

Защита важнейших объектов энергетической инфраструктуры от террористических актов

Сентябрь 2010

Тематический обзор № 2/2010 Антитеррористического подразделения (АТП)

“ЭФФЕКТИВНОЕ СОТРУДНИЧЕСТВО МЕЖДУ ГОСУДАРСТВАМИ-УЧАСТНИКАМИ ПО ЗАЩИТЕ ЖИЗНЕННО ВАЖНОЙ ЭНЕРГЕТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ОТ ТЕРРОРИСТИЧЕСКИХ АКТОВ БУДЕТ СПОСОБСТВОВАТЬ УКРЕПЛЕНИЮ БЕЗОПАСНОСТИ И СТАБИЛЬНОСТИ В РЕГИОНЕ ОБСЕ”, РЕШЕНИЕ СОВЕТА МИНИСТРОВ ОБСЕ NO.6/07 (30 НОЯБРЯ 2007)

Основное содержание

Данный Тематический обзор обобщает основные рекомендации по защите важнейших объектов энергетической инфраструктуры, выработанные в ходе Экспертного семинара ОБСЕ 2010 года с участием государственного и частного секторов.

Риск нападений со стороны террористов и прочих негосударственных структур на важнейшие объекты энергетической инфраструктуры растет. Нарушение работы или разрушение таких объектов инфраструктуры могло бы оказать серьезное влияние на здоровье, сохранность, безопасность или экономическое благополучие граждан. Страны должны произвести пересмотр уязвимых мест, в плане безопасности, своих энергетических инфраструктур и своих стратегий для решения данной проблемы.

Странам рекомендуется следовать данному подходу, основанному на регулярной оценке всех рисков, с учетом уязвимых мест в киберпространстве. Их подход должен быть направлен на снижение рисков до приемлемого уровня, в то же время, имея своей окончательной целью обеспечить устойчивость всей инфраструктуры и надежность энергоснабжения. Поступая подобным образом, государства должны гибко совмещать меры по предотвращению, защите и обеспечению готовности к нападениям, при этом они должны опираться на эффективное сотрудничество (межведомственное, между государственным и частным секторами, международное).

Контекст

Энергетическая безопасность, включая безопасность энергетической инфраструктуры, является одним из серьезнейших вызовов безопасности и экономике, как сегодня, так и в будущем. Наравне с экономическим ростом и социаль-

ным развитием, происходящим во всем мире, также растет и значение энергии и инфраструктуры, обеспечивающей производство и поставки энергии.

В последние годы международное сообщество уделяло особое внимание защите важнейших объектов энергетической инфраструктуры (ВОЭИ) от террористов. Ключевой целью для многих террористов является нанесение максимального экономического ущерба и дезорганизация жизни общества. Поэтому ВОЭИ, занимающиеся производством топлива, которое поддерживает рост мировой экономики и работу нашего общества, являются потенциальными идеальными целями для террористов.

Реальность террористической угрозы ВОЭИ часто обсуждается, в особенности владельцами и субъектами частного сектора. В общем, понятно то, что террористические акты, совершаемые в отношении ВОЭИ, представляют собой риски с низкой вероятностью осуществления, но с масштабными последствиями. Тем не менее, существуют признаки наличия угрозы нападений со стороны негосударственных структур в отношении энергетических инфраструктур, а также в них все еще существуют уязвимые места, несмотря на предпринятые усилия по повышению безопасности ВОЭИ. Такие угрозы и уязвимые места не должны оставаться без внимания, но, в то же время, страны не могут позволить себе чрезмерную реакцию в данном отношении.

Защита ВОЭИ от террористических нападений является особенно важным вопросом для ОБСЕ, в ряды государств-участников которой входят государства, являющиеся крупнейшими производителями и потребителями энергии, а также стратегические страны транзита энергии. В ноябре 2007 года государства-участники ОБСЕ приняли решения Совета министров иностранных дел по *Защите важнейших объектов энергетической инфраструктуры от террористических нападений* [[MC.DEC/6/07](#)], в соответствии с которым они взяли на себя обязательства по поддержанию

ТЕМАТИЧЕСКИЙ ОБЗОР

Антитеррористическое подразделение (АТП) ОБСЕ

взаимного сотрудничества и рассмотрению всех необходимых мер на национальном уровне, в целях обеспечения должного уровня защиты ВОЭИ от террористических нападений.

ОБСЕ провела *Экспертный семинар по вопросам государственно-частного партнерства в области защиты ядерной энергетической инфраструктуры от террористических актов* в период 11-12 февраля 2010 в Вене, на котором присутствовало 200 участников из 50 стран, 12 международных структур, и 30 организаций, представляющих частный сектор. На данном семинаре был выработан ряд стратегических рекомендаций, которые были включены в Концептуальную записку. Данные рекомендации не подразумевают обязательного признания государствами-участниками и Секретариатом ОБСЕ.

Рекомендации

1. Следовать комплексному подходу, основанному на оценке рисков.

Важность, уязвимые места и факторы риска для объектов энергетической инфраструктуры варьируют в отношении различных инфраструктур, стран, а также с течением времени. Меры по защите энергетической инфраструктуры должны предприниматься динамично и основываться на регулярно обновляемой оценке всех рисков, с учетом целого ряда антропогенных (случайных или злонамеренных) и природных рисков, а не только с учетом угрозы терроризма. Данная оценка должна включать в себя зависимости и взаимосвязи, существующие между секторами (например, транспортным сектором и сектором информационных технологий), а также между странами. На основе оценки рисков, меры по предотвращению, защите и обеспечению готовности к нападениям должны быть совмещены надлежащим образом, в целях снижения рисков до приемлемого уровня.

2. Расширять рамки многостороннего сотрудничества.

Комплексный подход к защите ВОЭИ, как указано выше, требует скоординированного участия большого количества заинтересованных сторон из различных государственных ведомств (например, министерств энергетики, внутренних дел/безопасности, окружающей среды, обороны), государственного и частного секторов, а также заинтересованных сторон за рубежом. Усилия должны быть направлены, на ранней стадии, на разработку стратегии защиты ВОЭИ, в целях укрепления диалога, взаимопонимания и формулировок, доверия и обмена ценной информацией. Усилия по содействию сближению/гармонизации подходов к оценке рисков и назначения важнейших объектов энергетической инфраструктуры должны стимулировать многостороннее сотрудничество. Странам следует изучить, какие из существующих и новых мер окажутся наиболее приемлемыми для продвижения сотрудничества на различных уровнях, в каждом соответствующем случае.

3. Разрабатывать гибкие меры по обеспечению безопасности, гарантирующие защиту на мини-

мальном надлежащем уровне. Уязвимые места и факторы риска для каждого ВОЭИ являются специфическими и динамичными; и при обеспечении их защиты необходимо принимать во внимание данный момент, чтобы она была соизмерима с рисками и экономически эффективна. Меры по обеспечению безопасности должны быть адаптированы к каждой инфраструктуре и идеально «встроены» в инфраструктуру в соответствии с планом. Меры могут реализовываться для того, чтобы одновременно служить различным целям, связанным с охраной труда, промышленной и общей безопасностью и охраной окружающей среды. Безопасность должна быть «соизмерима» с планами по наращиванию (либо уменьшению) мер, в зависимости от последней степени риска. Но «базовые» меры безопасности должны согласовываться, поскольку ВОЭИ жизненно важны для общества, и минимальные, преимущественно международные, стандарты безопасности должны обеспечивать равные условия для субъектов экономической деятельности, а также согласованность с оными, действующими за рубежом. В то время как затраты на обеспечение безопасности входят в обязанности по соблюдению осторожности владельцев и/или субъектов экономической деятельности и стратегию бесперебойной деятельности, существует необходимость обсудить инициативы и распределение расходов.

4. Уделять больше внимания обеспечению готовности к нападениям и общей устойчивости.

Возможность нарушения работы, случайного или нет, не может быть исключена полностью, поэтому существует необходимость гарантировать надежность инфраструктуры посредством обеспечения готовности к нападениям и управления последствиями. Обеспечение готовности к нападениям требует заблаговременного планирования действий в чрезвычайных ситуациях, проведения испытаний и учений, включая планы по поддержанию связи с общественностью/потребителями и энергетическими рынками. Страны могли бы рассмотреть возможность учреждения специализированных ведомств, обладающих возможностями быстрого реагирования/восстановления инфраструктуры. В отношении устойчивости, существует необходимость увеличения инвестирования в объединение сетей энергосистем и развитие альтернативных маршрутов, а также в целях наращивания мощностей по хранению/стратегическим резервам. Обеспечение общей устойчивости и надежности энергоснабжения требует рассмотрения прочих вопросов энергетической безопасности, помимо вопросов касательно инфраструктуры, таких как энергетическая солидарность, диверсификация энергетической структуры, диверсификация поставщиков энергии.

5. Определить и устранить уязвимые места энергетического сектора в киберпространстве.

На сегодняшний день, в мире, все более компьютеризируемом и зависимом от ИКТ, традиционных мер физической безопасности («пистолеты, решетки и стражи порядка») уже недостаточно. Необходимо в значительной мере повысить уровень общественной и корпоративной осведомлен-

ТЕМАТИЧЕСКИЙ ОБЗОР

Антитеррористическое подразделение (АТП) ОБСЕ

ности и понимания вопросов кибербезопасности, а также должно поощряться развитие специальных навыков в вопросах обеспечения кибербезопасности. Оценка кибербезопасности должна стать неотъемлемой частью оценки рисков инфраструктуры, в частности в отношении энергетического сектора (например, в отношении рынков, управления процессами инфраструктуры, систем эффективного энергоснабжения). Страны должны создать возможности реагирования на чрезвычайные ситуации в киберпространстве на национальном уровне и эффективную международную базу, в целях более успешного реагирования на чрезвычайные ситуации в киберпространстве.

6. Развивать эффективное государственно-частное партнерство (ГЧП). Сегодня большинством ВОЭИ владеют или управляют, полностью или частично, представители частного сектора. Соответственно, необходимо четко определить роли и обязанности заинтересованных сторон в частном секторе и органов государственной власти в области обеспечения энергетической безопасности. Но каждая сторона может извлекать пользу для себя при выполнении своей роли, оказывая поддержку другой стороне; эффективное обеспечение безопасности, в особенности готовности к нападениям, требует тесной, отработанной координации. Таким образом, должна быть обеспечена платформа для налаживания и поддержания диалога между государственным и частным секторами (возможно при помощи институциональных механизмов), которая позволит построить доверие, необходимое для своевременного и взаимного обмена ценной информацией между заинтересованными сторонами государственного и частного секторов. Партнерство может развиваться в целях осуществления единой оценки безопасности ВОЭИ, пересмотра мер безопасности, разработки планов действий в чрезвычайных ситуациях и подготовки к реагированию на инциденты. Более того, ГЧП помогает усилить поддержку тех сообществ, на территории которых расположены ВОЭИ, в целях укрепления превентивной безопасности, посредством создания заинтересованности сообществ в целостности инфраструктуры.

7. Укрепление трансграничного/ международного сотрудничества. Безопасность энергетической инфраструктуры и задачи по обеспечению энергетической стабильности на сегодняшний день приобретают значительные, все увеличивающиеся, международные масштабы. Национальные энергосистемы все более взаимосвязаны, а по всему миру строится все большее количество новых трансграничных нефтегазовых трубопроводов. Последствия нарушения работы одной энергетической инфраструктуры могут распространиться далеко за пределы национальных границ страны, где она расположена, будь

то прекращение поставок или другое повреждение, включая нанесение экономического (например, рост цен на нестабильных рынках сбыта энергии) или экологического ущерба. Страны должны критически рассмотреть такие прямые и косвенные зависимости, что должно повлечь за собой обоснованную заинтересованность в сотрудничестве, в целях обеспечения целостности энергетических инфраструктур. Существует ряд вариантов по укреплению трансграничного и международного сотрудничества, включая обмен (конфиденциальной) информацией, развитие стандартов безопасности, сотрудничество при чрезвычайных ситуациях (например, техническая поддержка, помощь в энергоснабжении); их преимущества должны быть рассмотрены странами и международным сообществом.

Возможная роль ОБСЕ

ОБСЕ, с ее уникальным составом участников, в который входят государства всего евразийского континента, и с ее всеобъемлющим подходом к обеспечению безопасности, с 2007 года уполномочена содействовать обмену успешной практикой и своевременному обмену информацией по защите ВОЭИ.

ОБСЕ, в координации с прочими соответствующими организациями, выражает готовность, по запросу государств, оказывать содействие в плане повышения осведомленности о проблемах и успешной практике, связанных с ВОЭИ, формирования стратегии защиты ВОЭИ, улучшения межведомственной координации, развития ГЧП, укрепления трансграничного сотрудничества, в особенности, посредством проведения семинаров на региональном и субрегиональном уровне, учений с воссозданием реальной ситуации, а также оказания консультативной/технической поддержки.

Контактная информация

Для получения более подробной информации, пожалуйста, свяжитесь с сотрудниками АТП ОБСЕ, работающим по программе обеспечения защиты важнейших объектов энергетической инфраструктуры:

Reinhard.Uhrig@osce.org or Mehdi.Knani@osce.org

Action against Terrorism Unit (ATU)
OSCE Secretariat
Wallnerstrasse 6
A-1010 Vienna, Austria
Tel: +43 1 514 36 6702
atu@osce.org
osce.org/atu

Организация по безопасности и сотрудничеству в Европе (ОБСЕ) работает во имя стабильности, процветания и демократии в 56 государствах путем политического диалога на темы общих ценностей и путем практических действий, обеспечивающих долговременные перемены к лучшему.