — это документ по планированию безопасности, разрабатываемый для каждого критического объекта и/или объекта энергетической инфраструктуры и содержащий подробную информацию, в том числе о потенциальном социально-экономическом воздействии незаконного вмешательства, конкретных мерах безопасности, плане управления чрезвычайными ситуациями и т.д.	стр. 40
	Модель анализа риска «ВСК»	Специальный инструмент анализа рисков, включающий многомерную идентификацию факторов риска, дерево событий, графы знаний и инструменты для оценки рисков безопасности, включая риски, связанные с терроризмом, для критически важных объектов энергетики.	стр. 57
	Моделирование атак в соответствии с выявленными рисками	Применение структурированной методологии для моделирования потенциальных террористических атак на КВЭИ, включая типологию атак, идентификацию целей, идентификацию преступников, оценку ресурсов и другие этапы	стр. 61
Информационная безопасность	Отраслевые правила и стандарты обработки конфиденциальной энергетической информации	Разработка четких правил и стандартов для отрасли по обработке конфиденциальной энергетической информации, включая информацию об уязвимостях, угрозах, местоположении, конструкции и т.д., для минимизации рисков физической и информационной безопасности	стр. 38
	Группы реагирования на инциденты, связанные с нарушением компьютерной безопасности на КВЭИ	Создание специализированных центров для сбора данных и отчетов по каждому инциденту, связанному с нарушением компьютерной безопасности на критических энергетических объектах, включая использование программ-вымогателей, фишинг и другие подобные угрозы	стр. 66-67
	Интегрированные системы безопасности данных для КВЭИ	Информационные системы безопасности критической инфраструктуры содержат оцифрованные записи условий безопасности для КВИ, включая объекты	стр. 67

Тематика	Международная передовая практика	Описание	Ссылка на страницу
		энергетики на всей территории страны. Эта система охватывает сбор, обработку, хранение и поиск информации	
	Лаборатории моделирования ИКТ-рисков на критически важных объектах нефтегазового комплекса	Использование как программных и аппаратных инструментов, а также «цифрового двойника» типичных информационных процессов в нефтегазовой компании для моделирования различных видов ИКТ-атак	стр. 67
	Протокол Светофор	Протокол Светофор - система классификации конфиденциальной информации, которая также используется в энергетической отрасли для предоставления рекомендаций по работе с несекретными данными с целью содействия более широкому обмену информацией и обеспечения того, чтобы информация была предоставлена соответствующей аудитории.	стр. 86
Физическая безопасность	Система наблюдения на основе инфракрасных датчиков	В системе наблюдения на основе инфракрасных датчиков используется инфракрасное излучение для обеспечения бесперебойного наблюдения и обнаружения на морских ветряных электростанциях. Она позволяет эффективно обнаруживать угрозы с моря, такие как небольшие суда без автоматических систем идентификации, и хорошо работает в коррозионной морской среде.	стр. 88
	Зоны безопасности вокруг критически важных нефтяных/газовых объектов	Установление специального регулирования, обязывающего операторов/владельцев КВЭИ создавать зоны вокруг нефтегазовых объектов с дополнительными требованиями безопасности, такими как правила допуска лиц и транзитной доступности	стр. 38
	Морское патрулирование вблизи объектов морской энергетической инфраструктуры	Физическая безопасность морской нефтегазовой инфраструктуры может быть обеспечена за счет активного патрулирования района патрульными катерами, называемыми «судами быстрого реагирования».	стр. 63

Тематика	Международная передовая практика	Описание	Ссылка на страницу
	Датчики обнаружения проникновения	Установка ограждения периметра, оборудованного датчиками обнаружения проникновения, такими как волоконно-оптический кабель, вокруг нефтегазовых объектов или вдоль трубопроводов представляет собой эффективный метод повышения физической безопасности КЭИ.	стр. 65, 88
	Системы обнаружения с технологиями ИИ	Датчики обнаружения на КВЭИ, интегрированные с технологиями ИИ, обеспечивают автоматическое распознавание и классификацию угроз, интеллектуальную фильтрацию сигналов тревоги и автоматизированные механизмы реагирования, такие как скриншоты и видеозапись.	стр. 89
	Управление информацией о физической безопасности (PSIM)	PSIM это инструмент 3D-визуализации для проектирования систем физической защиты на КВЭИ. Данный инструмент направлен на усиление мер эксплуатационной безопасности и выбор экономически эффективных методов защиты объектов энергетики.	стр. 60
Операционные рамки	Учения по обеспечению безопасности в нефтегазовой отрасли	Учения по обеспечению безопасности в нефтегазовой отрасли направлены на укрепление регионального сотрудничества путем разработки комплексных мер реагирования, включая политику и институциональные рамки, для эффективного устранения перебоев в поставках нефти и газа и ущерба инфраструктуре.	стр. 78
	Специализированные органы безопасности, ответственные за безопасность КВЭИ	Создание специального подразделения безопасности в структуре ответственного министерства для обеспечения защиты критически важных объектов энергетического сектора	стр. 46-47
	Сеть субъектов энергетического сектора под управлением уполномоченного государственного органа	Разработка совместного подхода к эффективному обмену информацией для защиты энергетической инфраструктуры с целью содействия обмену данными, знаниями и опытом между субъектами частного и государственного энергетического сектора	стр. 53

Тематика	Международная передовая практика	Описание	Ссылка на страницу
	Регулярные учения по реагированию на аварийные ситуации	Проведение учений ГЧП на случай возникновения аварийных ситуаций для обеспечения готовности к реализации соответствующих мер реагирования на непредвиденные сбои	стр. 52
	«Общеотраслевой подход»: вовлечение как частных, так и государственных субъектов в разработку политики безопасности КВЭИ	Участие субъектов частного сектора в разработке стандартов безопасности для защиты КВЭИ в случае, когда субъекты частного сектора могут предлагать изменения в существующие стандарты безопасности или рекомендации государственных органов, например, по трубопроводам в зонах безопасности, в рамках прозрачного и консенсусного процесса.	стр. 52
Трансграничное сотрудничество	Трансграничные совместные патрули	Осуществление двустороннего или многостороннего вооруженного морского или пешего патрулирования в приграничных районах или морских зонах, прилегающих к нефтяным платформам и газопроводам	стр. 80-81
	Трансграничные антитеррористические учения по защите КВЭИ	Проведение совместных антитеррористических учений и маневров для проверки и совершенствования взаимодействия в управлении чрезвычайными ситуациями	стр. 82-83
	Гармонизация контртеррористического законодательства по защите КВЭИ	Гармонизация национального законодательства по борьбе с терроризмом и содействие обмену нормативной информацией и практикой, касающимися мер по борьбе с терроризмом в энергетическом секторе	стр. 84
	Международные программы обучения для сотрудников служб безопасности	Разработка и проведение специализированных курсов по защите энергетического сектора для сотрудников служб безопасности с целью реагирования на новые и возникающие угрозы и вызовы безопасности	стр. 81-82

Приложение 2

Рекомендации по противодействию терроризму на объектах топливно-энергетического комплекса, принятые Организацией Договора о коллективной безопасности (ОДКБ), декабрь 2022 года

Приложение к
Резолюции № 15-5.1
Парламентской Ассамблеи ОДКБ
от 5 декабря 2022 г.

Рекомендации по противодействию терроризму на объектах топливно-энергетического комплекса

1. Общие положения

Рекомендации по противодействию терроризму на объектах топливно-энергетического комплекса направлены на установление общих подходов в государствах – членах ОДКБ к правовому регулированию противодействия терроризму на объектах топливно-энергетического комплекса.

1.1. Основные понятия, используемые в Рекомендациях, и их определения

Для целей Рекомендаций используются следующие основные понятия и их определения:

- антитеррористическая защищенность объекта топливно-энергетического комплекса – состояние здания, строения, сооружения или иного объекта топливно-энергетического комплекса, препятствующее совершению на нем террористического акта;
- зона безопасности объекта топливно-энергетического комплекса – территория (акватория) вокруг устанавливаемого правительством государства отдельного объекта топливно-энергетического комплекса, в границах которой реализуются меры по обеспечению особого режима защиты такого объекта от террористического акта;
- категорирование объекта топливно-энергетического комплекса – проведение комплекса мероприятий, направленных на определение соответствия объекта топливно-энергетического комплекса критериям категорирования и их показателям;
- критически важные объекты топливно-энергетического комплекса – объекты топливно-энергетического комплекса, нарушение или прекращение функционирования которых приведет к снижению управляемости или потере управления экономикой государства, одного или нескольких административно-территориальных образований страны, отрасли промышленности или энергетики, негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения в административно-территориальном образовании;
- критический элемент объекта топливно-энергетического комплекса – потенциально опасные элементы (участки) объекта топливно-энергетического комплекса, совершение террористического акта или иного противоправного действия в отношении которых приведет к

прекращению нормального функционирования объекта топливно-энергетического комплекса, его повреждению или к аварии на объекте топливно-энергетического комплекса;

- линейные объекты топливно-энергетического комплекса – система линейно-протяженных объектов топливно-энергетического комплекса (электрические сети, магистральные газопроводы, нефтепроводы и нефтепродуктопроводы), предназначенных для обеспечения передачи электрической энергии, транспортировки газа, нефти и нефтепродуктов;
- обеспечение антитеррористической защищенности объектов топливно-энергетического комплекса – реализация определяемой государством системы правовых, экономических, организационных, инженерно-технических, охранных и иных мер, направленных на воспрепятствование совершению террористического акта на объектах топливно-энергетического комплекса;
- объекты топливно-энергетического комплекса – объекты электроэнергетики, нефтедобывающей, нефтеперерабатывающей, газовой, газоперерабатывающей, угольной, углехимической, нефтехимической, сланцевой и торфяной промышленности, а также объекты нефтепродуктообеспечения, теплоснабжения и газоснабжения;
- паспорт антитеррористической защищенности объекта топливно-энергетического комплекса – документ, содержащий информацию об обеспечении антитеррористической защищенности объекта топливно-энергетического комплекса;
- потенциально опасные объекты топливно-энергетического комплекса – объекты топливно-энергетического комплекса, на которых используются, производятся, перерабатываются, хранятся, транспортируются или уничтожаются взрывоопасные, пожароопасные и опасные химические вещества, а также гидротехнические сооружения, аварии на которых, в том числе в результате совершения террористического акта, могут привести к возникновению чрезвычайных ситуаций с опасными социально-экономическими последствиями;
- потенциально опасные элементы (участки) объекта топливно-энергетического комплекса – территориально выделенные зоны (участки), конструктивные и технологические элементы объектов топливно-энергетического комплекса, аварии на которых, в том числе в результате совершения террористического акта или иного противоправного действия, могут привести к возникновению чрезвычайных ситуаций с опасными социально-экономическими последствиями;
- противодействие терроризму на объектах топливно-энергетического комплекса – деятельность субъектов противодействия терроризму по предупреждению терроризма на объектах топливно-энергетического комплекса, выявлению, пресечению, раскрытию и расследованию террористического акта и иных преступлений террористической направленности на объектах топливно-энергетического комплекса, минимизации и (или) ликвидации последствий совершения террористического акта на объектах топливно-энергетического комплекса;
- система физической защиты – совокупность методов и средств обеспечения физической целостности объекта топливно-энергетического комплекса, направленная на предотвращение террористического акта и иного противоправного действия;
- субъекты противодействия терроризму на объектах топливно-энергетического комплекса – органы государственной власти и органы местного управления и самоуправления, в

компетенцию которых входит проведение мероприятий по противодействию терроризму, субъекты топливно-энергетического комплекса, общественные объединения и иные организации, а также граждане, действующие в рамках полномочий, определенных законодательством государства, и оказывающие содействие органам государственной власти и органам местного управления и самоуправления в противодействии терроризму на объектах топливно-энергетического комплекса;

- субъекты топливно-энергетического комплекса – физические и юридические лица, владеющие на праве собственности или ином законном праве объектами топливно-энергетического комплекса;
- топливно-энергетический комплекс – совокупность отраслей экономики государства, обеспечивающих добычу, производство, транспортировку, хранение, переработку и использование всех видов энергетических ресурсов, за исключением ядерных материалов;
- требования обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса – правила, которые обязательны для выполнения и соблюдение которых обеспечивает антитеррористическую защищенность объектов топливно-энергетического комплекса.

Другие понятия, используемые в настоящих Рекомендациях, понимаются в соответствии с их определениями, установленными модельными законами государств – членов ОДКБ и национальным законодательством государства.

1.2. Правовая основа противодействия терроризму на объектах топливно-энергетического комплекса

Правовую основу противодействия терроризму на объектах топливно-энергетического комплекса составляют общепризнанные принципы и нормы международного права, международные договоры, иные применимые источники международного права, конституция государства и иные правовые акты государства.

1.3. Основные принципы противодействия терроризму на объектах топливно-энергетического комплекса

Основными принципами противодействия терроризму на объектах топливно-энергетического комплекса являются:

1. Законность;
2. Соблюдение прав и свобод человека и гражданина;
3. Объективность, полнота и всесторонность в оценке угроз террористического характера;
4. Приоритет мер предупреждения терроризма на объектах топливно-энергетического комплекса;
5. Комплексность использования мер противодействия терроризму;
6. Непрерывность реализации мер по противодействию терроризму;

7. Конфиденциальность сведений о специальных средствах, технических приемах, тактике осуществления мероприятий по противодействию терроризму на объектах топливно-энергетического комплекса, а также о составе их участников;
8. Научно-технологическое сопровождение построения и эксплуатации комплексных и информационных систем безопасности объектов топливно-энергетического комплекса;
9. Сочетание гласных и негласных методов противодействия терроризму на объектах топливно-энергетического комплекса;
10. Эффективное разграничение компетенции субъектов противодействия терроризму на объектах топливно-энергетического комплекса;
11. Единоначалие в руководстве силами и средствами, привлекаемыми для проведения контртеррористических операций;
12. Информирование общественности об акте терроризма и о проведении контртеррористических операций на объектах топливно-энергетического комплекса;
13. Международное сотрудничество с другими государствами и международными организациями;
14. Неотвратимость наказания за осуществление террористического акта;
15. Минимизация уступок террористам.

1.4. Цели и задачи противодействия терроризму на объектах топливно-энергетического комплекса

Противодействие терроризму на объектах топливно-энергетического комплекса осуществляется в целях устойчивого и безопасного функционирования топливно-энергетического комплекса, а также защиты интересов личности, общества и государства от терроризма.

Для достижения указанных целей необходимо решить следующие задачи:

1. нормативное правовое регулирование в области обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса;
2. разработка и реализация требований обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса;
3. разработка и реализация мер по созданию системы физической защиты объектов топливно-энергетического комплекса;
4. категорирование объектов топливно-энергетического комплекса;
5. определение угроз терроризма на объектах топливно-энергетического комплекса и предупреждение таких угроз;
6. защита государственных секретов в сфере обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса и противодействие иностранным техническим разведкам;
7. подготовка специалистов в сфере обеспечения безопасности объектов топливно-энергетического комплекса;

8. совершенствование оперативно-разыскной деятельности компетентных органов государства по противодействию терроризму;
9. организация совместной профилактической работы государственных органов, осуществляющих противодействие терроризму на объектах топливно-энергетического комплекса, с персоналом объектов топливно-энергетического комплекса, расположенных на территории государства;
10. организация контроля и надзора за исполнением законов в сфере обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса.

1.5. Категорирование объектов топливно-энергетического комплекса

Для установления дифференцированных требований обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса с учетом степени потенциальной опасности проводится категорирование объектов. При проведении категорирования учитываются:

1. информация о том, является ли объект топливно-энергетического комплекса критически важным объектом и (или) потенциально опасным объектом;
2. масштабы возможных социально-экономических последствий в результате совершения террористического акта на объекте топливно-энергетического комплекса;
3. наличие и защищенность критических элементов объекта топливно-энергетического комплекса;
4. наличие потенциально опасных элементов (участков) объекта топливно-энергетического комплекса;
5. наличие на объекте топливно-энергетического комплекса уязвимых мест;
6. наличие не объединенных единым периметром составных частей объекта топливно-энергетического комплекса;
7. наличие внешних угроз совершения террористического акта.

По результатам категорирования объекту топливно-энергетического комплекса присваивается одна из следующих категорий опасности:

- объекты высокой категории опасности (I категория);
- объекты средней категории опасности (II категория);
- объекты низкой категории опасности (III категория);

Если объект топливно-энергетического комплекса не соответствует критериям опасности и показателям этих критериев, ему не присваивается ни одна из таких категорий.

При наличии на объекте топливно-энергетического комплекса двух и более не объединенных единым периметром элементов (участков) категория опасности присваивается (не присваивается) каждому такому элементу (участку).

В соответствии с проведенным категорированием объекты включаются в перечень (реестр) объектов топливно-энергетического комплекса.

Порядок категорирования объектов топливно-энергетического комплекса определяется законодательством государства.

2. Правовая основа противодействия терроризму на объектах топливно-энергетического комплекса

2.1. Государственная политика в сфере противодействия терроризму на объектах топливно-энергетического комплекса

Государственная политика в сфере противодействия терроризму на объектах топливно-энергетического комплекса представляет собой совокупность мер государственного воздействия, направленных на обеспечение наиболее эффективного использования имеющихся ресурсов и выработку дополнительных мер для профилактики, выявления и пресечения террористической деятельности на объектах топливно-энергетического комплекса, минимизации и ликвидации последствий ее проявлений.

2.2. Система субъектов противодействия терроризму на объектах топливно-энергетического комплекса

Систему субъектов противодействия терроризму на объектах топливно-энергетического комплекса составляют государственные органы, органы местного управления и самоуправления, субъекты топливно-энергетического комплекса, общественные объединения и иные организации, а также граждане, действующие в рамках полномочий, определенных законодательством государства.

2.3. Меры, реализуемые субъектами топливно-энергетического комплекса

Субъект топливно-энергетического комплекса в целях противодействия терроризму реализует следующие меры:

1. Обеспечивает физическую защиту объектов топливно-энергетического комплекса;
2. Совершенствует систему мер антитеррористической защищенности объектов топливно-энергетического комплекса в соответствии с требованиями законодательства к категорированным объектам топливно-энергетического комплекса;
3. Обеспечивает конфиденциальность информации, бесконтрольное распространение которой может существенно понизить уровень антитеррористической защищенности объекта топливно-энергетического комплекса;
4. Допускает к непосредственной работе, связанной с обеспечением безопасности объекта топливно-энергетического комплекса, только лиц, не имеющих неснятую или непогашенную судимость за совершение умышленного преступления, прошедших специальное обучение, отвечающих квалификационным требованиям, не имеющих медицинских противопоказаний, а также прошедших в установленном порядке специальную проверку;

5. Информирует государственные органы, осуществляющие противодействие терроризму на объектах топливно-энергетического комплекса, об угрозе совершения и о совершении террористического акта на объектах топливно-энергетического комплекса, а также обо всех ставших известными фактах несанкционированных действий с потенциально опасными технологиями;
6. Внедряет инновационные организационно-управленческие формы и технологические решения обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса.

2.4. Участие органов местного управления и самоуправления, общественных объединений и иных организаций в противодействии терроризму на объектах топливно-энергетического комплекса

Органы местного управления и самоуправления, общественные объединения и иные организации участвуют в противодействии терроризму на объектах топливно-энергетического комплекса во взаимодействии с государственными органами, осуществляющими противодействие терроризму на объектах топливно-энергетического комплекса, в соответствии с законодательством государства.

2.5. Участие граждан в противодействии терроризму на объектах топливно-энергетического комплекса

Граждане на добровольных началах участвуют в решении задач по противодействию терроризму на объектах топливно-энергетического комплекса в форме оказания содействия государственным органам, осуществляющим противодействие терроризму на объектах топливно-энергетического комплекса. Порядок привлечения граждан к решению задач по противодействию терроризму на объектах топливно-энергетического комплекса определяется законодательством государства.

2.6. Порядок информирования об угрозе совершения или о совершении террористического акта на объектах топливно-энергетического комплекса и реагирования на полученную информацию

При поступлении информации об угрозе совершения террористического акта на объекте топливно-энергетического комплекса государственные органы, осуществляющие противодействие терроризму на объектах топливно-энергетического комплекса:

1. Осуществляют в установленном порядке прием, регистрацию и проверку указанной информации;
2. Осуществляют в первоочередном порядке информирование субъектов топливно-энергетического комплекса;
3. Передают в случае необходимости информацию должностным лицам, ответственным за организацию первоочередных мер по пресечению террористического акта на объекте топливно-энергетического комплекса.

Субъект топливно-энергетического комплекса обязан представлять информацию об угрозе совершения и о совершении террористического акта на объекте топливно-энергетического комплекса в государственные органы, осуществляющие противодействие терроризму на объектах топливно-энергетического комплекса.

Информирование субъектом топливно-энергетического комплекса государственных органов, осуществляющих противодействие терроризму на объектах топливно-энергетического комплекса, осуществляется незамедлительно:

1. После обнаружения субъектом топливно-энергетического комплекса угрозы совершения или совершения террористического акта на объекте топливно-энергетического комплекса;
2. При получении субъектом топливно-энергетического комплекса информации об угрозе совершения или о совершении террористического акта на объекте топливно-энергетического комплекса, в том числе анонимного характера.

Информация об угрозе совершения и о совершении террористического акта на объекте топливно-энергетического комплекса направляется субъектом топливно-энергетического комплекса посредством имеющихся в его распоряжении средств связи в государственные органы, осуществляющие противодействие терроризму на объектах топливно-энергетического комплекса, расположенные по фактическому местонахождению такого объекта.

Порядок взаимодействия государственных органов, осуществляющих противодействие терроризму на объектах топливно-энергетического комплекса, и субъектов топливно-энергетического комплекса при проверке информации об угрозе совершения террористического акта на объекте топливно-энергетического комплекса определяется законодательством государства.

3. Обеспечение антитеррористической защищенности объектов топливно-энергетического комплекса

3.1. Требования обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса

Обеспечение антитеррористической защищенности объектов топливно-энергетического комплекса осуществляется субъектами топливно-энергетического комплекса во взаимодействии с государственными органами, осуществляющими противодействие терроризму на объектах топливно-энергетического комплекса.

Требования обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса в зависимости от установленной категории опасности объектов определяются правительством государства.

Указанные требования являются обязательными для выполнения органами государственной власти и субъектами топливно-энергетического комплекса.

Требования обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса на этапе их проектирования и строительства (реконструкции) устанавливаются правительством государства в зависимости от потенциальной категории опасности объектов и являются обязательными для исполнения застройщиками объектов топливно-энергетического комплекса. Потенциальная категория опасности проектируемых, строящихся (реконструируемых)

объектов топливно-энергетического комплекса определяется по исходным данным без проведения категорирования объекта

Субъекты топливно-энергетического комплекса во взаимодействии с государственными органами, осуществляющими противодействие терроризму на объектах топливно-энергетического комплекса, обязаны совершенствовать систему мер антитеррористической защищенности объектов топливно-энергетического комплекса в соответствии с выявляемыми угрозами.

3.2. Планирование и реализация мер по обеспечению антитеррористической защищенности объектов топливно-энергетического комплекса

Для обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса субъектами топливно-энергетического комплекса во взаимодействии с государственными органами, осуществляющими противодействие терроризму на объектах топливно-энергетического комплекса, планируется и реализуется система мер по антитеррористической защищенности данных объектов.

Система мер по антитеррористической защищенности объектов топливно-энергетического комплекса отражается в паспорте антитеррористической защищенности объекта топливно-энергетического комплекса и включает правовые, организационные, инженерно-технические, охранные и иные меры.

Информация о системе мер по антитеррористической защищенности объектов топливно-энергетического комплекса, содержащаяся в паспорте антитеррористической защищенности объекта топливно-энергетического комплекса, является информацией, доступ к которой ограничен в соответствии с законодательством государства.

3.3. Физическая защита объектов топливно-энергетического комплекса

Обеспечение физической защиты объектов топливно-энергетического комплекса от угроз совершения террористических актов осуществляется на основе единой системы планирования и реализации технических и организационных мер, которые направлены на предотвращение несанкционированного проникновения на охраняемые объекты топливно-энергетического комплекса, своевременное обнаружение и пресечение терроризма на объектах топливно-энергетического комплекса.

Обеспечение физической защиты строящегося объекта топливно-энергетического комплекса, который после ввода в эксплуатацию будет отнесен к объектам высокой категории опасности (I категории опасности), осуществляется на стадии строительства.

Государственные органы, осуществляющие противодействие терроризму на объектах топливно-энергетического комплекса, подразделения охраны, привлеченные в установленном порядке для обеспечения физической защиты объектов топливно-энергетического комплекса, имеют право пресекать нахождение БПЛА в воздушном пространстве данных объектов в целях обеспечения целостности и безопасности охраняемых объектов посредством подавления или преобразования сигнала дистанционного управления и/или навигации беспилотными воздушными судами. Порядок

пресечения нахождения БПЛА в воздушном пространстве объектов топливно-энергетического комплекса определяется законодательством государства.

В целях повышения уровня антитеррористической защищенности объектов топливно-энергетического комплекса по результатам их категорирования вокруг отдельных объектов топливно-энергетического комплекса устанавливаются зоны безопасности объектов топливно-энергетического комплекса.

В зонах безопасности объектов топливно-энергетического комплекса обеспечивается особый режим защиты от террористических актов, включающий мероприятия по выявлению фактов подготовки или совершения террористических актов и иных противоправных действий в отношении данных объектов.

Объекты топливно-энергетического комплекса, вокруг которых устанавливаются зоны безопасности, с описанием местоположения границ таких зон, а также меры по обеспечению особого режима защиты от террористических актов определяются правительством государства.

3.4. Обеспечение безопасности критической информационной инфраструктуры объектов топливно-энергетического комплекса

К критической информационной инфраструктуре объектов топливно-энергетического комплекса относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, принадлежащие на праве собственности, аренды или на ином законном основании субъектам топливно-энергетического комплекса и используемые ими для осуществления видов деятельности в сфере топливно-энергетического комплекса.

Обеспечение безопасности критической информационной инфраструктуры объектов топливно-энергетического комплекса осуществляется на основе государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты в соответствии с законодательством государства в области обеспечения безопасности критической информационной инфраструктуры

Субъекты топливно-энергетического комплекса обязаны незамедлительно информировать о компьютерных инцидентах государственные органы, осуществляющие противодействие терроризму на объектах топливно-энергетического комплекса. Информация о критической информационной инфраструктуре объектов топливно-энергетического комплекса является информацией, доступ к которой ограничен в соответствии с законодательством государства.

3.5. Ответственность за нарушение законодательства в сфере противодействия терроризму на объектах топливно-энергетического комплекса

Лица, виновные в нарушении законодательства в сфере противодействия терроризму на объектах топливно-энергетического комплекса, несут гражданскую, административную, уголовную и иную ответственность в соответствии с законодательством государства.

4. Международное сотрудничество в сфере противодействия терроризму на объектах топливно-энергетического комплекса

4.1. Правовая основа международного сотрудничества в сфере противодействия терроризму на объектах топливно-энергетического комплекса

Правовую основу международного сотрудничества в сфере противодействия терроризму на объектах топливно-энергетического комплекса составляют общепризнанные принципы и нормы международного права, международные договоры, иные применимые источники международного права, конституция государства и иные правовые акты государства.

4.2. Цели международного сотрудничества в сфере противодействия терроризму на объектах топливно-энергетического комплекса

Международное сотрудничество в сфере противодействия терроризму на объектах топливно-энергетического комплекса осуществляется в целях:

1. Выработки согласованной политики и объединения усилий государств в сфере противодействия терроризму на объектах топливно-энергетического комплекса;
2. Исключения практики применения двойных стандартов в сфере противодействия терроризму на объектах топливно-энергетического комплекса;
3. Повышения эффективности взаимодействия государственных органов, осуществляющих противодействие терроризму на объектах топливно-энергетического комплекса;
4. Совершенствования правовой базы международного сотрудничества в сфере противодействия терроризму на объектах топливно-энергетического комплекса;
5. Гармонизации национального законодательства государств в сфере противодействия терроризму на объектах топливно-энергетического комплекса.

4.3. Основные направления и формы международного сотрудничества в сфере противодействия терроризму на объектах топливно-энергетического комплекса

Международное сотрудничество в сфере противодействия терроризму на объектах топливно-энергетического комплекса осуществляется по следующим основным направлениям:

1. договорно-правовое;
2. научно-информационное;
3. научно-техническое;
4. организационное;
5. информационно-аналитическое;
6. профилактическое;
7. образовательное.

Основными формами международного сотрудничества в сфере противодействия терроризму на объектах топливно-энергетического комплекса являются:

1. взаимодействие государственных органов по вопросам совершенствования их деятельности;
2. проведение взаимных консультаций по проблемам международного сотрудничества;
3. разработка и принятие согласованных мер по устранению причин и условий, способствующих информационной агрессии террористических и экстремистских организаций;
4. проведение совместных информационно-аналитических мероприятий;
5. оказание содействия в проведении информационно-аналитических мероприятий;
6. совместная подготовка и переподготовка кадров, повышение квалификации специалистов и стажировка представителей государственных органов;
7. обмен информацией, результатами научных исследований и опытом практической деятельности;
8. организация научных семинаров и иных научных мероприятий;
9. проведение совместных научных и научно-технических исследований;
10. обмен техническими разработками;
11. совершенствование правового обеспечения противодействия терроризму на объектах топливно-энергетического комплекса;
12. оказание взаимной правовой помощи в соответствии с международными договорами государств;
13. обмен методическими разработками.

5. Контроль и надзор в сфере противодействия терроризму на объектах топливно-энергетического комплекса

5.1. Государственный контроль в сфере противодействия терроризму на объектах топливно-энергетического комплекса

Государственный контроль в сфере противодействия терроризму на объектах топливно-энергетического комплекса осуществляется государственными органами, осуществляющими противодействие терроризму на объектах топливно-энергетического комплекса, посредством проведения плановых и внеплановых проверок антитеррористической защищенности объектов топливно-энергетического комплекса на основании решения руководителей данных государственных органов в соответствии с законодательством государства.

5.2. Надзор за законностью деятельности по противодействию терроризму на объектах топливно-энергетического комплекса

Надзор за исполнением законодательства в сфере противодействия терроризму на объектах топливно-энергетического комплекса осуществляют генеральный прокурор государства и подчиненные ему прокуроры в пределах своей компетенции.

Библиография

Руководящие принципы для государств-членов ООН по противодействию использованию новых и развивающихся технологий в террористических целях, доступ оп ссылке https://documents.un.org/doc/undoc/gen/n23/427/65/pdf/n2342765.pdf?token=wXjQs88uWTUysSOoLA&fe=true.

Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons.

Доклад ИДКТК о тенденциях "*Physical Protection of Critical Infrastructure against Terrorist Attacks*", 2017, доступ по ссылке https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted-trends-report-march-2017-final.pdf.

КТУ ООН – *Пять тематических модулей по защите уязвимых целей от террористических нападений*, 2022, доступ по ссылке https://www.un.org/counterterrorism/es/node/20481.

Руководства КТУ ООН (модули) по защите особо уязвимых целей от террористических нападений, в частности, *Защита уязвимых целей от террористических атак с использованием беспилотных летательных систем*, 2022, доступ по ссылке https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf.

Глобальный доклад о приобретении, оснащению и применению беспилотных авиационных систем негосударственными вооруженными группами в террористических целях, доступ по ссылке https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_car_global_report_web_en.pdf.

Использование беспилотных летательных систем негосударственными вооруженными группами, 2024, доступ по ссылке https://unidir.org/wp-content/uploads/2024/01/UNIDIR_Use_of_Uncrewed_Aerial_Systems_by_Non_State_Armed_Groups_Africa.pdf.

Оценка террористической угрозы: использование новых технологий в террористических целях*, 2023*, доступ по ссылке https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_conducting_terrorist_threat_web.pdf.

Marina Mitrevska, Toni Mileski, Robert Mikac (2019), *Critical infrastructure concept and security challenges*, доступ по ссылке https://cip-association.org/wp-content/uploads/2020/07/Chapter1.pdf.

Сборник ООН передовой практики по защите критически важных инфраструктур от террористических атак, 2022, доступ по ссылке https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf.

Резолюция Генеральной Ассамблеи ООН 63/210 (19 декабря 2008) Un Doc A/RES/63/210, доступ по ссылке https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F63%2F210&Language=E&DeviceType=Desktop&LangRequested=False.

Резолюция Генеральной Ассамблеи ООН 67/263 (17 мая 2013) Un Doc A/RES/67/263, доступ по ссылке https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F67%2F263&Language=E&DeviceType=Desktop&LangRequested=False.

Резолюция Генеральной Ассамблеи ООН 77/298 (22 июня 2023) Un Doc A/RES/77/298, доступ по ссылке https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F63%2F210&Language=E&DeviceType=Desktop&LangRequested=False.

Резолюция Генеральной Ассамблеи ООН 78/149 (19 декабря 2023) Un Doc A/RES/78/149, доступ по ссылке https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F67%2F263&Language=E&DeviceType=Desktop&LangRequested=False.

Резолюция Совета Безопасности ООН 1373 (28 сентября 2001) UN Doc S/RES/1373, доступ по ссылке https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1373(2001)&Language=E&DeviceType=Desktop&LangRequested=False.

Резолюция Совета Безопасности ООН 1540 (28 апреля 2004) UN Doc S/RES/1540, доступ по ссылке https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1540(2004)&Language=E&DeviceType=Desktop&LangRequested=False.

Резолюция Совета Безопасности ООН 2325 (15 декабря 2016) UN Doc S/RES/2325, доступ по ссылке https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2325(2016)&Language=E&DeviceType=Desktop&LangRequested=False.

Резолюция Совета Безопасности ООН 2341 (13 февраля 2017) UN Doc S/RES/2341, доступ по ссылке https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2341(2017)&Language=E&DeviceType=Desktop&LangRequested=False.

Резолюция Совета Безопасности ООН 2370 (2 августа 2017) UN Doc S/RES/2370, доступ по ссылке https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2370(2017)&Language=E&DeviceType=Desktop&LangRequested=False.

Резолюция Совета Безопасности ООН 2396 (21 декабря 2017) UN Doc S/RES/2396, доступ по ссылке https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2396(2017)&Language=E&DeviceType=Desktop&LangRequested=False.

Совет Безопасности ООН *Письмо от 28 декабря 2018 от Председателя Комитета СБ ООН, учрежденного резолюцией 1373 (2001) по контртерроризму в адрес Председателя СБ ООН (28 декабря 2018)* UN Doc S/2018/1177, доступ по ссылке https://undocs.org/Home/Mobile?FinalSymbol=S%2F2018%2F1177&Language=E&DeviceType=Desktop&LangRequested=False.

Понимание вызова

Ahmad J., Shahid A., Reuters (2023), *Islamist militants in Pakistan kill six at oil and gas production site*, доступ по ссылке https://www.reuters.com/world/asia-pacific/islamist-militants-kill-six-gas-oil-extraction-plant-pakistan-2023-05-23/.

Al-Qaeda's North Africa branch claims attack on Algerian gas plant, Reuters, 2016, доступ по ссылке https://www.reuters.com/article/idUSKCN0WL0AM/.

На основе статистики из отчетов «Лаборатории Касперского» об основных инцидентах в области безопасности промышленных информационно-коммуникационных технологий за 2020, 2021, 2022, 2023 годы, доступ по ссылке: https://ics-cert.kaspersky.com/publications/reports/.

Bell, Alison & Rogers, Brooke & Pearce, Julia. (2018). *The Insider Threat: Behavioral indicators and factors influencing likelihood of intervention*. International Journal of Critical Infrastructure Protection. 24. 10.1016/j.ijcip.2018.12.001. Доступ по ссылке https://www.researchgate.net/publication/329419966_The_Insider_Threat_Behavioral_indicators_and_factors_influencing_likelihood_of_intervention.

Digitalisation – Essential for Energy System Transformation. But What About Communications? 12 June 2023, доступ по ссылке https://www.techuk.org/resource/digitalisation-essential-for-energy-system-transformation-but-what-about-communications-guest-blog-by-grid-scientific-limited.html.

Digitalisation, International Energy Agency, доступ по ссылке https://www.iea.org/energy-system/decarbonisation-enablers/digitalisation.

Digitalisation of the energy system, доступ по ссылке https://energy.ec.europa.eu/topics/energy-systems-integration/digitalisation-energy-system_en.

Donya Fakhravar, Nima Khakzad, Genserik Reniers, Valerio Cozzani, *Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network, Process Safety and Environmental Protection*, Volume 111, 2017, Pages 714-725, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2017.08.036, доступ по ссылке https://www.sciencedirect.com/science/article/abs/pii/S0957582017302914.

Energy sector faces 39% of critical infrastructure attacks, Security, доступ по ссылке https://www.securitymagazine.com/articles/99915-energy-sector-faces-39-of-critical-infrastructure-attacks.

Gambrell J., *Saudi Arabia: Drone attacks knocked out half its oil supply*, AP News, 2019, доступ по ссылке https://apnews.com/article/d20f80188e3543bfb36d512df7777cd4.

Gas pipeline in Egypt's Sinai attacked, Israel imports unaffected, Al Jazeera, 2020, доступ по ссылке https://www.aljazeera.com/economy/2020/2/3/gas-pipeline-in-egypts-sinai-attacked-israel-imports-unaffected.

Gökçe Küçük, *Daesh attacks oil facilities in Libya*, 2019, доступ по ссылке https://www.aa.com.tr/en/energy/energy-security/daesh-attacks-oil-facilities-in-libya/26031.

James A. Piazza, *Oil and Terrorism: An Investigation of Mediators*, Public Choice 169 (2016): 251–68, https://doi.org/10.1007/s11127-016-0357-0.

Keystone Pipeline System, доступ по ссылке https://www.tcenergy.com/operations/oil-and-liquids/keystone-pipeline-system/.

Лаврухин, М. *Терроризм в энергетической промышленности*. Энергетическая политика, том 179, 2023. стр. 24-37, доступ по ссылке https://doi.org/10.46920/2409-5516.2023_1179.24.

Law enforcement capabilities framework for new technologies in countering terrorism, UNOCT, UNCCT, INTERPOL, доступ по ссылке: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_law_enforecement_capabilities_web2.pdf.

Lee, Chia-yi. (2022). *Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructure*. Energy Research & Social Science. 87. 102459. 10.1016/j.erss.2021.102459.

Libya: National Oil Corporation's Tripoli offices attacked, Al Jazeera, 2018, доступ по ссылке https://www.aljazeera.com/news/2018/9/10/libya-national-oil-corporations-tripoli-offices-attacked.

Manar Alanazi, Abdun Mahmood, Mohammad Jabed Morshed Chowdhury, *SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues*, Computers & Security, Volume 125, 2023, 103028, ISSN 0167-4048, DOI: 10.1016/j.cose.2022.103028, доступ по ссылке https://www.sciencedirect.com/science/article/pii/S0167404822004205.

Multi-Billion Dollar Opportunities in Cross-Border Cooperation for Oil and Natural Gas Projects in Southern Africa, доступ по ссылке https://energychamber.org/multi-billion-dollar-opportunities-in-cross-border-cooperation-for-oil-and-natural-gas-projects-in-southern-africa/.

New Danish rules on screening and approval of foreign investments, MAGNUSSON, доступ по ссылке https://www.magnussonlaw.com/news/new-danish-rules-on-screening-and-approval-of-foreign-investments/.

ОБСЕ Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства, доступ по ссылке https://www.osce.org/files/f/documents/7/5/103954.pdf.

Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS), 2022, доступ по ссылке: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf

Prodan T., "Maritime Terrorism and Resilience of Maritime Critical Infrastructure", National Security and the Future, 1-2/18 (2017), p. 103. pp. 103-122.

Sonangol Suffers Attempted Cyber-Attack, Business Elites Africa, 2019: https://businesselitesafrica.com/sonangol-suffers-attempted-cyber-attack/?v=04c19fa1e772.

Syria says pipeline blast was terrorist attack, U.S. suspects IS, Reuters, 2020, доступ по ссылке https://www.reuters.com/article/us-syria-blast-electricity/explosion-on-syria-gas-pipeline-a-terrorist-attack-minister-idUSKBN25K062/.

James A. Piazza, "*Oil and Terrorism: An Investigation of Mediators*," Public Choice 169 (2016): 251–68, https://doi.org/10.1007/s11127-016-0357-0.

The attack against Danish, critical infrastructure, 2023, доступ по ссылке https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf.

The Global Terrorism Database™ (GTD), доступ по ссылке https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=202012240006.

"*The In Amenas Attack, Report of the Investigation into the Terrorist Attack on In Amenas*," Statoil, February 2013, доступ по ссылке www.statoil.com/en/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf.

Thomas G. Pledger, *The Role of Drones in Future Terrorist Attacks*, доступ по ссылке https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf.

Tichý, Lukáš. (2019). *Energy Infrastructure as a Target of Terrorist Attacks from the Islamic State in Iraq and Syria*. International Journal of Critical Infrastructure Protection. 25. 10.1016/j.ijcip.2019.01.003

Toft, Peter & Duero, Arash & Bi, Ar. (2010). *Terrorist targeting and energy security*. Energy Policy. 38. 4411-4421. 10.1016/j.enpol.2010.03.070.

Total declares force majeure on Mozambique LNG after insurgent attacks, Reuters, 2021: https://www.reuters.com/world/africa/frances-total-declares-force-majeure-mozambique-lng-project-2021-04-26/.

TotalEnergies, Mozambique LNG: TotalEnergies' response, 2023, доступ по ссылке https://totalenergies.com/media/news/press-releases/mozambique-lng-totalenergies-response.

Trans-European Networks for Energy, 2020, доступ по ссылке https://energy.ec.europa.eu/topics/infrastructure/trans-european-networks-energy_en.

Wang L., Wang X., Zhao Q., Zhao Y. *Multi-objective policing emergency logistics scheduling on multi-location coordinated terrorist attacks*, 2017, Xitong Gongcheng Lilun yu Shijian/System Engineering Theory and Practice. 37, доступ по ссылке https://www.researchgate.net/publication/322482361_Multi-objective_policing_emergency_logistics_scheduling_on_multi-location_coordinated_terrorist_attacks.

Взгляд в глубину: использование террористами и насильственными экстремистами Dark Web и Cybercrime-as-a-Service (киберпреступности как услуги) в целях осуществления кибератак, опубликовано UNICRI и КТУ/КТЦ ООН (Глобальная программа по борьбе с терроризмом в области кибербезопасности и новых технологий).

Алгоритмы и терроризм: Злоумышленное использование искусственного интеллекта в террористических целях, опубликовано UNICRI и КТУ/КТЦ ООН (Глобальная программа по борьбе с терроризмом в области кибербезопасности и новых технологий).

Национальные подходы к снижению связанных с терроризмом рисков для КВЭИ: роль участников и передовой опыт

Act of 1 July 2011 on the security and protection of critical infrastructure, available at https://crisiscentrum.be/sites/default/files/documents/files/2021-03/PDFsam_15_2.pdf.

Anti-terrorism exercises were held at an oil and gas facility in Dagestan (Дагестане на нефтегазовом объекте прошли антитеррористические учения), AiF-Dagestan (АиФ-Дагестан), 2020: https://dag-aif-ru.turbopages.org/turbo/dag.aif.ru/s/society/v_dagestane_na_neftegazovom_obekte_proshli_antiterroristicheskie_ucheniya.

Bimo, Prabaswari, *Protecting critical infrastructure from cyberthreats*, The Jakarta Post, 2023, available at https://www.thejakartapost.com/paper/2023/08/09/cybersecurity-strategy-for-indonesias-critical-infrastructure-protection.html.

Christer Pursiainena, Eero Kytömaa, *From European critical infrastructure protection to the resilience of European critical entities: what does it mean?* Sustainable and Resilient Infrastructure 2023, VOL. 8, Pages 85–101, https://doi.org/10.1080/23789689.2022.2128562 available at https://www.tandfonline.com/doi/epdf/10.1080/23789689.2022.2128562?needAccess=true.

Commercial facilities as targets: New threats to critical infrastructures, Social Value Creation Report, NEC, 2016, available at https://sg.nec.com/en_SG/pdf/brochures/PublicSafety/SocialValueCreationReport_en_Vol.1.pdf.

Community Resilience Planning Guide for Buildings and Infrastructure System, available at https://crsreports.congress.gov/product/pdf/R/R47666.

Donya Fakhravar, Nima Khakzad, Genserik Reniers, Valerio Cozzani, *Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network*, Process Safety and Environmental Protection, Volume 111, 2017, Pages 714-725, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2017.08.036, available at https://www.sciencedirect.com/science/article/abs/pii/S0957582017302914.

Doran M., *New cyber offences for targeting key infrastructure, reporting of ransomware attacks made mandatory*, ABC News, 2021, available at https://www.abc.net.au/news/2021-10-13/government-will-mandate-business-reporting-ransomware-attacks/100534890.

Early Warning System for the Kuwait Oil Company, Telegrafia, 2017, available at https://www.electronic-sirens.com/success-story-early-warning-system-kuwait-oil-company/.

Energy Sector Regulatory Framework, Abu Dhabi Government, Department of Energy, available at: https://www.doe.gov.ae/en/Legislation-and-Compliance/Laws-and-Regulations.

Federal law of the Russian Federation № 256 from 26 July 2011 “On security of energy infrastructure”, available at https://base.garant.ru/12188188/.

Handbook for Implementing the Principles for Resilient Infrastructure, UNDRR, 2020, available at https://www.undrr.org/media/87213/download?startDownload=20240612.

Handbook For Implementing the Principles for Resilient Infrastructure, UNDRR, 2023, available at https://www.undrr.org/media/87213.

Information security regulation in industrial control systems used in the energy sector (Enerji sektöründe kullanilan endüstriyel kontrol sistemlerinde bilişim güvenliği yönetmeliği), 2017, available at: https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm.

Infrastructure Codes, Standards, and Regulations: Frequently Asked Questions, 2023, available at: https://sgp.fas.org/crs/misc/R47666.pdf.

KRITIS-Sektor definition Energie, available at: https://www.openkritis.de/it-sicherheitsgesetz/sektor_energie.html.

Melkunaite, Laura & Giroux, Jennifer, *Information Sharing for Critical Energy Infrastructure Protection: Finding value & overcoming challenges*. NATO Energy Security Centre of Excellence, 2013, available at: https://www.researchgate.net/publication/281584950_Information_Sharing_for_Critical_Energy_Infrastructure_Protection_Finding_value_overcoming_challenges.

Nereim V., *Aramco and Saudi navy start exercises to thwart drone and missile attacks*, World Oil, 2021, available at: https://www.worldoil.com/news/2021/3/22/aramco-and-saudi-navy-start-exercises-to-thwart-drone-and-missile-attacks.

Política Nacional de Defensa, Brazil, available at: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf.

Política Nacional de Segurança de Infraestruturas Críticas, DECRETO Nº 9.573, DE 22 DE NOVEMBRO DE 2018, available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm.

Order of the Minister of Economy, Commerce and Business Environment no. 1.178 of 6 June 2011, available at: https://cncpic.mai.gov.ro/en/sectoare/energetic.

OSCE, *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*, Vienna, 2013, available at: www.osce.org/atu/103500?download=true.

Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastructure državnega pomena v Republiki Sloveniji, 2012.

PRESS RELEASE: *Power system stress test: Federal Ministry for Economic Affairs and Climate Action stepping up precautionary measures to safeguard power grid stability this winter*, German Federal Ministry for Economic Affairs and Climate Action, 2022, available at: https://www.bmwk.de/Redaktion/EN/Pressemitteilungen/2022/09/20220905-power-system-stress-test.html.

Resolution of the Government of Kazakhstan on approval of the Rules and criteria for classifying objects as vulnerable to terrorism.

Security strategy of the Czech Republic, 2023, available at: https://mzv.gov.cz/file/5119429/MZV_BS_A4_brochure_WEB_ENG.pdf.

Strategic Environmental Assessment on the Development of a Petroleum Hub in Ghana, available at: https://www.phdc.gov.gh/documents/SEA%20for%20Petroleum%20Hub%20-%20Main%20Technical%20Report.pdf.

Subsecretaría de protección civil y abordaje integral de emergencias y catástrofes (1/2015), available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242082/norma.htm.

The Japanese Cybersecurity Policy for CIP, June 2022 (revised March 2024), available at: https://www.nisc.go.jp/eng/pdf/cip_policy_2024_eng.pdf.

The Petroleum Act, The United Republic of Tanzania, 2015, available at: https://www.ewura.go.tz/wp-content/uploads/2020/04/The-Petroleum-Act-2015-1.pdf.

UK's Public summary of sector security and response plan, 2018, available at: https://assets.publishing.service.gov.uk/media/5c8a7845ed915d5c1456006a/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf.

UK's Sector Security and Resilience Plans, available at: https://www.gov.uk/government/collections/sector-resilience-plans.

Valentin Weber, Maria Pericàs Riera, Emma Laumann, *Mapping the World's Critical Infrastructure Sectors*, 2023, available at: https://dgap.org/en/research/publications/mapping-worlds-critical-infrastructure-sectors.

Yao, Xijun & Wei, Hsi-Hsien & Shohet, Igal & Skibniewski, Miroslaw. (2020). *Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation*. Applied Sciences. 10. 7162. 10.3390/app10207162, available at: https://www.researchgate.net/publication/346227204_Assessment_of_Terrorism_Risk_to_Critical_Infrastructures_The_Case_of_a_Power-Supply_Substation.

Zakon o kritičnim infrastrukturama NN 56/13, 114/22, 2022, available at: https://www.zakon.hr/z/591/Zakon-o-kritičnim-infrastrukturama.

Международные усилия по защите КВЭИ

Акт от 1 июля 2011 по безопасности и защите критической инфраструктуры, доступ по ссылке https://crisiscentrum.be/sites/default/files/documents/files/2021-03/PDFsam_15_2.pdf.

Anti-terrorism exercises were held at an oil and gas facility in Dagestan (в Дагестане на нефтегазовом объекте прошли антитеррористические учения), AiF-Dagestan (АиФ-Дагестан), 2020: https://dag-aif-ru.turbopages.org/turbo/dag.aif.ru/s/society/v_dagestane_na_neftegazovom_obekte_proshli_antiterroristicheskie_ucheniya.

Bimo, Prabaswari, *Protecting critical infrastructure from cyberthreats*, The Jakarta Post, 2023, доступ по ссылке https://www.thejakartapost.com/paper/2023/08/09/cybersecurity-strategy-for-indonesias-critical-infrastructure-protection.html.

Christer Pursiainena, Eero Kytömaa, *From European critical infrastructure protection to the resilience of European critical entities: what does it mean?* Sustainable and Resilient Infrastructure, 2023, VOL. 8, стр. 85–101, https://doi.org/10.1080/23789689.2022.2128562 доступ по ссылке https://www.tandfonline.com/doi/epdf/10.1080/23789689.2022.2128562?needAccess=true.

Commercial facilities as targets: New threats to critical infrastructures, Social Value Creation Report, NEC, 2016, доступ по ссылке https://sg.nec.com/en_SG/pdf/brochures/PublicSafety/SocialValueCreationReport_en_Vol.1.pdf.

Community Resilience Planning Guide for Buildings and Infrastructure System, доступ по ссылке https://crsreports.congress.gov/product/pdf/R/R47666.

Donya Fakhravar, Nima Khakzad, Genserik Reniers, Valerio Cozzani, *Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network*, Process Safety and Environmental Protection, Volume 111, 2017, Pages 714-725, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2017.08.036, доступ по ссылке https://www.sciencedirect.com/science/article/abs/pii/S0957582017302914.

Doran M., *New cyber offences for targeting key infrastructure, reporting of ransomware attacks made mandatory*, ABC News, 2021, доступ по ссылке https://www.abc.net.au/news/2021-10-13/government-will-mandate-business-reporting-ransomware-attacks/100534890.

Early Warning System for the Kuwait Oil Company, Telegrafia, 2017, доступ по ссылке https://www.electronic-sirens.com/success-story-early-warning-system-kuwait-oil-company/.

Energy Sector Regulatory Framework, Abu Dhabi Government, Department of Energy, доступ по ссылке: https://www.doe.gov.ae/en/Legislation-and-Compliance/Laws-and-Regulations.

Федеральный закон от 21 июля 2011 г. N 256-ФЗ "О безопасности объектов топливно-энергетического комплекса", доступ по ссылке: https://base.garant.ru/12188188/.

Handbook for Implementing the Principles for Resilient Infrastructure, UNDRR, 2020, доступ по ссылке https://www.undrr.org/media/87213/download?startDownload=20240612.

Handbook For Implementing the Principles for Resilient Infrastructure, UNDRR, 2023, доступ по ссылке https://www.undrr.org/media/87213.

Information security regulation in industrial control systems used in the energy sector (Enerji sektöründe kullanilan endüstriyel kontrol sistemlerinde bilişim güvenliği yönetmeliği), 2017, доступ по ссылке: https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm.

Infrastructure Codes, Standards, and Regulations: Frequently Asked Questions, 2023, доступ по ссылке: https://sgp.fas.org/crs/misc/R47666.pdf.

KRITIS-Sektor definition Energie, доступ по ссылке: https://www.openkritis.de/it-sicherheitsgesetz/sektor_energie.html.

Melkunaite, Laura & Giroux, Jennifer, *Information Sharing for Critical Energy Infrastructure Protection: Finding value & overcoming challenges*. NATO Energy Security Centre of Excellence, 2013, доступ по ссылке: https://www.researchgate.net/publication/281584950_Information_Sharing_for_Critical_Energy_Infrastructure_Protection_Finding_value_overcoming_challenges.

Nereim V., *Aramco and Saudi navy start exercises to thwart drone and missile attacks*, World Oil, 2021, доступ по ссылке: https://www.worldoil.com/news/2021/3/22/aramco-and-saudi-navy-start-exercises-to-thwart-drone-and-missile-attacks.

Política Nacional de Defensa, Brazil, доступ по ссылке: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf.

Política Nacional de Segurança de Infraestruturas Críticas, DECRETO Nº 9.573, DE 22 DE NOVEMBRO DE 2018, доступ по ссылке: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm.

Order of the Minister of Economy, Commerce and Business Environment no. 1.178 of 6 June 2011, доступ по ссылке: https://cncpic.mai.gov.ro/en/sectoare/energetic.

Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства, Вена, 2013, доступ по ссылке: www.osce.org/atu/103500?download=true.

Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastructure državnega pomena v Republiki Sloveniji, 2012.

ПРЕСС-РЕЛИЗ: *Power system stress test: Federal Ministry for Economic Affairs and Climate Action stepping up precautionary measures to safeguard power grid stability this winter*, German Federal Ministry for Economic Affairs and Climate Action, 2022, доступ по ссылке: https://www.bmwk.de/Redaktion/EN/Pressemitteilungen/2022/09/20220905-power-system-stress-test.html.

Постановление Правительства Республики Казахстан «Об утверждении Правил и критериев отнесения объектов к объектам, уязвимым в террористическом отношении».

Стратегия безопасности Чешской Республики, 2023, доступ по ссылке: https://mzv.gov.cz/file/5119429/MZV_BS_A4_brochure_WEB_ENG.pdf.

Strategic Environmental Assessment on the Development of a Petroleum Hub in Ghana, доступ по ссылке: https://www.phdc.gov.gh/documents/SEA%20for%20Petroleum%20Hub%20-%20Main%20Technical%20Report.pdf.

Subsecretaría de protección civil y abordaje integral de emergencias y catástrofes (1/2015), доступ по ссылке: http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242082/norma.htm.

The Japanese Cybersecurity Policy for CIP, June 2022 (revised March 2024), доступ по ссылке: https://www.nisc.go.jp/eng/pdf/cip_policy_2024_eng.pdf.

The Petroleum Act, The United Republic of Tanzania, 2015, доступ по ссылке: https://www.ewura.go.tz/wp-content/uploads/2020/04/The-Petroleum-Act-2015-1.pdf.

UK's Public summary of sector security and response plan, 2018, доступ по ссылке: https://assets.publishing.service.gov.uk/media/5c8a7845ed915d5c1456006a/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf.

UK's Sector Security and Resilience Plans, доступ по ссылке: https://www.gov.uk/government/collections/sector-resilience-plans.

Valentin Weber, Maria Pericàs Riera, Emma Laumann, *Mapping the World's Critical Infrastructure Sectors*, 2023, доступ по ссылке: https://dgap.org/en/research/publications/mapping-worlds-critical-infrastructure-sectors.

Yao, Xijun & Wei, Hsi-Hsien & Shohet, Igal & Skibniewski, Miroslaw. (2020). *Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation*. Applied Sciences. 10. 7162. 10.3390/app10207162, доступ по ссылке: https://www.researchgate.net/publication/346227204_Assessment_of_Terrorism_Risk_to_Critical_Infrastructures_The_Case_of_a_Power-Supply_Substation.

Zakon o kritičnim infrastrukturama NN 56/13, 114/22, 2022, доступ по ссылке:

https://www.zakon.hr/z/591/Zakon-o-kritičnim-infrastrukturama.

Защита инфраструктуры возобновляемых и нетрадиционных источников энергии

Belgium evacuates nuclear plant staff after attacks, CBS news, доступ по ссылке: https://www.cbsnews.com/news/belgium-attacks-evacuation-tihange-nuclear-plant-staff-isis-dirty-bomb.

Breach at Kudankulam nuclear plant may have gone undetected for over six months, доступ по ссылке: https://economictimes.indiatimes.com/news/politics-and-nation/breach-at-kudankulam-nuclear-plant-may-have-gone-undetected-for-over-six-months-group-ib/articleshow/79412969.cms?from=mdr.

Ex-Ontario Power Generation employee accused of sharing information with foreign entity or terrorist group, Power Engineering, 2024, доступ по ссылке: https://www.power-eng.com/news/ex-ontario-power-generation-employee-accused-of-sharing-information-with-foreign-entity-or-terrorist-group/#gref.

How rotating wing turbine blades impact the Nexrad Doppler weather radar, Radar Operations Center, 2022, доступ по ссылке: https://www.roc.noaa.gov/wsr88d/windfarm/turbinesimpacton.aspx.

Japan's Nuclear Infrastructure: Risks and Mitigation Strategies, 2023, доступ по ссылке: https://www.democracylab.uwo.ca/research/current_research/Japan-Report.pdf.

Johnson Jay, *Roadmap for Photovoltaic Cyber Security*, Report number: SAND2017-13262, 2017, доступ по ссылке: https://www.researchgate.net/publication/322568290_Roadmap_for_Photovoltaic_Cyber_Security.

Nuclear security in India, 2015, доступ по ссылке: https://www.orfonline.org/wp-content/uploads/2015/02/NUCLEAR_SECURITY_IN_INDIA.pdf.

Police data management and analysis (Radiological and Nuclear), INTERPOL, доступ по ссылке: https://www.interpol.int/Crimes/Terrorism/Radiological-and-Nuclear-terrorism/Our-response-to-radiological-and-nuclear-terrorism.

Siciliano J., *FBI joins investigation into alleged terror attack on Las Vegas solar plant*, S&P Global, 2023, доступ по ссылке: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/fbi-joins-investigation-into-alleged-terror-attack-on-las-vegas-solar-plant-73776901.

Staggs, Jason & Ferlemann, David & Shenoi, Sujeet. (2017). *Wind farm security: Attack surface, targets, scenarios and mitigation*. International Journal of Critical Infrastructure Protection. 17. 10.1016/j.ijcip.2017.03.001, доступ по ссылке: https://www.researchgate.net/publication/315590797_Wind_farm_security_Attack_surface_targets_scenarios_and_mitigation.

The Civil Nuclear Constabulary (CNC), доступ по ссылке: https://www.gov.uk/government/organisations/civil-nuclear-constabulary/about.

Update on cyber security incident, The Nordex Group, 2022, доступ по ссылке: https://www.nordex-online.com/en/2022/04/update-on-cyber-security-incident/.

Анализ практических примеров

Канадская ресурсная инфраструктура Nexus (CRIRN)

Energy infrastructure security division, доступ по ссылке: https://natural-resources.canada.ca/sites/nrcan/files/science-and-data/science-research/cyber-security/eisd-booklet-en.pdf.

Практический пример - компьютерные командно-штабные учения «Eternity-2023»

“Eternity-2023” computer-assisted Command and Staff Exercises held in Baku ended, Ministry of Defence of Azerbaijan, 2023, доступ по ссылке: https://mod.gov.az/en/news/eternity-2023-computer-assisted-command-and-staff-exercises-held-in-baku-ended-video-49709.html.

Анализ практических примеров - субъекты КВЭИ в Турции

The Regulation on Information Security of Industrial Systems Used in the Energy Sector, 13 July 2017, доступ по ссылке: https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm.

Анализ практических примеров - Рекомендации Комиссии ЕС 2019/553 по кибербезопасности в энергетическом секторе

Commission Recommendation (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector (notified under document C(2019) 2400), EUR-Lex, 2019, доступ по ссылке: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019H0553.

Анализ практических примеров - Департамент охраны стратегических трубопроводов МВД Грузии (SPPD)

Источник: https://police.ge/en/ministry/structure-and-offices/strategiuli-milsadenebis-datsvis-departamenti?sub=9658.

Анализ практических примеров - Национальная система Ганы предупреждения и противодействия насильственному экстремизму и терроризму (NAFPCVET)

Национальная система Ганы предупреждения и противодействия насильственному экстремизму и терроризму, 29 января 2020, доступ по ссылке: https://www.peacecouncil.gov.gh/storage/2019/09/NAFPCVET-Document-29-Jan-2020.pdf.

Анализ практических примеров - Центр обучения и демонстрации в области физической ядерной безопасности МАГАТЭ

Центр обучения и демонстрации в области физической ядерной безопасности (NSTDC), Международного агентства по атомной энергии, доступ по ссылке: https://www.iaea.org/about/organizational-structure/department-of-nuclear-safety-and-security/division-of-nuclear-security/iaea-nuclear-security-training-and-demonstration-centre.

Анализ практических примеров - Индонезийское ГЧП в защите энергетических объектов от террористических атак

Укрепление безопасности национального критически важного объекта Пертамина – ВМС Индонезии проводят учения по реагированию на чрезвычайные ситуации, Пертамина, 2023 г., доступ по ссылке: https://www.pertamina.com/en/news-room/news-release/strengthening-security-of-national-vital-object-pertamina-indonesian-navy-conducts-emergency-drill.

Анализ практических примеров - Международные совместные учения «ADMM-Plus Maritime Security Field Training Exercise»

ADMM-Plus Maritime Security Field Training Exercise, MINDEF Сингапур, 2019, доступ по ссылке: https://www.mindef.gov.sg/web/wcm/connect/mindef/14d67a7b-f7a4-473c-958b-0ae2093590a0/Infographic.pdf?MOD=AJPERES&CVID=mGI0R7G.

Анализ практических примеров - Совместные антитеррористические учения АТЦ СНГ

Совместные антитеррористические учения государств - участников СНГ «Каспий-Антитеррор - 2021», АТЦ СНГ, 2021, доступ по ссылке: https://eng.cisatc.org/1289/133/161/9077.

Анализ практических примеров - Нефтяная полиция Ирака

Знакомство с системой обеспечения безопасности в Ираке: агентства и их задачи, июль 2020 г., отчет ORSAM, доступ по ссылке: https://orsam.org.tr/d_hbanaliz/understanding-the-security-bureaucracy-in-iraq-agencies-and-their-tasks.pdf.

Анализ практических примеров – Комитет по защите нефти и критической инфраструктуры Совета сотрудничества стран Персидского залива (Саудовская Аравия, Кувейт, Объединенные Арабские Эмираты, Катар, Бахрейн и Оман)

Двенадцатое: образование и обучение в области безопасности, Совет сотрудничества арабских государств Персидского залива, доступ по ссылке: https://www.gcc-sg.org/en-us/CooperationAndAchievements/Achievements/SecurityCooperation/Achievements/Pages/Twelftheducationandsecuritytra.aspx.

Анализ практических примеров – Меры обеспечения физической безопасности на проекте Восточноафриканского нефтепровода (EACOP) в Уганде

Проект Восточноафриканского нефтепровода, доступ по ссылке: https://eacop.com/overview.

Отчет о воздействии проекта строительства Восточноафриканского нефтепровода на окружающую среду и социальную сферу, Уганда, 2019 г., доступ по ссылке: https://www.eia.nl/projectdocumenten/00009498.pdf.

Анализ практических примеров – ГЧП в защите КВЭИ в Алжире

Алжир выделяет 400 млн долларов на защиту нефтяных объектов от терроризма, Asharq Al Awsat, 2023, доступ по ссылке: https://english.aawsat.com/home/article/4102616/algeria-allocates-400-mln-protect-oil-facilities-against-terrorism.

Анализ практических примеров – Подход Туркменистана к межведомственной координации в сфере защиты природного газа от террористических атак

Гарантии надежности и безопасности, Государственное информационное агентство Туркменистана, 2013, доступ по ссылке: https://turkmenistan.gov.tm/ru/post/19819/garantii-nadezhnosti-i-bezopasnosti.

Анализ практических примеров – План протокола безопасности трубопроводов и восстановления после аварий в США

План протокола безопасности трубопроводов и восстановления после аварий, Министерство национальной безопасности, 2010, доступ по ссылке: https://www.tsa.gov/sites/default/files/pipeline_sec_incident_recvr_protocol_plan.pdf.

Инструменты

Инструмент – Лаборатория моделирования ИКТ-рисков на критически важных объектах нефтегазового комплекса **(РГУ имени И.М. Губкина)**

В РГУ им. И. М. Губкина создана учебная лаборатория по изучению отражения компьютерных атак, доступ по ссылке: https://en.gubkin.ru/news/university-life/the-training-laboratory-to-study-computer-attack-detention-was-established-at-gubkin-university/.

Инструмент – АТЦ СНГ 2019 Методические рекомендации по организации взаимодействия между органами безопасности, специальными службами и правоохранительными органами государств-участников СНГ в обеспечении антитеррористической защиты критической энергетической инфраструктуры

Материалы сбора руководящего состава органов безопасности и специальных служб государств-участников СНГ: Сборник материалов– М.: Издательство «Принт Торг», 2019. – 362 с.

Инструмент – Моделирование атак при разработке сценария угроз

Жадиков Р.С., Бекжанов М.А. *Организация системы антитеррористической защиты объектов, уязвимых в террористическом отношении: науч.-практ. пособие.* Алматы. Академия Комитета национальной безопасности Республики Казахстан, 2018. 104 стр.

Инструмент – Сведения о КВЭИ

Информация о критической энергетической/электрической инфраструктуре, Федеральная комиссия по регулированию энергетики США, доступ по ссылке: https://www.ferc.gov/ceii.

Sarah G. Freeman, Matthew A. Kress-Weitenhagen, Jake P. Gentle, Megan J. Culler, Megan M. Egan, Remy V. *Stolworthy Attack Surface of Wind Energy Technologies in the United States*, 2024, доступ по ссылке https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf?utm_medium=email&utm_source=govdelivery.

Инструмент – Руководство ОБСЕ по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства

ОБСЕ 2013, *Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства*, 2013, доступ по ссылке: www.osce.org/atu/103500?download=true.

Инструмент – Управление информацией о физической безопасности (PSIM)

Инструмент PSIM «Система физической защиты компании Итерация», доступ по ссылке https://iter.ru/en/TERATION_PHYSICAL_PROTECTION_SYSTEM.pdf.

Инструмент – модель метода анализа риска «ВСК».

Rongchen Zhu, Xiaofeng Hu, Yiping Bai, Xin Li, *Risk analysis of terrorist attacks on LNG storage tanks at ports*, Safety Science Volume 137, May 2021, 105192, доступ по ссылке: https://www.sciencedirect.com/science/article/abs/pii/S0925753521000370.

Инструмент – Сертификат безопасности («паспорт безопасности») критически важных объектов энергетики как часть управления рисками в Азербайджане, Казахстане, Российской Федерации

Постановление от 10 ноября 2022 г. N 2034 «Об утверждении Правил разработки и формы паспорта безопасности критически важного объекта», доступ по ссылке: https://base.garant.ru/405693779/.

Правовое обеспечение безопасности объектов топливно-энергетического комплекса: опыт СНГ), 2022, доступ по ссылке: https://gubkin.ru/faculty/faculty-of-complex-safety-of-the-fuel-and-energy-complex/kafedry-i-podrazdeleniya/knb/files/metod_materialy/prav_obespech_obj_tek.pdf.

Об утверждении типового паспорта антитеррористической защищенности объектов, уязвимых в террористическом отношении, 2023, доступ по ссылке: https://adilet.zan.kz/rus/docs/V2300032950.

www.un.org/counterterrorism/vulnerable-targets

КОНТРТЕРРОРИСТИЧЕСКОЕ УПРАВЛЕНИЕ
ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ