январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Материалы по организациям и

Правительства
- Г-н Стивен Калдвел, Счетная Палата Правительства США, LINK
- Д-р Феликс Кванема, Natural Resources Canada, LINK
-Разведывательная служба Румынии, LINK
- Министерство внутренних дел Республики Грузии, LINK

Международные структуры
- Г-н Хосе Хойос Перез, Европейская Комиссия, LINK
- Полковник Андрей Новиков, Антитеррористический центр Содружества Независимых Государств (АТЦ СНГ), LINK

Научно-исследовательские институты
- Д-р Хейко Борхерт и г-жа Карина Форстер, Международная сеть по связям с общественностью, LINK
- Г-жа Дженнифер Жиру, Центр по исследованиям вопросов безопасности (CSS), LINK
- Проф. Вольфганг Крёгер, Швейцарский федеральный институт технологий (ETH) в Цюрихе, LINK
- Д-р Кевин Роснер, Институт анализа глобальной безопасности, LINK
- Д-р Франк Умбах, Центр европейских стратегий безопасности (CESS), LINK

Предприятия/компании
- Д-р Брюс Аврилл, Strategic Energy Security Solutions LLC, LINK
- Г-н Дэвид Бейкер, IOActive, LINK
Г-н Умберто Сакконе, начальник службы безопасности, ENI spa, LINK
Г-н Дэвид Тейлор-Смит, G4S, LINK

Контактную информацию об авторах статей в настоящем Специальном бюллетене можно получить в Антитеррористическом подразделении ОБСЕ

Материалы по темам

Оценка угроз
- Г-жа Дженнифер Жиру, Центр по исследованиям вопросов безопасности (CSS), LINK
- Разведывательная служба Румынии, LINK

Национальные подходы
- Д-р Феликс Кванема, Natural Resources Canada, LINK
- Министерство внутренних дел Республики Грузии, LINK

Региональное сотрудничество
- Г-н Хосе Хойос Перез, Европейская Комиссия, LINK
- Полковник Андрей Новиков, Антитеррористический центр Содружества Независимых Государств (АТЦ СНГ), LINK
- Д-р Кевин Роснер, Институт анализа глобальной безопасности, LINK

Государственно-частное партнерство
- Д-р Брюс Аврилл, Strategic Energy Security Solutions LLC, LINK
- Д-р Хейко Борхерт и г-жа Карина Форстер, Международная сеть по связь с общественностью, LINK
- Г-н Дэвид Тейлор-Смит, G4S, LINK

Защита нефтегазовой инфраструктуры
- Г -н Стивен Калдвел, Счетная Палата Правительства США, LINK
- Г -н Умберто Сакконе, начальник службы безопасности, ENI spa, LINK
- Министерство внутренних дел Республики Грузии, LINK

Защита инфраструктуры электроснабжения
- Г-н Дэвид Бейкер, IOActive, LINK
- Проф. Вольфганг Крёгер, Швейцарский федеральный институт технологий (ETH) в Цюрихе, LINK

Кибер безопасность
- Г-н Дэвид Бейкер, IOActive, LINK
- Д-р Франк Умбах, Центр европейских стратегий безопасности (CESS), LINK

➲ Контакты

Райнхард Уриг
Советник по антитеррористическим вопросам
Reinhard.Uhrig@osce.org

Мэди Кнани
Младший сотрудник по программам (Редактор Бюллетеня)
Mehdi.Knani@osce.org

Tel: +43 1 514 36 6702
Fax: +43 1 514 36 6687
E-mail: atu@osce.org
www.osce.org/atu

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Слово редактора

Значимость энергетической безопасности и безопасности энергетической инфраструктуры не может быть переоценена. Она относится к наиболее серьезным вопросам безопасности и экономики как сегодня, так и в будущем. Вместе с ростом экономик стран мира и развитием общества, возрастает и значимость сектора энергетики. Так же, как и значимость объектов инфраструктуры, которые производят и поставляют энергию.

В последние годы повышается внимание со стороны международного сообщества к защите важнейших объектов энергетической инфраструктуры (ВОЭИ) от террористов, с полным на то правом. Основной целью для увеличивающегося числа террористов является нанесение максимального экономического ущерба и общественной дестабилизации. И поскольку ВОЭИ предоставляют топливо, приводящее глобальную экономику в движение и заставляющее наши общества работать, наша зависимость от этих объектов инфраструктуры становится идеальной мишенью для терроризма.

Реальность террористической угрозы ВОЭИ часто обсуждается, в особенности собственниками и операторами частного сектора. Но существует явное доказательство той степени ущерба, который могут нанести теракты объектам энергетической инфраструктуры. И, несмотря на все предпринимаемые усилия, все еще существуют уязвимые места. Защита ВОЭИ от террористических актов является вопросом, особенно важным для ОБСЕ, в 56 государств-участников которой входят некоторые крупнейшие производители и потребители энергии, а также стратегические транзитные страны.

Государства-участники ОБСЕ приняли в ноябре 2007 года Решение Совета министров о защите важнейших объектов энергетической инфраструктуры от террористических актов [MC.DEC/6/07], согласно которому они обязуются сотрудничать и рассматривать все необходимые меры на государственном уровне для обеспечения соответствующей защиты ВОЭИ от террористических атак.

В соответствии с решением, Антитеррористическое подразделение ОБСЕ (АТП) организует 11-12 февраля 2010 года в Вене, по инициативе Соединенных Штатов Америки, *Экспертный семинар по вопросам государственно-частного партнерства в области защиты неядерной энергетической инфраструктуры от террористических актов* [см. пригласительный пакет, представленный 17 ноября 2009 года, SEC.GAL/188/09, и памятку, представленную 19 января 2010 года, SEC.GAL/8/10].

Цель настоящего Специального Бюллетеня CTN – упростить обмен информации и мотивировать размышления в преддверии данного предстоящего семинара. Страны-участницы, через свои КТС контакты в ОБСЕ, получили просьбы представить статьи, а также была выражена просьба к ряду международных структур, представителям частного сектора и исследователям поделиться своими взглядами.

Материалы, полученные АТП и собранные в данном Специальном Бюллетене, предназначены для предоставления пищи для размышления по различным вопросам в области защиты ВОЭИ от террористических атак, в том числе:

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

- Методологии оценки рисков, в том числе определение *важнейших* объектов инфраструктуры и взаимозависимостей;
- Физические и кибер уязвимости ВОЭИ и соответствующие профилактические и подготовительные меры;
- Национальные подходы, возможности и мероприятия;
- Необходимость в государственно-частных партнерствах (ГЧП);
- Возможности для трансграничного и международного сотрудничества;
- Возможный вклад международных структур, и, в частности, ОБСЕ [в этом отношении см. отчет Генерального Секретаря ОБСЕ, SEC.GAL/202/08].

Безопасность ВОЭИ представляет проблемы в плане угроз, которые стоят перед нами, и возможности в плане того, как мы можем реагировать на эти угрозы. АТП с большим нетерпением ждет работы с вами Безопасность ВОЭИ представляет проблемы в плане угроз, которые стоят перед нами, и возможности в плане того, как мы можем реагировать на эти угрозы. АТП с большим нетерпением ждет работы с вами в этой области. Пожалуйста, можете обращаться к нам для обмена информацией и идеями о возможных инициативах по защите ВОЭИ от террористических актов. Надеюсь, что вам понравится Специальный Бюллетень, Надеюсь, что вам понравится Специальный Бюллетень,

С уважением,

Рафаель Ф. Перл
Начальник антитеррористического подразделения ОБСЕ

ОБСЕ

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Морская инфраструктура: проблемы при защите топливно-энергетических танкеров

Г-н Стивен Л. Калдвел, Директор по вопросам морской безопасности
Счетная Палата Правительства США (GAO)

Значимость топливно-энергетических танкеров для экономик многих стран

Многие развитые страны сильно зависят от судов-танкеров при импорте нефти, газа и прочих энергоносителей из-за рубежа. Эта уже экстенсивная зависимость от импортируемых энергоносителей, по прогнозам, будет расти, в некоторых случаях значительно. Например, прогнозируется, что импорт сжиженного природного газа (СПГ) в Соединенные Штаты увеличится более чем на 400 процентов к 2015 году. Транспортировка этих зачастую опасных энергоносителей по морю осуществляется посредством глобальной цепи поставок, зарождающейся в ряде государств на Среднем Востоке, Африке, Латинской Америке и странах Карибского бассейна (в зависимости от энергоносителей), и заканчивающейся в различных развитых странах в Европе, Северной Америке и Азии. Транспортировка данных энергоносителей также осуществляется на танкерах, принадлежащих многим различным компаниям, а также по маршрутам международных вод, которые не контролирует ни одно правительство. Всего зарегистрировано более 3000 танкеров сырой нефти и свыше 200 танкеров СПГ.

Наличие множества угроз в отношении топливно-энергетических танкеров

Цепочка поставок посредством топливно-энергетических танкеров, являясь жизненно важной, также уязвима в плане атак со стороны террористов и пиратов. Портовые терминалы (как в странах-отправителях, так и в странах назначения) являются, по существу, уязвимыми, поскольку они должны предоставлять доступ по суше и морю, и поскольку они разрастаются зачастую неподалеку от оживленных центров населенных пунктов. Также танкеры, перевозящие данную продукцию, являются уязвимыми, так как они плывут по прямым маршрутам, которые известны заранее, и определенную часть своих маршрутов им иногда приходится проплывать через узкие проливы (называемые «бутылочными горлами»), что не позволяет им совершать маневры в случае возможных атак. Поскольку задействовано так много различных участников, у террористов есть возможность «пробовать» систему поставок на поиск слабого звена. Несмотря на наличие насыщенной охраны, террористы предпринимали попытки (и в некоторых случаях успешно) атаковать топливно-энергетические танкеры и терминалы. Успешными примерами являются нападение на танкер *«Лимбург»* около Йемена в 2002 году, захват танкера *«Пенрайдер»* неподалеку от Малаккского пролива в 2003 году, нападение на морские терминалы вблизи Ирака в 2004 году, и штурм газового терминала в Нигерии в 2006 году. Помимо атак террористов, в последнее время проводят успешные захваты танкеров и пираты, например, танкеров *«Сириус Стар»* и *«Лонгчамп»* около Сомали.

Как показали выше указанные примеры, существует несколько видов атак на танкеры, которые могут иметь серьезные последствия. Наиболее тревожными являются сценарии суицидных нападений (удар и взрыв боковины танкера), атак без входа в зону поражения (запуск ракеты или прочего оружия в танкер), или вооруженных штурмов (взятие на абордаж и захват танкера). Другими возможными видами нападений могут быть сговор команды и столкновения с другими судами, управляемыми террористами. Хотя нападений на топливно-энергетические танкеры и терминалы было мало, успешные атаки могут иметь существенные общественные, экологические и экономические последствия, которые будут различаться в зависимости от энергоносителей.

«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 № 6/07***

Например, легко воспламеняемые продукты, например, СПГ, могут загореться или, возможно, взорваться. Менее воспламеняемые продукты, такие как сырая нефть, могут нанести ущерб окружающей среде, поскольку они не рассеиваются, а ликвидация последствий может стоить дорого. Наконец, экономические последствия крупного нападения могут включать в себя временный резкий скачок цен, отражающий страх дальнейших атак и сбоев в поставках. В то время как потеря одного танкера может не иметь значительных последствий, если атака приводит к закрытию порта на несколько дней или недель, то ценовая реакция и более высокие издержки могут означать потери в экономическом благосостоянии для потребителей, компаний и правительств, выражаемые в миллиардах долларов.

Реализация основных мер безопасности

Многое делается, как на международном, так и на государственном уровне, для защиты топливно-энергетических танкеров и портовых сооружений от нападений. Международная морская организация и ее Кодекс ISPS устанавливают основные требования к морской безопасности. Правительства стран и операторы терминалов предпринимают такие действия, как повышение физической безопасности в портах и осуществление морского патрулирования. Например, порты сообщают о соответствии требованиям Кодекса ISPS, а операторы танкеров сообщают об укреплении своей безопасности во время погрузочных работ и в море. Много военно-морских сил патрулирует в водах, представляющих угрозу, например, в Персидском заливе и Аденском заливе. В Соединенных Штатах принимаются дополнительные меры помимо мер, требуемых Кодексом ISPS для защиты энергетической цепочки поставок. Эти меры включают в себя мониторинг прибытия танкеров и экипажей, посадку на борт избранных судов до того, как они зайдут в порт, сопровождение избранных танкеров в порт и обеспечение береговой охраной в топливно-энергетических терминалах. Кроме того, должностные лица, отвечающие за безопасность в портах, разработали планы реагирования на атаки и уменьшение последствий. Наконец, должностные лица проводят упражнения для тестирования своих операционных возможностей и своих панов реагирования. Эти упражнения помогают определять сильные и слабые стороны различных планов и способность множества организаций или сообществ реагировать на чрезвычайные ситуации, связанные с морской энергетической инфраструктурой.

Обеспечение безопасности все еще представляет проблемы

Несмотря на осуществляемые защитные меры, должностные лица по вопросам морской безопасности сталкиваются с постоянными проблемами при защите топливно-энергетических танкеров и соответствующей портовой инфраструктуры. Для танкеров, проходящих транзитом международные воды, основной проблемой является патрулирование длинных маршрутов и частые опасные зоны с очень ограниченным количеством военных кораблей. По портовой инфраструктуре, некоторым портам трудно соответствовать Кодексу ISPS. Посещения работниками GAO энергетических сооружений за рубежом показали, что у некоторых портов меры безопасности чрезмерны, а у некоторых портов имелись такие проблемы, как неохраняемые ворота и низкое ограждение. Прочие защитные меры, такие как посадка на борт и сопровождение танкеров, требуют дорогих ресурсов, таких как корабли и должным образом обученные работники правоохранительных органов. Порты также сталкиваются с проблемами при планировании и осуществлении реагирования на нападения на топливно-энергетические танкеры или терминалы. Часть проблемы заключается в том, что может быть много участников, отвечающих за планирование и исполнение различных компонентов реагирования, например, правоохранительные органы, органы охраны окружающей среды и противопожарные службы. И, опять же, ресурсы являются проблемой для многих из этих участников. В некоторых портах, например, у местных пожарных служб нет достаточного количества пожарных катеров или они недостаточно обучены

«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 № 6/07***

морскому пожаротушению. Наконец, учитывая проблемы с ресурсами, важно, чтобы решения, связанные с безопасностью, и мероприятия по защите танкеров и прочей морской инфраструктуры исполнялись в контексте управления рисками. Никакая сумма денег не может полностью защитить суда и порты от нападений врага, обладающего ресурсами и решимостью.

Примечание: *Статья основана на отчете: Морская безопасность: Федеральные попытки, необходимые для решения проблем при защите и реагировании на террористические атаки на танкеры с энергоносителями (GAO-08-141). См.* www.gao.gov/cgi-bin/getrpt?GAO-08-141 .

Фото: Служба береговой охраны США усиливает зону безопасности вокруг танкера СПГ (источник – GAO)

Защита важнейших объектов энергетической инфраструктуры от террористических актов: Канадский подход

Д-р Феликс Кванема, Директор/Специальный советник, безопасность энергетической инфраструктуры, энергетический сектор,
Natural Resources Canada (NRCan)

Система защиты объектов энергетической инфраструктуры Канады основана на трех фундаментальных и взаимосвязанных элементах.

Первый элемент – предотвращение; обеспечивающий хорошее понимание уязвимых сторон, обмен передовым опытом, и наличие лучшей информационной и коммуникационной сети для реагирования на риски, какими бы ни были источники, стихийные бедствия, злоумышленные атаки, внутренние угрозы и т.д. Второй элемент – реагирование во время чрезвычайной ситуации; способность своевременно и эффективно реагировать. Третий элемент – устойчивость; способность восстанавливать системы инфраструктуры или стратегические активы для возобновления топливно-энергетических поставок.

Основанием для системы является Национальная стратегия безопасности 2004 года, Обеспечение открытого общества: Национальная стратегия безопасности Канады; Закон об управлении чрезвычайными ситуациями 2007 года, и Программа 2008 года по выполнению Национальной стратегии и Плана действий по проекту отчета о жизненно важной инфраструктуре.

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Кроме того, существуют и другие аспекты, которые поддерживают систему. Энергетическая инфраструктура Канады является огромной, комплексной и переплетенной системой, включающей в себя нефть и газ, электроэнергию, производство гидроэнергии и прочие энергетические сооружения по всей стране; причем у каждого сектора своя специфика .

Объекты энергетической инфраструктуры также широко раскинуты географически и должны отвечать множеству подведомственных и законодательных требований. Существует также большое количество участников, включая собственников-операторов, агентств безопасности и разведки, инспекторов, представителей федеральных, провинциальных и территориальных департаментов, научных сообществ, промышленных ассоциаций и т.д.

Сообщество сектора энергетики и коммунального хозяйства – это форум, объединяющий всех участников энергетического сектора для обсуждения вопросов, представляющих общий интерес – обсуждение методологий по профилям риска, определение взаимозависимостей, программы управления чрезвычайными ситуациями и коммуникационные планы.

Другим важным аспектом канадского подхода является проведение два раз в год систематизированных заседаний по обмену информации на секретном уровне. Данные систематизированные брифинги посещает избранное число представителей собственников-операторов объектов энергетической инфраструктуры, промышленных ассоциаций и научных сообществ. Кроме того, Natural Resources Canada также проводит и иные заседания по информационному обмену на уровне «только для официального пользования».

Данные форумы предоставляют отличную возможность участникам энергетического сектора развивать доверительные отношения, что упрощает обмен соответствующей информацией, «не подлежащей оглашению», с пониманием того, что она не будет распространена.

Через партнерство с научными сообществами, Natural Resources Canada начала ряд исследований по стратегии в области защиты важнейшей инфраструктуры. Данные исследования внесли очень важный теоретический и эмпирический научный вклад в разработку стратегий.

Инициативы по защите важнейшей энергетической инфраструктуры также были подкреплены научным моделированием и аналитической работой, выполненной Канадской научно-исследовательской лабораторией взрывчатых веществ. Ученые и инженеры этой лаборатории также были членами многофункциональной группы экспертов, которая проводила оценку уязвимости и безопасности конкретных важнейших объектов энергетического сектора.

Таким образом, подход Канады к защите важнейших объектов энергетической инфраструктуры можно охарактеризовать как «комплексный, активный, совместный и информационный», основанный на стратегии национальной безопасности, законодательстве и регулировании. Он охватывает всех основных участников. Обмен важной информацией, в том числе систематизированные брифинги для тех, «кому необходимо знать», является основой системы. Вся осуществляемая аналитическая и стратегическая экспертиза подкрепляется научным моделированием и анализом, а также научными стратегическими исследованиями.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Управление рисками в процессе определения и защиты важнейшей инфраструктуры, как основной фактор региональной стабильности и безопасности

Разведывательная служба Румынии (SRI)

Мировое торговое экономическое развитие, формируемое ускоренным прогрессом технологий и поразительным влиянием глобализации, показало тесную взаимосвязь систем, обеспечивающих безопасность и благосостояние общества.

> *Необходимость во взаимосвязи систем, связанная с мировыми тенденциями в направлении к устранению административных барьеров, доступу к развивающимся рынкам и интеграции инфраструктурных систем – мотивирует изменения в отношении всемирной безопасности и стабильности.*

Объем асимметричных рисков, которые, вероятно, увеличатся в будущем, отражает роль и значимость важнейшей инфраструктуры как **существенного** элемента (оборудование, установки, чертежи, транспортные сооружения и т.д.), **организационного** элемента (транспортные системы, энергетические системы, производство и распределение нефти и продуктов природного газа и т.д.), а также **информационного** элемента (информационные потоки и передача данных, процедуры и т.д.), которые являются жизненно важными для соответствующей социальной жизни и поддерживают экономическое развитие в условиях стабильности и безопасности.

> *Ее слабая сторона – увеличение значения данного показателя усиливается значимостью обслуживаемой системы, в основном, уровнем защиты от угроз – представляет собой ключевую область стратегий и политик безопасности.*

Сложность защиты жизненно важной инфраструктуры определила связь стратегий, инициированных на государственном уровне и на уровне крупных альянсов, с необходимостью определять и повышать ее уровни безопасности, как **элемента, реагирующего на угрозы**, а также как основного **носителя внутренних/внешних угроз.**

Определение и идентификация важнейшей инфраструктуры

Инфраструктура (как отдельный элемент или целиком) может считаться **жизненно важной** с точки зрения ее **уникального статуса** и **дополняющего характера** в рамках системы, ее основной **роли** в обеспечении стабильности, осуществимости, безопасности, эксплуатации и безопасности в целом, ее повышенной **незащищенности** в отношении прямых угроз, а также тех угроз, направленных на процессы, компонентом которых она является, или с точки зрения особых **слабых сторон** в плане изменения состояния и, в особенности, внезапных изменений фактического положения дел.

> ***Критерии классификации*** *возникают из отраслевого/межотраслевого воздействия и обладают следующими* ***элементами оценки****:* ***физический*** *(или критерий этого, если среди прочих сооружений, размер, разбросанность, износостойкость, надежность),* ***функциональный*** *(или роль критерия - что «составляет» эту инфраструктуру),* ***безопасность*** *(что является безопасной инфраструктурой, оцениваемой в плане*

«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 № 6/07***

последствий, которые могут получены из-за нарушения основных условий), ***гибкость*** *(которая показывает, что существует определенная динамика и гибкость в плане важнейших объектов инфраструктуры, некоторые из них включены в категорию, когда они могут стать общественными при определенных условиях, жизненно важными объектами инфраструктуры и наоборот),* ***непредсказуемость*** *(то, что выглядит обычным или специальным объектом может стать контекстуальным важнейшим объектом инфраструктуры) и т.д.*

Таким образом, защита жизненно важной инфраструктуры представляет огромный интерес в развитии, связанном с глобализацией, поскольку задача по определению рисков, слабых сторон, угроз и опасных ситуаций, связанных с ними (*в основном, из-за религиозных убеждений, или вследствие террористических актов и экстремальных погодных условий*), является определяющей, вместе с инициацией предотвращения и контрмер, направленных на обеспечение безопасной и стабильной среды.

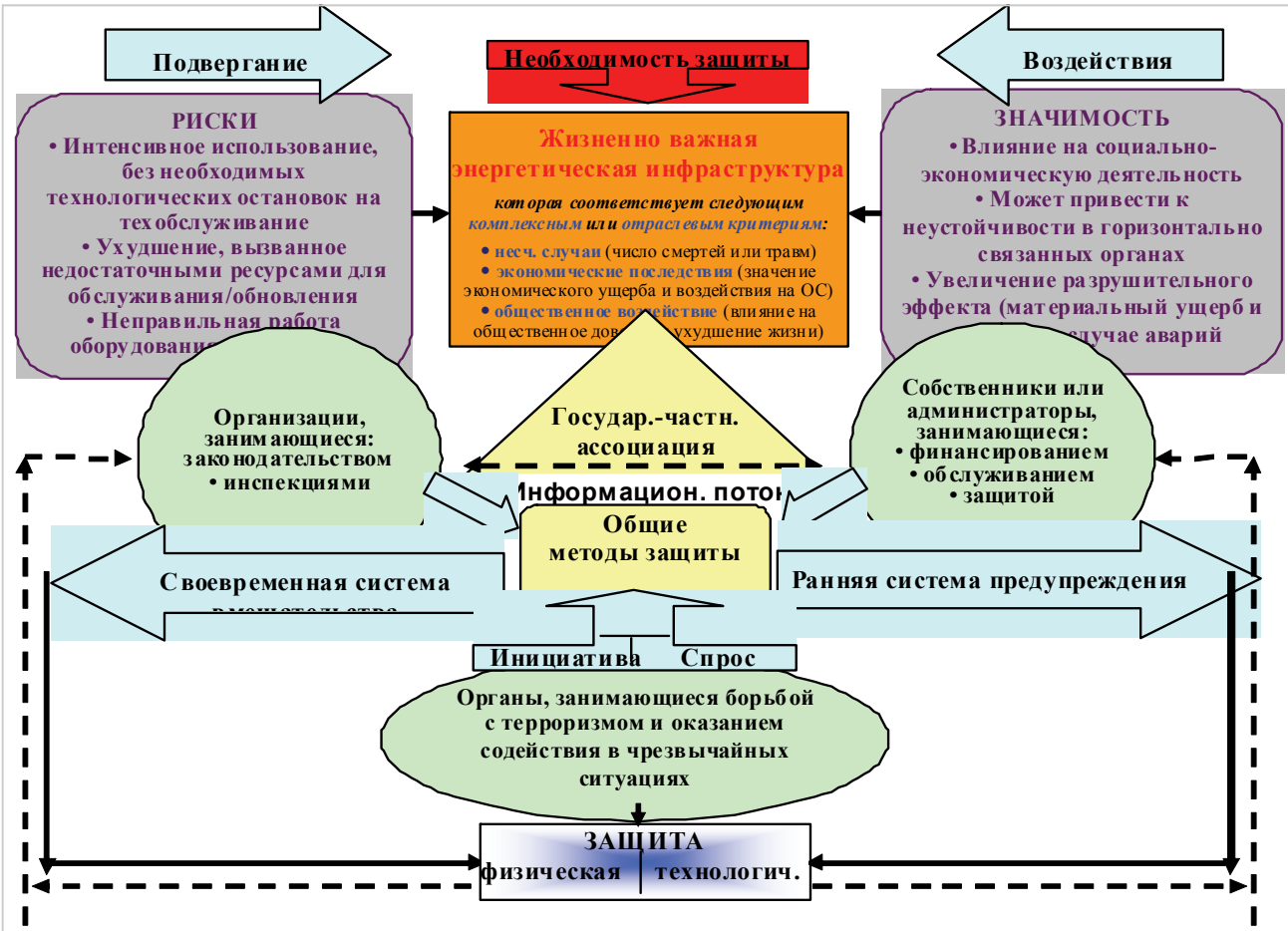
Риски, связанные с важнейшей инфраструктурой в энергетическом секторе

С учетом роста терроризма в мире, важнейшая инфраструктура в области энергетики заслуживает особого внимания, поскольку она может являться потенциальной мишенью для террористических групп, вследствие огромных последствий, которые могут иметь место (**на мультинациональном/ межгосударственном уровне**, из-за взаимосвязи компонентов). Кроме того, вопрос обозначения важнейшей инфраструктуры становится очень значительным, учитывая растущее число сбоев в работе инфраструктуры (в том числе отключения), экстремальных погодных условий и несанкционированных вторжений.

Соответствующие риски	Формы	Последствия
Интенсивное использование, без необходимых технологических остановок на техобслуживание **Состояние ухудшения,** вызванное недостаточным распределением ресурсов для техобслуживания/ремонта или для обновления физически и морально устаревшего оборудования **Неправильная эксплуатация** оборудования и установки, вызванная человеческой ошибкой **Отсутствие мер безопасности/ защиты**	• **Применение определенной практики, в основном** ориентированной на максимизацию прибыли, без учета реальной мощности установки • **Недостаточное участие** администраторов инфраструктуры в целях обеспечения сумм, необходимых для техобслуживания/ремонта/обновления • **Неправильное использование** оборудования и установки, вследствие человеческой ошибки или недостаточного числа обученного персонала • **Отсутствие координирования** между эксплуатацией и реальными технологическими требованиями установки • **Использование необученного персонала** для обеспечения безопасности/защиты, и неэффективное исполнение контрактных условий компаниями безопасности	● **Уменьшение пригодности оборудования**, ведущее к невозможности добиться расчетных технических параметров ● **Продолжительное ухудшение** оборудования и установки, что влияет на их функциональную безопасность ● **Порождение технических неполадок,** которые ведут к технологическим остановкам и сбоям в процессе, с негативными последствиями в плане попыток поддержания стабильной национальной/ региональной энергетической системы ● **Игнорирование роли,** которую играют эти важные элементы в плане достижения своих экономических задач ● **Аварии,** приводящие к существенному материальному ущербу и/или негативному воздействию на окружающую среду ● **Возможность несанкционированных** вторжений, в основном, с целью воровства

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***



Заключение

С точки зрения процесса и применимости, достижение задач, связанных с защитой жизненно важной инфраструктуры, имеет огромное значение в плане укрепления и межгосударственного, и институционального сотрудничества, а также оно имеет важный трансграничный подтекст, относящийся к созданию единой законодательной структуры, тесно связанной с сохранением экономических интересов и интересов безопасности, и к применению последовательных, интегрированных мер защиты.

Таким образом, начиная с глобального контекста рисков и интереса европейских организаций к вопросу (в соответствии с их национальными потребностями), крайне необходимо принять, на уровне каждого государства, систему комплексных мер, которая будет способна достичь, в конце концов, соответствия систем инфраструктуры требованиям по безопасной эксплуатации. Преследование данной цели является приоритетом, хотя это и подразумевает последовательные экономические и финансовые усилия (в результате определения, реабилитации, модернизации и защиты объекта инфраструктуры), и более усиленное общение между государственным и частным сектором.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. Marian, Rizea; Mariana, Marinică; Alexandru, Barbăsură; Lucian, Dumitrache; Cătălin, Ene, *Protecția infrastructurilor critice în spațiul euroatalantic*, Editura ANI, Bucureşti, 2008;
2. МакЛафлин, Дж..; Колинсон, Р.; Паттен, Д., *Брифинг директоров – Анализ SWOT*, Business Hotline Publications Ltd., Лондон, 2000.
3. Минтцберг, Х.; Квинн, Дж. Б., *Процесс стратегии. Концепции, контексты, примеры*, Prentice Hall, Нью-Йорк, 1996.
4. Popescu, M. D., *Globalizarea şi dezvoltarea trivalentă*, Editura Expert, Bucureşti, 1999

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Трубопроводы на территории Грузии как компонент евро-атлантической энергетической инфраструктуры и вопрос их безопасности

Министерство внутренних дел Грузии

Трубопроводы, расположенные на территории Грузии (Баку-Тбилиси-Джейхан и Южно-кавказский трубопровод), являются частью важнейшей энергетической инфраструктуры западного, евро-атлантического региона. Традиционные угрозы и возможные риски в отношении этих трубопроводов обусловлены текущими процессами, происходящими на Южном Кавказе. Эта ситуация, в целом, влияет на мировой энергетический рынок и геополитическую среду кавказского региона, а также на внутренние и внешние дела Грузии, риски и угрозы для ее энергетической инфраструктуры. Многие страны евро-атлантического региона зависят от энергоресурсов, которые находятся в нестабильных регионах; следовательно, существуют различные факторы, которые могут повлиять на энергетическую безопасность:

1. Мировой энергетический рынок – согласно данным, предоставленным Международным энергетическим агентством (IEA), спрос на энергоресурсы увеличится на 50% в 2005-2030 гг.; то есть может ожидаться дефицит энергии. Эта проблема может также быть вызвана постоянными изменениями цен на энергетические ресурсы и продукты, а также нестабильной ситуацией на энергетическом рынке.
2. Опасность терактов и саботажа в отношении энергетической инфраструктуры. Такие действия могут привести к серьезным задержкам в поставке ресурсов на мировой рынок, тем самым увеличивая напряжение. По этой причине данный вид атак становится все более привлекательным для террористов. Грузия уже пострадала от таких атак, произведенных на ее территории:

   - Взрыв радиопередающей станции, обслуживающей нефтепровод вблизи села Чорчана в Грузии 17 ноября 2004 года. Угроза прихода групп боевиков с территорий, не контролируемых Правительством Грузии, и осуществления ими подрыва нефтепроводов все еще сохраняется;
   - 12 августа 2008 года, во время вооруженного конфликта в Грузии, был взорван нефтепровод Баку-Супса на 27-ом километре; также следует подчеркнуть, что это был первый прецедент, когда были использованы боевые тактические ракеты «Искандер» (согласно отчету НАТО - SS-26 Stone). Ракета типа SS-26 взорвалась на 26-ом километре нефтепровода. К счастью, она прошла мимо своей цели на расстоянии 40 метров;

     В результате спланированного нападения на нефтепровод, работа нефтепровода была приостановлена на определенный период времени.

План безопасности объекта энергетической инфраструктуры обычно формируется на основании средств и тактики, разработанной после идентификации, оценки и анализа рисков.

«Риск обычно определяется как коэффициент вероятности угрозы в отношении инфраструктуры, уязвимости этой инфраструктуры и ожидаемых последствий или воздействия на инфраструктуру, если эта угроза материализуется. Согласно данному утверждению, оценка риска включает в себя идентификацию возможного объекта, который может быть атакован, того, насколько успешной может быть атака, и какое потенциальное последствие она может иметь. Следовательно, система безопасности состоит из нескольких элементов: технологического; структурного; электронного и тактического.

Правильная, реалистичная оценка риска дает нам возможность установить соответствующий тактический элемент; используя правильные технические, структурные и электронные элементы во время формирования проекта и строительства объекта, можно избежать успешного нападения и потенциальных негативных последствий.

Специальный бюллетень CTN

январь 2010

Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

1 января 2006 года был сформирован Департамент стратегической защиты нефтепроводов (ДСЗН), и с этого времени он являлся одним из департаментов Министерства внутренних дел (МВД) Грузии.

Ввиду вышеуказанных угроз, деятельность ДСЗН основана на оперативных принципах антитеррористических групп. Группы патрулирования осуществляют следующие меры разведки и безопасности на маршрутах нефтепроводов и прилегающей территории:
Патрулирование территорий нефтепроводов 24 часа в сутки (обход и патрулирование на потенциальных негативных последствий.

1 января 2006 года был сформирован Департамент стратегической защиты нефтепроводов (ДСЗН), и с этого времени он являлся одним из департаментов Министерства внутренних дел (МВД) Грузии.

Ввиду вышеуказанных угроз, деятельность ДСЗН основана на оперативных принципах антитеррористических групп. Группы патрулирования осуществляют следующие меры разведки и безопасности на маршрутах нефтепроводов и прилегающей территории:

- Патрулирование территорий нефтепроводов 24 часа в сутки (обход и патрулирование на транспортных средствах);
- Контролирование подъездных дорог к нефтепроводам;
- Проверка и регистрация всех лиц и транспортных средств, проходящих по территории нефтепроводов;
- Скрытое наблюдение за территорией, прилегающей к нефтепроводам;
- Скорое и эффективное реагирование в случае чрезвычайной ситуации;
- Сбор разведывательной информации;

Оперативные действия в соответствии с Законом Грузии «Об оперативной разведывательной деятельности».
ДСЗН осуществляет свою деятельность в соответствии с законодательством Грузии, а именно: выполняя свои функции и обязанности, Департамент действует в соответствии со следующими правовыми нормами:

- Конституция Грузии;
- Закон Грузии о полиции;
- Закон Грузии об оперативной разведывательной деятельности;
- Нормативно-правовые акты МВД, утвержденные приказом № 614, изданным Министром внутренних дел Грузии 27 декабря;
- Нормативно-правовые акты Департамента стратегической защиты нефтепроводов МВД, утвержденные приказом Министра внутренних дел Грузии;
- Различные документы, утвержденные приказом руководителя Департамента стратегической защиты нефтепроводов МВД;
- Соглашение с государством-собственником недр, подписанное 18 ноября 1999 года;

В рамках программы НАТО, с сентября 2006 года, ежегодно в Анкаре (Турция) проводится международный курс «Eternity». Ежегодно в заседаниях принимают участие представители Министерств обороны и внутренних дел Азербайджана, Грузии и Турции.

Департамент стратегической защиты нефтепроводов поддерживает тесную связь с Жандармерией и Министерством обороны Турции, а также со Службой государственной охраны, Министерством государственной безопасности и Министерством обороны Азербайджана.

Тактика, применяемая ДСЗН, может защитить нефтепроводы от «обычных» террористических атак. Но существующие угрозы ведут к необходимости в совместных действиях и сотрудничестве в области безопасности жизненно важной энергетической инфраструктуры. Текущая ситуация заставляет нас думать о создании общей системы безопасности энергетической инфраструктуры Европы, а также в рамках ОБСЕ.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Инициатива Европейской Комиссии по защите важнейшей энергетической инфраструктуры: Обзор

Г-н.Хосе Антонио Хойос Перез, Политический Советник, Группа С1, вопросы энергетической стратегии и безопасности снабжения, Генеральный директорат энергетики и транспорта (DG TREN), Европейская Комиссия

В июне 2004 года Европейский Союз начал стратегическую инициативу, относящуюся к защите объектов инфраструктуры, являющихся жизненно важными в обеспечении таких показателей, как благосостояние граждан Европы, работа государственных органов или функционирование внутреннего рынка.

В этой связи, 20 октября 2004 года Европейская Комиссия приняла [1] Коммюнике *о защите жизненно важной инфраструктуры в борьбе с терроризмом*, в котором выдвинуты предложения по предотвращению, готовности и реагированию на террористические атаки на жизненно важные объекты инфраструктуры.

Открытый диалог с общественностью являлся ключевым в развитии данного процесса, чтобы Комиссия могла обеспечить соответствие любых правовых или финансовых инициатив, которые могут быть предприняты, с потребностями и ожиданиями заинтересованных сторон. С этой целью Комиссия представила 17 ноября 2005 года «Зеленый документ» о европейской программе по защите жизненно важной инфраструктуры.

Данный консультационный процесс привел к выпуску Комиссией Коммюнике [2] от 12 декабря 2006 года по *Европейской программе по защите жизненно важной инфраструктуры* и последующему запуску программы (ЕПЗЖВИ), охватывающей широкий ряд мероприятий, которые преследуют одну конечную цель, а именно обеспечение целостности и функциональности жизненно важных объектов инфраструктуры. В тот же день Комиссия представила Совету предложение по Директиве *об определении и обозначении жизненно важных объектов европейской инфраструктуры и оценке необходимости в повышении их защиты,* которая была принята в декабре 2008 года [3].

Хотя изначально ЕПЗЖВИ была нацелена на все секторы, со временем Комиссия решила перейти к стратегии, в которой определенным секторам отдавался приоритет. Так было с энергетикой и транспортом, в отношении которых 2 февраля 2007 года Комиссия приняла Коммюнике [4], именуемое «Защита жизненно важной инфраструктуры энергетики и транспорта Европы».

Образы действий ЕПЗЖВИ

Как было сформулировано в 2006 году, ЕПЗЖВИ состоит из нескольких образов действий, которые можно вкратце охарактеризовать следующим образом:

- Информационный обмен: предупредительная информационная система жизненно важной инфраструктуры (CIWIN), использование экспертных групп по защите жизненно важной инфраструктуры (ЗЖВИ) на уровне ЕС, процессы обмена информации по ЗЖВИ и определение и анализ взаимосвязей;
- Защита национальных жизненно важных объектов инфраструктуры (НЖВОИ). Признавая, что защита НЖВОИ является ответственностью собственников, операторов и самих стран-участниц, Комиссия оказывает поддержку в этой области по запросу стран-участниц. Поощряется, когда каждая страна-участница составляет национальную программу защиты;
- Внешняя масштабность, причастность третьих стран. Сотрудничество с международными организациями в области ЗЖВИ также относится к данному заголовку;

«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 № 6/07***

- Соответствующие финансовые меры и, в частности, предлагаемая ЕС программа по «Предотвращению, готовности и управлению последствиями терроризма и прочих рисков, связанных с безопасностью» на 2007-2013 гг., в которой представлены возможности финансирования мероприятий по ЗЖВИ, которые могут передаваться по ЕС;
- Процедура определения и обозначения европейских жизненно важных объектов инфраструктуры (ЕЖВОИ), и общий подход к оценке необходимости в повышении защиты этих объектов. Это необходимо реализовывать через вышеуказанную Директиву, которая была официально принята 8 декабря 2008 года.

Правовая структура

Директива 2008/114/ЕС от 8 декабря 2008 года «об определении и обозначении жизненно важных объектов инфраструктуры Европы и оценке необходимости в укреплении их защиты» является основой для действующей стратегии ЕС в области защиты жизненно важной инфраструктуры. Ее основные аспекты приведены ниже.

Определение «европейских жизненно важных объектов инфраструктуры» или «ЕЖВОИ»: *означает жизненно важные объекты инфраструктуры, расположенные в государствах-членах ЕС, подрыв или разрушение которых будет иметь существенное последствие, как минимум, для двух государств-членов ЕС. Значительность последствия следует оценивать в плане комплексных критериев. Сюда относятся и последствия, возникающие из межсекторной зависимости от других видов инфраструктуры;*

Область действия Директивы ограничивается секторами транспорта и энергетики. Указываются следующие подсекторы:

Энергетика
1.Электроэнергия: объекты инфраструктуры и сооружения по производству и передаче электроэнергии в плане энергоснабжения
2. Нефть: добыча, рафинирование, очистка, хранение и транспортировка нефти
3. Газ: добыча, рафинирование, очистка, хранение и транспортировка газа. Терминалы СПГ
Сооружения атомной энергетики исключены из области действия.

Транспорт
4. Автомобильный транспорт
5. Железнодорожный транспорт
6. Авиатранспорт
7. Речной внутренний транспорт
Морской транспорт и порты8.

В Директиве разъясняются критерии по оценке жизненной важности объекта инфраструктуры в плане серьезности последствий, которые могут иметь его подрыв или разрушение. Необходимо учитывать следующие общие или комплексные критерии:

- Критерий несчастных случаев (оценивается потенциальное количество смертельных случаев или травм);
- Критерий экономического воздействия (оценивается значимость экономического убытка и/или ухудшения товаров или услуг; в том числе возможное воздействие на окружающую среду);
- Критерий общественного воздействия (оценивается влияние на общественное доверие, физический ущерб и ухудшение повседневной жизни; в том числе потеря основных видов услуг).

Точные пороговые значения, применимые к комплексным критериям, должны определяться индивидуально к каждому случаю странами-участницами, обеспокоенными определенной жизненно важной инфраструктурой.

«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 № 6/07***

Транснациональный масштаб последствия, присутствующий в определении ЕЖВОИ, подчеркивается посредством так называемых отраслевых критериев, которые определяют эти объекты инфраструктуры с трансграничными последствиями. Процесс определения и обозначения ЕЖВОИ, как поясняется в Директиве, должен выполняться странами-участницами в течение двухлетнего периода после принятия Директивы.

После такого обозначения, последствия на фактических ЕЖВОИ являются незамедлительными:

I) Формирование Плана безопасности оператора (ПБО)
В ПБО будет указываться следующее:

1. Идентификация значимых активов;
2. Будет проводиться анализ рисков, основанный на ключевых сценариях угроз, уязвимости каждого актива и потенциальном воздействии;
3. Определение, отбор и приоритетность контрмер и процедур с различием между:

– Постоянными мерами безопасности, которые определяют обязательные инвестиции в сферу безопасности и средства, которые подходят для использования в любое время

Дифференцированными мерами безопасности, которые могут быть активированы в соответствии с изменяющимися уровнями рисков и угроз.

II) Создание должности сотрудника связи по безопасности (ССБ)
ССБ должен функционировать как контактное лицо по вопросам безопасности между собственником/оператором ЕЖВОИ и соответствующим органом государства-члена ЕС.

В Директиве также содержатся некоторые обязательства в отношении государств-членов, в которых находятся ЕЖВОИ. Это относится к проведению оценки угроз в отношении подсекторов ЕЖВОИ, если обозначен ЕЖВОИ, и если существует необходимость представить отчет о результатах Комиссии. На основании данных отчетов, Комиссия и государства-члены должны оценивать на отраслевой основе, следует ли рассматривать для ЕЖВОИ дальнейшие меры защиты на уровне Сообщества.

Дополнительные мероприятия

Хотя процесс выполнения Директивы государствами-членами еще находится на стадии реализации, существует ряд дополнительных мероприятий в рамках различных аспектов ЕПЗЖВИ:

Проекты, финансируемые Программой по предотвращению, готовности и управлению последствиями терроризма и прочих рисков, связанных с безопасностью;

- Исследования, финансируемые тематическими службами Комиссии по вопросам ЗЖВИ;
- Седьмая рамочная программа исследований (FP7) 2007-2013, в рамках которой Европейская Комиссия выделила 1,4 млрд. евро специально на исследования вопросов безопасности [5] (ЗЖВИ и т.д.).

Помимо прочих вопросов, приоритетные темы, охватываемые этими инструментами, включают в себя оценку угроз и уязвимых сторон, взаимозависимости, кибер безопасность, управление рисками, планирование чрезвычайных обстоятельств, обмен опытом и обучение.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Резюме

Защита жизненно важной инфраструктуры является относительно новой областью на институциональном уровне в Европейском Союзе, поскольку традиционно это было ответственностью исключительно государств-членов.

Европейская программа по защите жизненно важной инфраструктуры представляет собой основу данной стратегической попытки, при этом первые шаги в сторону формирования специальной правовой структуры были уже предприняты посредством Директивы 2008/114/ЕС.

Меры, предлагаемые Европейской Комиссией, и меры, которые государства-члены применяют по своей инициативе, представляют подлинный прогресс в обеспечении высокого уровня защиты жизненно важной инфраструктуры на территории Европейского Союза.

ПРИМЕЧАНИЯ:
[1] COM(2004) 702 окончательная версия, 20.10.2004
[2] COM(2006) 786 окончательная версия, 12.12.2006
[3] Директива Совета 2008/114/EC от 08.12.2008
[4] COM(2007) SEC(2006)1697, 02.02.2007
[5] Информация по финансированию FPVII http://cordis.europa.eu/fp7/security/home_en.html

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ*: Приведенное мнение является исключительно мнением автора и ни при каких обстоятельствах не может считаться выражением официальной позиции Европейской Комиссии*

Защита критических объектов энергетической инфраструктуры от террористических актов в государствах-участниках СНГ

Руководитель Антитеррористического центра государств-участников СНГ генерал-полковник милиции

Сегодня мы наблюдаем смысловую модификацию глобального терроризма. Во-первых, террористическая деятельность приобрела формат модифицированной партизанской войны, что обусловило и переход силовых структур государств от форматов войсковых действий к технологиям точечных контртеррористических операций. Во-вторых, геоэкономическая карта мира оказывается «матрицей», на которую налагается «предметный слой» географии современного терроризма. Имеет место устойчивая связь географии повышенной террористической активности с региональным распределением добычи углеводородов и иных энергоресурсов.

Прогноз Университета ООН «Глобальные Энергетические Сценарии» до 2020 года содержит следующие утверждения: мир вступил в эпоху войн за ресурсы; главной целью многих террористических и экстремистских группировок становится не свержение центрального правительства или приобретение гражданских прав, которых была лишены их социальная, этническая, религиозная группа, а *установление и удержание контроля над ресурсами.* Примечательно, что на взаимосвязь террористической активности в регионе с ростом цен на углеводороды еще в 2007г. указывали и авторы доклада Всемирного экономического форума, посвященном глобальным рискам. Не менее определенные оценки вероятности дестабилизации Центральноазиатского региона в связи с «проклятием ресурсов» дают и авторы известного аналитического центра Crisisgroup в докладе № 133 «Азия» (май 2007г.).

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

В орбиту «энергетического» терроризма оказались втянуты и государства СНГ. Здесь определенно сформировался самостоятельный объект диверсионно-террористических посягательств – нефте- и газопроводы. Анализ ситуации показывает, что географические контуры обеспечения энергетической безопасности, а соответственно и террористических угроз, находятся на территориях прикаспийских государств и государств Центральной Азии. Непосредственным объектом потенциально возможных диверсионно-террористических посягательств становятся, прежде всего, энергетические коммуникации. Проблема обеспечения безопасности поставок нефти затрагивает экономические и политические интересы такого государства как Казахстан. Нефтепровод из Западного Казахстана только в Китай имеет протяженность 1200 километров и способен транспортировать от 10 до 20 миллионов тонн нефти в год. В намерении снизить террористические риски Казахстан и Китай объединили свои усилия. Диверсифицируя поставки газа, Туркменистан развивает сеть газопроводов. Часть из них по проектам может проходить через территории, которые по оценкам ООН не являются безопасными с точки зрения террористических угроз. Очевидно, что такие крупные проекты как экспортные нефте- и газопроводы, являющиеся по сути транспортными коридорами, будут привлекать внимание не только экономических конкурентов, но и террористов. Снижение террористических рисков на указанных объектах – прямая задача спецслужб и правоохранительных органов государств.

Несомненно, контур антитеррористической безопасности государств-участников СНГ отчетливо накладывается на контур их экономических интересов. Полагаю, активизация бизнеса, возобновление масштабных экономических связей государств СНГ в сфере энергоносителей и энергопоставок, в особенности на Центральноазиатском направлении, заставляет обратиться к обеспечению контртеррористической составляющей стратегии транспортной безопасности с более прагматических и юридически выверенных позиций. Мой профессиональный опыт показывает, что при решении вопросов о защите критически важных объектов от диверсионно-террористических атак акцент следует делать на специфике региональных рабочих стратегий.

Антитеррористический центр государств-участников СНГ связывает приоритетные меры по предупреждению актов терроризма на нефте- газопроводах со следующими действиями: распространение единой Концепции транспортной безопасности на все государства СНГ; имплементация Модельного закона СНГ «О транспортной безопасности» в национальные нормативные акты государств Содружества; модификация Модельного закона СНГ «О трубопроводном транспорте» с учетом актуальных задач борьбы с терроризмом на нефте- и газопроводах и последующее его восприятие в правовом поле суверенных государств Содружества; организация в масштабах СНГ мониторинга объектов (участков) нефтегазопроводов, потенциально опасных с точки зрения совершения диверсионно-террористических актов (здесь предполагается применение современных технологий прогнозирования, расчет рисков); продолжение практики проведения совместных антитеррористических учений на техногенно-опасных объектах и распространение такой практики на объекты транспортных коридоров государств-участников СНГ.

Думается, что квалифицированной работы спецслужб государств (при всей ее огромной важности) уже недостаточно. Видимо, следует ставить вопрос о взаимодействии государств, которые являются поставщиками, транзитерами и получателями энергоресурсов. На повестке дня - необходимость новых форматов контртеррористического сотрудничества спецслужб государств-энергодоноров (а это государства, входящие в СНГ) и европейских государств-получателей энергоносителей. Государства Содружества всерьез обеспокоены обеспечением безопасности ценнейшего экономического ресурса. Такой статус требует реального обеспечения постоянной региональной стабильности.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Безопасность важнейших объектов энергетической инфраструктуры (ВОЭИ): как продвинуть взаимодействие государственного и частного сектора

Д-р. Хейко Борхерт и Карина Форстер

Нет энергетической безопасности без безопасности энергетической инфраструктуры, а глобальная энергетическая инфраструктура (ЭИ) сегодня хрупка. В будущем данная ситуация, скорее всего, ухудшится, так как энергетические потребности наших стран растут. Как результат, давление на существующую ЭИ так же вырастет. Следовательно, этот документ становится началом государственно-частного подхода к защите ВОЭИ и предлагает конкретные шаги по взаимодействию между государственным и частным сектором в области энергетической безопасности.

Существуют серьезные риски…

Недостаточные инвестиции, законодательные различия, а также специфические уязвимые места, возникающие из-за физических или кибер рисков, все они воздействуют на глобальную ЭИ. Сложная ситуация еще больше ухудшается тем фактом, что некоторые страны защищают свои энергетические ресурсы, тем самым, препятствуя конкуренции и задерживая передачу технологий в ущерб эффективности ЭИ. Существующие проблемы ЭИ усилятся новыми вызовами, такими как изменение климата, политические требования по выбросу углеродов и их транспортировке/хранению, межрегиональное инфраструктурное взаимодействие и ввод малых сетей в зависимости от информационно-коммуникационных технологий (ИКТ).

В настоящий момент нет ни единой законодательной среды, ни адекватной управляющей структуры, решающей вопросы безопасности вдоль всей глобальной цепи поставки энергоресурсов, начинающейся в странах-производителях, затем идущей через транзитные страны и заканчивающейся на потребительских рынках.

Это является проблемой, так как зависимость от эластичной ЭИ, скорее всего, вырастет из-за растущей энергетической потребности. Поэтому наиболее фундаментальным вопросом безопасности ВОЭИ является необходимость в налаживании процесса управления и взаимодействия между многочисленными представителями государственных и частных игроков по всей глобальной энергетической цепи.

…требующие государственно-частного взаимодействия по безопасности

В начале 21 века тесное государственно-частное взаимодействие по безопасности стало незаменимым. Новые проблемы безопасности, глобализация рынков и обществ, а также передача традиционных государственных функций частному сектору привела к переплетению национальной и корпоративной безопасности. Недочеты в одном секторе неизбежно повлияют на другой. Тем не менее, можно сделать существенные выводы при планировании безопасности при обязательном подключении многих игроков и пересечении через различные политические области.

Что касается безопасности ВОЭИ, частному сектору, необходимо взаимодействовать с владельцами и операторами ЭИ, строительными компаниями, сообществами ИКТ и компаниями, работающими в области безопасности и обороны. Все они предлагают решения по безопасности, им также нужно работать со страховыми и финансовыми компаниями, помогающими получить инвестиционные стимулы. Частный сектор должен также взаимодействовать с политиками, экономическими регуляторами, инспекторами по окружающей среде, государственными инвесторами, службами ЧС, военными/охранными структурами, а также разведывательными службами.

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

В этой сложной паутине взаимоотношений государственно-частное сотрудничество по безопасности ведет к необходимому государственно-частному взаимодействию, а именно:
Координации, гармонизации и, возможно, интеграции целей, стратегий, процессов, структур, возможностей и мощностей в различных областях взаимодействия для того, чтобы продвинуть безопасность и защиту ЭИ на всех этапах вдоль глобальной энергетической цепи.

Государственно-частное сотрудничество по безопасности не должно быть ограниченно простыми областями сотрудничества, такими как анализ рисков, планирование, обучение и образование, научные исследования, закупки или операции при чрезвычайных ситуациях. Скорее всего оно должно быть разработано как постоянный процесс, включающий все сферы показанные на Рис. 1.

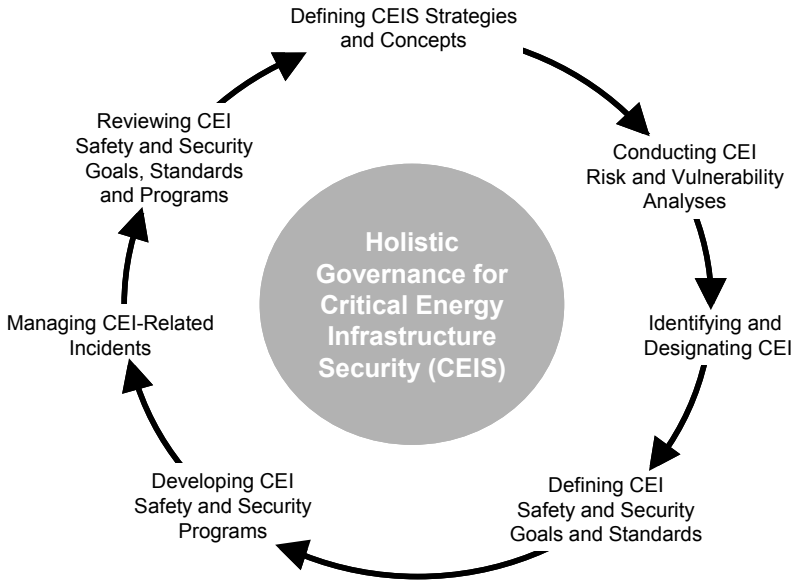


Рис 1: Стандартные блоки государственно-частного подхода по безопасности жизненно важных объектов энергетической инфраструктуры

Стратегии и концепции

БЭИ не единственный вопрос на который должны ответить представители государства и частного сектора. Важным является гармонизация стратегий специфичных для ЭИ с другими программами по безопасности.

Со стороны государства поощряется согласованность политики. Программы БЭИ должны быть выровнены с национальными стратегиями по инфраструктурной безопасности. Эти стратегии, в свою очередь, должны тщательно вплетаться в общую национальную стратегию безопасности. Например, несколько стран используют сценарии национальной безопасности для продвижения сотрудничества между агентствами для подготовки к возможным последствиям. Это также может помочь при координации государственных ожиданий в отношении собственников и операторов ЭИ. Также государственным представителям следует тщательно проверять акты/законодательство по безопасности с учетом дополнительных требований, которым должны отвечать собственники и операторы ЭИ.

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Самой важной стратегической задачей для частного сектора является принятие корпоративной безопасности как конкурентного преимущества и незаменимого стандартного блока национальной безопасности. Повышая осведомленность по корпоративной безопасности, компании не должны только концентрироваться на своих основных бизнес процессах. Скорее, есть растущая потребность в Постоянном Управлении Бизнесом вдоль всей глобальной энергетической цепи поставок и цепи поставок в других важных инфраструктурных секторах. Требуется более интенсивный двухсторонний диалог по вопросам безопасности между собственниками и операторами ЭИ и партнерами за пределами энергетического сектора.

Анализ рисков и уязвимых мест

При обсуждении рисков и уязвимых мест основной задачей является совместное осознание ситуации и совместное понимание основных угроз возникших перед различными представителями вдоль всей глобальной энергетической цепи поставок. Также предполагается всесторонний анализ внешней и внутренней зависимости на национальном и международном уровнях.

Государственный сектор может поддержать анализ рисков и уязвимых мест посредством создания доверительной атмосферы, которая поможет при обмене секретной информации по рискам и угрозам, основанной на расчетах разведки. Данная поддержка предоставит значительную мотивацию частному сектору. Общие методологии, помогающие идентифицировать, классифицировать, оценить риски также помогут, в частности, мелким собственникам и операторам ЭИ, работающим в жестких рыночных условиях. Государственный сектор совместно с корпоративными партнерами также должны обсуждать возможные последствия для безопасности развязывания цен ЭИ и продажи ЭИ финансовым инвесторам.

Собственники и операторы ЭИ играют ключевую роль в расширении объема анализа рисков и уязвимых мест за пределами энергетического сектора. Энергетическим компаниям и поставщикам ИКТ, например, следует объединить усилия для анализа взаимозависимости и разработать стандарты реагирования по соответствующим уязвимым местам. Собственники и операторы ЭИ могут также вести диалог с ключевыми клиентами, например, в химическом, транспортном, финансовом секторах и здравоохранении для обозначения межсекторной зависимости и уязвимых мест.

Определение и назначение

Определение и назначение ЭИ на национальном, европейском и глобальном уровне очень важно, так как назначение скорее всего будет иметь прямое влияние на собственников и операторов ЭИ. Поэтому есть необходимость в прозрачности процессов и критериев определения и назначения ВОЭИ на национальном и международном уровне.

Многие правительства избегают законодательства, определяющего и назначающего ВОЭИ. Вместо этого они предпочитают вести переговоры с частными операторами. Тем не менее, это может быть неоднозначным. Разные министерства могут иметь отличающиеся друг от друга философии определения безопасности. Если эти различия будут показаны корпоративным партнерам, они могут отступить и отказаться от повторных попыток. Поэтому государственному сектору важно определить общие правила по определению компонентов ВОЭИ перед началом сотрудничества с частным сектором.

Предложение государственного сектора не издавать законы дает собственникам и операторам ЭИ значительную дискреционную власть, которой следует распоряжаться ответственно. Им следует вовлечься в обмен информацией с государственным сектором и следует думать о корпоративных ВОЭИ, за которую они несут прямую ответственность.

«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 № 6/07***

В дополнение, собственники и операторы ЭИ, вовлеченные в международные инфраструктурные проекты, могут взаимодействовать со странами поставщиками и транзитными странами для развития общей методологии определения межграничных зависимостей ЭИ и согласовывать распределение задач и ответственности по разную сторону границ.

Цели и стандарты

Существует несколько проблем при определении стандартов ВОЭИ. Растущая зависимость от ИКТ говорит о необходимости стандартов по кибер безопасности в энергетическом секторе. Взаимозависимость энергетического и других инфраструктурных секторов приводит к необходимости определения уровня безопасности, необходимого во всех важных инфраструктурных секторах для избегания нечестного конкурентного преимущества компаниями, работающими при различных рыночных условиях. Общие стандарты должны появляться соразмерно динамичному риску окружающей среды. Здесь, изменения в окружающей среде могут рассматриваться как один из факторов, ставящих ЭИ под серьезное напряжение.

Один из основных вопросов, на который должен ответить государственный сектор, - это соответствие промышленных стандартов в свете сегодняшних и, скорее всего, будущих проблем безопасности. Государственным наблюдательным органам необходима методология оценки соответствия существующих промышленных стандартов. В дополнение, государственному сектору также, возможно, будет необходимо рассматривать задачи экономических регуляторов. Если возврат инвестиций является единственной задачей, то экономические регуляторы, скорее всего, установят регуляторное стимулирование, которое будет невыгодно для корпоративных инвестиций в области безопасности. Безопасность является общественной ценностью, с которой экономические регуляторы должны считаться при принятии решения о необходимости инвестиций, предоставленных собственниками и операторами ЭИ для оправдания своих цен.

Среди прочего, собственники и операторы ЭИ могут признать, что общие промышленные стандарты безопасности не всегда соответствуют ожиданиям государственного сектора. Защита целостных концепций для продвижения стандартов Постоянного Бизнес Управления за пределами энергетического сектора, например, могла бы быть конкретным шагом, принятым энергетическим сообществом, показывающим, что общественный страх возможных сбоев в поставке через различные секторы принимается всерьез. Кроме того, частные собственники и операторы ЭИ могут также вести диалог касательно стандартов безопасности с энергетическими компаниями, управляемыми или принадлежащими государству в поставляющих или транзитных странах.

Программы по охране и безопасности

Когда речь заходит о программах по охране и безопасности и о том, какие меры принять, чтобы ЭИ была более эластичной, то основная ответственность лежит на частных собственниках и операторах ЭИ. Значительной услугой, предлагаемой частными собственниками и операторами ЭИ, были бы инспекции совместно с рекомендациями по охране и безопасности, полученными из разведывательных оценок. Государственный сектор также мог бы рассматривать регуляторное стимулирование. В некоторых странах существуют государственные бюджеты на специфичные меры, прописанные в национальных планах по гражданской безопасности. Другие варианты могут включать предпочтительное налоговое обложение для инвестиций в безопасность ВОЭИ. В частности, при инвестициях в энергетический сектор государственный сектор должен принять во внимание взаимоотношения между международными, региональными/местными поставщиками энергоресурсов. Программы по охране и безопасности должны отражать эти различия, чтобы избежать дезорганизации рынка из-за жестких требований, предъявляемых всем участникам.

«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 № 6/07***

Собственники и операторы ЭИ, в свою очередь, могут увеличить прозрачность своих инвестиций в охрану и безопасность ВОЭИ. Например, они могут раскрыть информацию об инвестициях в проект, ремонте, обновлении инфраструктуры, обучении, и безопасности ИКТ. Собственники и операторы ЭИ, а также небольшие компании, зависимые от поставок энергоносителей, могли бы пользоваться программами «Руководство по управлению поставками» для определения общих подходов по безопасности поставок энергоносителей. Обмен передовым опытом (например, безопасность ИКТ) с партнерами по цепи поставок энергоносителей и партнерами из других важных инфраструктурных секторов также будет полезным.

Управление непредвиденными событиями

Межрегиональные энергетические рынки создаются посредством соединения национальных ЭИ. Тем не менее, без адекватных мер предосторожности риски вырастут экспоненциально, так как существующая ЭИ была разработана, в первую очередь, для обслуживания национальных рынков. Сегодня существует серьезный недостаток информации по имеющимся возможностям по решению межграничных инцидентов. Многие страны проводят учения по защите гражданского населения, которые также охватывают собственников и операторов ЭИ. Объем этих учений должен быть расширен для того, чтобы обучить также управлению непредвиденными событиями по разные стороны границ. В поддержку этих учений также следует подумать о совместных государственно-частных операционных картинах, которые объединяют информацию, полученную из частных и государственных областей в единый командно-контрольный подход. Что касается регулирования, государственный сектор также должен обсудить схемы компенсаций при оказании помощи на границах.

Собственники и операторы ЭИ могут также поддержать государственный сектор посредством инвестиций в моделирование и симуляцию (М/С). М/С важны при выявлении сложных сторон ВОЭИ и понимании зависимостей между компонентами ЭИ, а также ЭИ и важными инфраструктурными компонентами. В случае непредвиденных событий М/С необходимы для принятия информированных решений о вмешательстве в хрупкую систему ЭИ для избегания непреднамеренных каскадных последствий. В конечном итоге М/С можно использовать для оценки целесообразности стандартов безопасности ЭИ. В дополнение, международные собственники и операторы ЭИ могут поддержать построение мощностей для управления непредвиденными событиями в странах поставщиках и транзитных странах.

Обзор

Структура безопасности ВОЭИ должна постоянно развиваться. Но, как известно, любая структура безопасности хороша только при определенных усилиях, направленных на обучение и обзор. Это вопрос, на который также должны ответить совместно государственные и частные участники. Имеет смысл, например, подумать о постепенном подходе к обзору безопасности ВОЭИ. Самооценка, основанная на аудите или самопроверке, может служить основой. Следующим этапом может быть оценка с третьей стороны. Например, предусмотреть создание совместных команд из представителей частных и государственных структур. Также можно проводить совместные учения. Параллельно награды за лучшие практики могут стимулировать инновации. А также обсуждения с агентствами по финансовым рейтингам и страховыми компаниями о том, как оценить корпоративные инвестиции в безопасность, могут предоставить дальнейшую мотивацию.

Целостная система управления

В общем, успешное внедрение предложенной структуры безопасности ВОЭИ будет зависеть от целостной системы управления. Это важно, так как сегодня большинству стран недостает институтов для управления государственно-частным взаимодействием в области безопасности.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Целостная система управления включает в себя регулярные встречи государственных и частных представителей для создания личных связей и построения доверия. А также для определения точек контакта для обмена информацией. Последнее, но не менее важное, совместная рабочая атмосфера также должна включать современное оборудование ИКТ для создания совместной информированности о ситуации и совместном понимании ситуации, что является центром государственно-частного партнерства по безопасности.

Примечание: *Карина Форстер является управляющим директором сети IPA в Берлине, Др. Хейко Борхерт является членом консультационного совета IPA и управляет политической консультацией в Швейцарии и Австрии.*

Глобальные платформы и большая рентабельность инвестиций: энергетическая инфраструктура в 21 веке

Г-жа Дженнифер Жиру, Центр по исследованиям вопросов безопасности (CSS), Швейцарский Федеральный Технологический Институт (ETH), Цюрих

Террористические атаки между 70-90 годами 20 века были нацелены на ЭИ в нефтегазовой отрасли (НГО), они возникали время от времени и имели ограниченные последствия. Например, взрывы на трубопроводе Тихоокеанской Газовой и Электрической компании в Калифорнии в середине 70-ых были спонсированы Новым Всемирным Либеральным Фронтом и не имели больших последствий, кроме символического значения атаки. Тем не менее, спустя годы, нацеленность на ЭИ распространилась на территорию от Канады далее к Мексике, Колумбии, Нигерии, Алжиру, Судану, Йемену, Эфиопии, Пакистану, Ираку, Саудовской Аравии, России и Евразии. При близком рассмотрении видно, что атаки происходят не только часто и имеют большие последствия, но также более не ограничиваются актами

терроризма или другими проявлениями политического насилия. Скорее АГРЕССИВНЫЕ НЕГОСУДАРСТВЕННЫЕ АКТОРЫ (АНА) все больше мотивированы спектром целей, где различия между политической и криминальной мотивацией размыты. Данное развитие поддерживается приходом глобализации, когда мировые рынки стали зависимы друг от друга, а значительное продвижение информационных технологий ускорило возможность производить дешево, делиться и обмениваться информацией через огромные расстояния.

Это мотивировало распространение идеологий, сетей, технологий и предоставило возможность группам к новому доступу, глобальному видению и прибыльным нелегальным предприятиям. Структурно АНА заменили иерархические структуры с небольшими, рассредоточенными и высоко приспособляемыми сетями, которые больше ведомы желанием обогатиться, чем получить государственную независимость.

Политические платформы

Нацеленность на ЭИ является формой экономического таргетирования, которая позволяет АНА распространять политические обиды в дифференцированной манере и дестабилизировать государство посредством вызова в способности защитить важный сектор. Успешные атаки могут привести государство к финансовым потерям, разрушить инфраструктуру и остановить производство, а также привести к реакции рынка НГО и панике (особенно среди международных и национальных нефтяных компаний). Атаки обычно включают использование взрывных устройств и/или атаки боевиков, использующих легкое оружие. Далее, последние тенденции показывают проблему важности инфраструктуры.

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

В то время как энергетический сектор можно рассматривать как важный, есть также и другой слой, который связан с важностью некоторых узлов внутри инфраструктуры сектора, остановка работы которого может иметь неожиданное и серьезное последствие по всей системе. Хотя этот момент является важным, он может служить преувеличению тенденции к низко прибыльным атакам с большими последствиями, нацеленными на важные компоненты. Тем не менее, заметные кампании в Колумбии, Ираке и Нигерии показали что частые, небольшие атаки на ЭИ могут привести к продолжительным остановкам производства, которые ведут к значительным затратам.

Например, в середине 80-ых Революционные Вооруженные Силы Колумбии (ФАРК) и Национальная Освободительная Армия (НОА) начали нацеливаться на трубопровод Кано Лимон – Ковенас в Колумбии протяженностью 480 миль и пропускной способностью 100 000 баррелей в день. В 1996 году атаки начали увеличиваться и достигли пика в 2001 году с более чем 170 повреждениями от небольших, но частых атак, что оставило трубопровод по большому счету в нерабочем состоянии и стоило Колумбийскому правительству 500 миллионов долларов США в виде неполученной прибыли. В 2003 году мятежники в Ираке начали кампанию по атакам на ЭИ с целью создания значительных нарушений в поставках. К настоящему моменту было зафиксировано около 500 атак, большинство которых были небольшими. Многие из них были повторными, в то время как некоторые из них были нацелены на крупные узлы и оборудование, что привело к серьезным повреждениям и долгим ремонтам. До 2008 года мятежникам удавалось расстраивать планы по защите ЭИ, создавая постоянное состояние разрушений, что серьезно подорвало экспорт нефти и поступление прибыли. Это привело к появлению того, что аналитики называют надбавкой за безопасность, от минимума 4 доллара до 25 долларов США за баррель. Такое поведение на рынке привело к неопределенности во всем регионе. Другие производители в НГО, такие как Саудовская Аравия и Йемен также не защищены от атак, были многочисленные попытки разрушить местные трубопроводы с одновременными призывами групп Салафи Джихади к атакам на трубопроводы, танкеры и другие активы. Морские активы также были подвержены рискам атак. Террористическая атака в 2002 на Лимбург, французский танкер, перевозивший примерно 400 000 баррелей нефти из Ирана в Малайзию увеличила страховочную премию на 300% для кораблей, заходящих в Йеменские порты. Это привело к временному сокращению в отправках морем, что стоило Йемену 4 миллиона долларов в месяц
Недавно, в июле 2009 года, 25 человек, связанных с Аль-Кайда, были арестованы египетскими спецслужбами за попытку атаковать танкеры, пересекающие Суэцкий канал. Вследствие этого, кувейтские власти доложили об аресте представителей, связанных с Аль-Кайдой, которые якобы использовали Google Earth для планирования атак на НПЗ Шуайба.

Аналогичным образом боевики в районе дельты реки Нигер, нефтедобывающем районе Нигерии, продолжительное время атаковали ЭИ на суше и на воде. После образования Движения за освобождение дельты реки Нигер (MEND) в конце 2005 г. появилась информация о еще более агрессивных атаках, которые привели к снижению ежедневной добычи нефти на 25 процентов (что составляет от 500.000 до 700.000 баррелей в день).

В ходе развития этого конфликта многие иностранные рабочие, занятые в НГО, были эвакуированы, а некоторые нефтедобывающие компании в этом регионе приостановили работу. В 2008 г. MEND взяло на себя ответственность за атаки, нанесенные в акватории месторождения Бонга компании Shell, которое является его основным прибрежным месторождением и приносит 225.000 баррелей нефти в день на полной мощности. Вместе с требованием о высылке иностранных рабочих из Нигерии в заявлении подчеркивалось, что «место сегодняшней атаки было намеренно выбрано для того, чтобы исключить все мысли о том, что оффшорная добыча нефти не находится у нас в руках».

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

В настоящее время атаки на ЭИ сократились благодаря проводимой правительством программе амнистии боевиков. Тем не менее, подобная программа уже была начата в 2005 г., и частично вследствие ее провала разразилась новая волна атак в период между 2006 и 2009 гг.

Примеры малых кампаний включают продолжающиеся конфликты в Индии и Пакистане, в предыдущие годы Объединенный Фронт Освобождения Асома многократно проводил атаки, нацеленные на сектор природного газа и сырой нефти, при этом в пакистанской провинции Белуджистан боевики регулярно наносили бомбовые удары по газопроводам и объектам инфраструктуры энергосистемы. В 2007 г. Народная Революционная Армия (PRA) Мексики взяла на себя ответственность за кратковременную, но интенсивную бомбардировку газопроводов, вызвавшую разрушения и скачок цен на газ. PRA оправдывало свои действия “национальной кампанией притеснения интересов олигархов и этого нелегитимного правительства, которая была пущена в ход». Несмотря на это, вышеописанные случаи являются примерами относительно низкобюджетных кампаний, направленных на достижимые цели, и представляют собой существенные рычаги для изменения оперативной обстановки. Большее беспокойство для НГ отрасли представляет тот факт, что в период между 2002/3 и 2008 гг. атаки на ЭИ сыграли значительную роль во всемирном повышении цен на сырую нефть, которая достигла исторической величины 147 долл. США за баррель в июле 2008 г.

Прибыльные предприятия

Другое произошедшее недавно событие в данной сфере - это появление атак на ЭИ, управляемых криминальными амбициями. В этом случае преступники могут собрать финансовый урожай от незаконных врезок в трубопроводы и их повреждения с целью хищения нефти, а также захвата танкеров, перевозящих энергоносители и похищения сотрудников сектора НГО с целью получения значительных сумм выкупа. Например, существенно возросло пиратство в Аденском заливе; сообщалось свыше чем о 150 нападениях в 2008 и 2009 гг. соответственно. Танкеры, перевозящие энергоносители подвергались нападениям примерно в 25 % случаев. В ноябре 2008 г. захват супертанкера Саудовской Аравии, проходящего на удалении 450 миль от побережья Сомали и перевозящего 2 млн. баррелей нефти стоимостью свыше 100 млн. долл. США, широко освещался в средствах массовой информации по всему миру и привел к резкому скачку цен на сырую нефть. Через один год, невзирая на присутствие в регионе международных военно-морских и военно-воздушных сил, пиратам удалось захватить еще один супертанкер, проходящий на удалении около 1.000 миль от берега и перевозящий груз сырой нефти стоимостью 20 млн. долл. США. Вооруженные гранатами и автоматическими винтовками и обладающие техникой, доступом и желанием получить значительные суммы выкупа, эти группы создали прибыльный бизнес, заключающийся в захвате судов, за которые можно выручить в любом случае от 500 тысяч до 3 миллионов долл. США за каждое. Согласно докладу Чатем-Хауса, в 2008 г. пираты получили где-то между 18 - 30 млн. долл. США в виде выкупов. Помимо всего прочего сомалийских пиратов также связывают с сомалийской организацией воинов защиты Ислама «Аль-Шабаб Аль-Муджахидин», предоставляющей пиратам благоприятную среду для проведения их операций в обмен на деньги и различные услуги, такие как контрабанда и прочие незаконная деятельность. Гвинейский залив в Западной Африке также стал зоной возросшего количества криминальных атак на танкеры, перевозящие энергоносители.

Кроме атак по политическим причинам АНА также замешаны в хищениях нефти с помощью диверсий на трубопроводах, что приносит довольно значительный доход исполнителям и, по правительственным оценкам, наносит ежегодные убытки государству в размере 12 млрд. долларов США. Естественно, эта цифра меняется в зависимости от рыночных цен на сырую нефть. Соответственно, хищения нефти в Нигерии превратились в крупный бизнес, при этом Управление ООН по наркотикам и преступности сообщает о том, что на нелегальное производство приходится примерно 10% от общего объема производства.

«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 № 6/07***

В действительности, хотя число нападений по политическим причинам в настоящее время сократилось, число нападений с целью хищения нефти увеличилось. Независимо оттого, происходит ли врезка дополнительных трубопроводов в магистральный трубопровод компании, или на трубопроводе происходит диверсия с целью создания запасного трубопровода, похищенная нефть подается на региональный и международный энергетический рынок, а прибыль идет замешанным в этом группам боевиков, частным компаниям- соучастникам преступления, коррумпированным государственным чиновникам.

В другом примере криминально-политического симбиоза российско-чеченский конфликт 90-х годов пролил свет на масштабные операции по хищению нефти, когда чеченские повстанцы делали врезки в трубопроводе Баку-Грозный-Новороссийск более ста раз. Похищенная нефть отправлялась на секретные нефтеперерабатывающие заводы, где производился дешевый бензин, что создавало стабильный доход, который шел на продолжение операций и доход криминальных структур. В 2009г. по сообщениям отчетов, мексиканские организованные преступные группировки расширили свою деятельность с незаконного оборота наркотиков до незаконной торговли нефтью. Они также проводили врезки в трубопроводы и строили туннели и независимые трубопроводы для перекачки растущего количества похищенной нефти, которая продается как на отечественном, так и на американском рынке.

Опасные замыслы

Если рассматривать в совокупности все вышеприведенные случаи, то можно получить представление о гораздо более широком явлении, где нападения АНА оказывают более широкое влияние. Имея возможность разрушить мощности, связанные с поставкой и производством нефти, оказать влияние на формирование нефтяных цен, оказываться в центре внимания средств массовой информации, и создавать возможности для привлекательных выкупов, то, что целью АНА являются ЭИ, демонстрирует пример современной глобализационной парадигмы, где события редко проходят изолированно, а круги от них идут по всему миру. Действительно, такие тенденции высвечивают роль, которую играет безопасность энергетических инфраструктур в настоящем и озабоченность, которую она может вызвать в будущем. За последнее десятилетие энергетические инфраструктуры стали гораздо более неустойчивыми, что усугубляется сильными колебаниями нефтяных цен, растущим мировым спросом на НГ ресурсы, национально-ориентированным подходом к ресурсам, и усиливающимся расчетом при производстве и транзите на проблематичные морские и наземные пути, где процветают атаки на ЭИ. Так как многие производители, среди которых Венесуэла, Иран, Саудовская Аравия, Россия и Нигерия, наряду со многими все еще значительными, но менее масштабными поставщиками, продолжают бороться с проблемами нестабильности, вопросы безопасности энергетических инфраструктур будут вызывать еще большую озабоченность, потребуют больше ресурсов, и в конечном счете потребуют коллективных действий, направленных на улучшение понимания того, что в центре внимания должны быть ЭИ, а также на рассмотрение существующих узких мест, которые существуют по всей цепочке ЭИ, из-за несоответствия стандартов защиты и безопасности.

***ПРИМЕЧАНИЕ**: Г-жа Дженнифер Жиру является научным сотрудником в Центре по исследованиям вопросов безопасности (CSS) Федерального Технологического института г. Цюриха, где она возглавляет проект по планированию работы по энергетической инфраструктуре.*

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Характеристики и уязвимые стороны важнейшей энергетической инфраструктуры

Профессор Вольфганг Крёгер, Швейцарский федеральный институт технологий (ETH) г. Цюрих

Энергетическая инфраструктура направлена на обеспечение соответствующего, доступного энергоснабжения, тем самым, состоя из целой цепочки поставок - от производства до зон потребления, включая транспортировку и передачу. Сосредоточиваясь на подаче электрической энергии и высоковольтных сетях передач, соответственно, необходимо - помимо прочего - уметь справляться с «вариациями», справляться с последствиями/атаками и приводить систему в первоначальное состояние - избегая, тем самым, крупного подрыва в оказании услуг.

Электроэнергетическая сеть, например, континентальной Европы, являясь крупномасштабной, раскинутой, синхронизированной системой, в целом, открытой, несистематично развивающейся, подвергалась скорым изменениям (например, интегрированию перемежающихся источников энергии, таких как ветряная и солнечная энергия) и организационным изменениям (например, от монополий до нерегулируемых рынков и разгруппированных структур).

Электричество рассматривается как общественное благо, и соответствующая инфраструктура обладает всеми характеристиками комплексности, в том числе нелинейные, внезапно возникающие свойства, которые трудно предсказать. Она сталкивается с разнообразными техническими и человеческими ошибками, стихийными бедствиями и различными угрозами, включая злоумышленные действия. Повсеместное использование современных информационно-коммуникационных технологий (ИКТ) позволило добиться полезной интеграции системы, но также привело к появлению новых рисков, например, отказы по общей причине и кибер атаки.

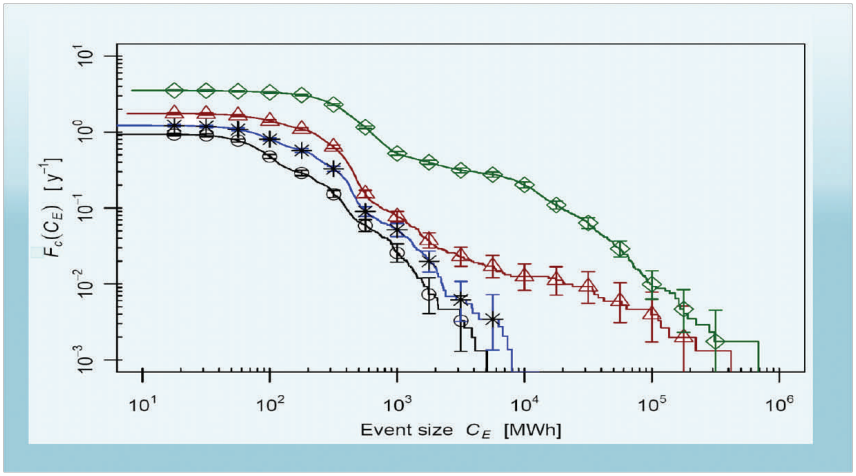
Недавние масштабные выключения в индустриальных странах выявили определенные уязвимые стороны, которым были свойственны общие признаки, такие как:

- Функционирование систем сверх изначальных расчетных параметров (либерализация рынка, интеграция ветряной энергии и т.д.)
- Неисправная работа жизненно важного оборудования и неправильная работа защитных механизмов; недостаточная система автоматизации в некоторых случаях
- Недостаточность ситуационной осведомленности и краткосрочная подготовка к чрезвычайным ситуациям
- Слабое координирование времени в случае непредвиденных ситуаций в зонах контроля
- Несоответствие критерия безопасности N-1, его реализации/оценки

Помимо практического опыта необходимы теоретические исследования для получения материалов, которые можно использовать для определения, снижения и/или лучшего контроля уязвимых сторон. Это требует сочетания методов в рамках аналитической структуры и, в конечном счете, нового системного подхода [1].

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***



Дополнительные кумулятивные частоты отключений F_C и масштабность событий C_E для различных уровней нагрузки сети: 100% (кружки), 110% (звездочки), 120% (треугольники) и 137% (ромбики)

Подход двухслойного, ориентированного на объект моделирования и моделирования Монте-Карло стали хорошим механизмом для понимания свойств реакции электросетей на «помехи». На следующем рисунке показана частота отключений с масштабностью событий и подтверждается чувствительность к повышенным нагрузкам сетей. Другие результаты показывают значимость адекватного (т.е. в течение первых 15 минут) времени реагирования оператора [2]. Структурные исследования путем применения графической теории помогают понять топологию данной системы и ее чувствительность к «атакам». Большая часть систем электропередач являются, скорее, «случайного типа», тем самым, являясь восприимчивыми к случайным сбоям и надежными против нацеленных атак, в то время как «немасштабные системы» (с узловыми центрами) показывают обратное, но противостоят каскадам сбоев (поддерживают «секционирование»).

Помимо зависимостей в рамках инфраструктурных взаимозависимостей между объектами инфраструктуры, либо физические, геопространственные, информационные и логические, либо сопряженные характеристики имеют большую практическую значимость. Многие жизненно важные объекты инфраструктуры зависят от имеющегося электричества; система электроснабжения тесно связана с информационно-коммуникационными системами для системы диспетчерского управления и сбора данных (SCADA). Использование свободно доступного Интернета для передачи данных и команд варьируется в зависимости от стран, что важно для уровня кибер безопасности. Использование неспециального коммерческого программного и аппаратного обеспечения может усиливать риск отказов по общей причине.

Из динамических анализов известно, что потеря одного элемента, в том числе подстанций, из-за технического сбоя, нацеленной атаки или даже крупномасштабного события (например, землетрясения) может привести к отключениям энергии на местном/региональном уровне, но не перейдет неизбежно на национальный или транснациональный уровень (UCTE), что говорит о высоком уровне надежности.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Одна из больших задач в борьбе с уязвимыми сторонами жизненно важной энергетической инфраструктуры – это соответствующая осведомленность, готовность осуществлять (и платить за) мероприятия по снижению избыточного напряжения и готовность к сбою основного энергоснабжения.

Примечание: *Данная статья частично основана на результатах, полученных соответствующим проектом, начатым Швейцарским федеральным агентством гражданской защиты.*

Использованная литература:

[1] В. Крёгер, Жизненно важная инфраструктура в опасности: необходимость в новом концептуальном подходе и улучшенных аналитических инструментах, в технике обеспечения надежности и безопасности систем, Том 93, № 12, 12/08

[2] М. Шлапфер, Т. Кесслер, В. Крёгер, Анализ надежности систем электросетей с использованием гибридного

Как ОБСЕ может внести реальный вклад в энергетическую безопасность

Д-р Кевин Роснер, старший исследователь, Институт анализа глобальной безопасности, Вашингтон, округ Колумбия

Мало известно, и еще менее понятна роль Организации по безопасности и сотрудничеству в Европе (ОБСЕ) в области энергетической безопасности. Вероятно, являясь наиболее известной за свою деятельность по наблюдению за выборами, ОБСЕ имеет поручение продвигать диалог по энергетической безопасности, в том числе на экспертном уровне, с участием стран-производителей, транзитных стран и стран-потребителей. Данное поручение является и инструктивным, и значимым. Среди 56 стран-участниц организации, ОБСЕ является единственной европейской многонациональной организацией, в которую входят и европейские, и североамериканские производители и экспортеры энергии, такие как Канада, Казахстан, Норвегия, Российская Федерация, Туркменистан, наряду с некоторыми крупнейшими в мире странами-потребителями энергии, такими как США, Россия и Германия. В нее также входят и основные страны транзита энергии для Европы, в том числе Беларусь, Украина, Польша, Азербайджан, Грузия и Турция. Таким образом, ОБСЕ однозначна в том, что она предоставляет уникальную платформу для диалога, конечно, в рамках европейского контекста между странами-производителями энергии, странами-потребителями энергии и транзитными странами, считающимися полноправными участницами организации.

В последние месяцы в рамках ОБСЕ имело место усиление мероприятий по энергетической безопасности. В июле 2009 года Правительство Словакии спонсировало конференцию ОБСЕ «Укрепление энергетической безопасности в регионе ОБСЕ». В ходе обсуждений Министр иностранных дел Словакии Мирослав Лайчак отметил, что «вопрос энергетической безопасности охватывает обширный ряд технических, технологических, экономических аспектов и аспектов безопасности, укрываемых одним политическим зонтом. Роль ОБСЕ заключается не в дублировании, а в дополнении мероприятий международных энергетических организаций. Она изъявляет политическую волю и выражает стремление к согласию в плане необходимости осуществления изменений в области внешней энергетической безопасности. ОБСЕ может стать форумом, выражающим политическую поддержку для шагов, предпринимаемых другими инициативами и организациями. В подтверждение этих слов, результат обсуждений в рамках ОБСЕ может служить примером существующих общих подходов и совместных интересов стран-участниц ОБСЕ».

Задача для ОБСЕ – определить, как она может повысить эффективность деятельности других организаций в сфере энергетики, и, тем самым, поддержать политический диалог в рамках других

«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 № 6/07***

организаций, ведущий к лучшей согласованности между производителями, потребителями и транзитными государствами по вопросам, важным для обеспечения безопасности энергоснабжения и безопасности инфраструктуры энергоснабжения.

Как ОБСЕ может повысить эффективность?

Одной ключевой областью, в которой ОБСЕ может повысить эффективность, где отсутствовали другие институциональные инициативы, является область отслеживания и детализации сбоев важнейших объектов энергетической инфраструктуры (ВОЭИ) в зоне ответственности ОБСЕ. ОБСЕ обязалось заняться вопросом террористических атак на ВОЭИ во время конференции ОБСЕ в Мадриде в ноябре 2007 года. Тем не менее, чтобы иметь устойчивые и надежные значения, отслеживание инцидентов, которые подрывают, ослабляют и разрушают важнейшие объекты инфраструктуру, должно охватывать, помимо прочего, следующие виды инцидентов:

- Умышленные нападения;
- Сбои технического характера или сбои, произошедшие вследствие случайной человеческой ошибки;
- Подрыв или разрушение важнейшего объекта инфраструктуры из-за стихийного бедствия;
- Ущерб коммерческого или политического характера.

Недавние события

Защита важнейшей инфраструктуры – основа безопасности энергоснабжения и стабильности мировых цен. Цены на энергию во времена нехватки [низкие в настоящее время цены на энергию из-за мирового спада являются ничем иным, как отклонением от будущего роста цен на энергию] особенно уязвимы даже к небольшим атакам на мировое энергоснабжение в отношении объектов инфраструктуры, которые служат транзитом. Как отмечают исследователи Центра исследования безопасности в Цюрихе, «основными факторами роста цен на сырую нефть с 2004 года по середину 2008 года могут служить рекордный спрос из-за глобального экономического бума, неэластичность цен и сжатые объемы поставок. Тем не менее, политическая нестабильность в странах-производителях еще больше усложнило эти трудные условия. Подобная турбулентность привела к тому, что аналитики называют безопасностью или «надбавкой за риск» – колеблясь от 4 долларов США до 25 долларов США за баррель – которая добавлялась к ценам на сырую нефть в течение данного периода времени. На самом деле, во время данного периода можно обнаружить прямую связь между атаками на объекты энергетической инфраструктуры (ОЭИ) и мировым повышением цен энергию, осуществляемым трейдерами и перекупщиками, которые рассматривали нацеливание на ОЭИ как угрозу для энергоснабжения и, вероятно, как возможность для повышения цен». Вкратце, избирательное нацеливание на ВОЭИ со стороны террористов, криминальных банд или групп, стремящихся использовать давление на правительства стран для достижения политических, экономических или социальных задач через нацеливание на энергетическую инфраструктуру внесло значительный вклад не только в процесс докризисного повышения цен на энергию (2004-2008 гг.), но и в непостоянство цен в последние годы (как для потребителей, так и для производителей).

Система стратегии ОБСЕ по энергетической безопасности

Участие ОБСЕ в вопросах энергетической безопасности основано на Маастрихтском стратегическом соглашении 2003 года, одобренном в декабре 2003 года на Маастрихтском совете министров. В данном документе отмечается, что высокий уровень энергетической безопасности требует прогнозируемого, надежного, экономически приемлемого, коммерчески здравого и экологически приемлемого энергоснабжения. В нем также подчеркивается необходимость обеспечения безопасности энергетических маршрутов.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

В 2006 году в Брюсселе Совет министров принял более сфокусированный подход, подчеркивая важность энергетического диалога с партнерскими организациями, такими как Энергетическая хартия и Международное энергетическое агентство.

Совет отметил, что концепция ОБСЕ по энергетической безопасности касается не только безопасности энергоснабжения, но и включает в себя безопасность энергопотребления и безопасность транзита, а также эффективность использования энергии. Во время бельгийского председательства в 2006 году, Председатель также попросил Секретариат ОБСЕ осуществить техническую миссию для сбора и анализа информации по энергетической безопасности в пределах зоны ОБСЕ и представить рекомендации по возобновленному международному диалогу.

Данное поручение было вновь подтверждено в Афинах 2 декабря 2009 года, когда был выражен призыв к интенсивному диалогу и сотрудничеству в области энергетической безопасности, тем не менее, без указания каких-либо конкретных положений, в которых следует разработать практические механизмы, которые поведут процесс диалога далее. Разработка базы данных для детализации и отслеживания событий, которые воздействуют на жизненно важную энергетическую инфраструктуру, в пределах зоны ОБСЕ и за ее пределами, придаст стремлениям ОБСЕ форму материального результата.

Почему ОБСЕ?

Страны-поставщики, транзитные страны и страны-потребители энергии – все имеют ясный национальный интерес в целостности трансграничных энергетических потоков. Отслеживание и детализация сбоев европейских сетей энергоснабжения – это основа в защите данных интересов. Разработка отдельного и хорошо определенного аналитического инструмента, под протекцией ОБСЕ, для лучшего понимания, оценки и предотвращения будущих событий с негативным воздействием на ВОЭИ, станет полезным для всех стран-участниц ОБСЕ.

Несколько других международных структур предприняли или планируют инициативы по предотвращению сбоев. В 2007 году страны АТЭС рассмотрели региональную инициативу для разработки системы быстрого реагирования для защиты ВОЭИ. Организация Североатлантического договора также получила полномочия по защите важнейшей инфраструктуры в своем регионе. Тем не менее, восприятие роли НАТО в защите важнейшей энергетической инфраструктуры отличается от одной страны-участницы к другой, и, таким образом, это затруднило достижение консенсуса по этому вопросу.

ОБСЕ, как отмечалось, является организацией, в которой много стран-участниц. В то время как некоторые страны-участницы НАТО могут рассматривать разработку и полезность этой базы данных изначально как обязанность международных нефтяных компаний (МНК), что отличается от многих участниц ОБСЕ, где энергоснабжение находится в руках государственных компаний. Кстати, это отражает форму собственности большого количества нефтегазовых активов и их запасов по всему миру (т.е. государственные активы и активы, находящиеся в частной собственности и управлении) и эквивалент распространяется на форму собственности большей части нефтегазовых активов в зоне ОБСЕ. ОБСЕ предлагает различный ряд перспектив и приоритетов, позволяя применять большую степень влияния в рамках ее комплексной структуры. Следовательно, делается выбор в пользу ОБСЕ в качестве места для разработки инфраструктурной базы данных по жизненно важным объектам энергетической инфраструктуры (ИБД ВОЭИ).

В отличие от Экономической комиссии ООН для Европы, которая также проводит энергетический диалог, ОБСЕ имеет мандат безопасности и, как таковая, может охватить много мероприятий, таких как разработка фактического механизма, в данном случае в форме ИБД ВОЭИ, для предотвращения, смягчения или помощи в реагировании на проблемы, с которыми сталкиваются производители энергии, транзитные страны и конечные пользователи, и которые касаются инфраструктуры.

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Несколько государств, поставляющих энергию, являются участниками ОБСЕ и могут осуществить конкретный и совместный шаг вперед для обеспечения своих собственных внутренних энергетических ресурсов и объектов инфраструктуры, через которые они идут транзитом.

Что такое инфраструктурная база данных и почему это важно?

База данных важнейшей инфраструктуры является по существу интеллектуальным средством, основанным на знаниях. Она содержит информацию, полученную от несобственных информационных ресурсов, которые отслеживают и максимально детализируют атаки по всему миру, которые были нанесены жизненно важным энергетическим активам. Эта база данных приведет к возможности осуществлять последовательный анализ нападений на ВОЭИ в мировом масштабе. В общем, если нельзя предсказать конкретное нападение на конкретный объект, можно оценить вероятность формы нападения, на основании эмпирических аналитических инструментов.

При отборе и импорте информации в базу данных является достаточной несобственная информация, так как она охватывает примерно 95% от всех инцидентов, имевших место в отношении данной инфраструктуры. Кто-то может поспорить, что наиболее важными являются оставшиеся пять процентов. Данные инциденты обычно детализируются национальными службами разведки и обороны, но задача базы данных – это, в первую очередь, анализ тенденций, а не конкретный анализ инцидентов. Для этого существует хороший прецедент.

В то время как ИБД ВОЭИ можно сформировать с нуля, ее также можно получить на основе существующей программной платформы. Может быть применена трансфертная модельная база данных SIPRI (Стокгольмского международного исследовательского института мира) для отслеживания и детализации инцидентов энергетической инфраструктуры. База данных SIPRI пользуется уважением среди военных структур по всему миру, и она также использует несобственные источники информации.

Во-вторых, государства-участники ОБСЕ могут возражать против отбора и ввода информации об инцидентах, связанных с энергетической инфраструктурой на глобальном уровне, сосредоточиваясь исключительно на инцидентах, которые имеют место в зоне ОБСЕ. Это будет ошибкой. Если террористические действия совершаются в отношении физических лиц или объекта инфраструктуры, документируется миграционный характер веществ, используемых для осуществления атак. Например, самодельные взрывные устройства, использовавшиеся в Ираке, являются сейчас широко используемым орудием в Афганистане. Таким же образом формы атак на энергетические активы и объекты инфраструктуры «мигрируют» из одного «театра» в другой или даже в пределах конкретных «театров». Государствам и энергетическим компаниям важно знать, от чего необходимо защищаться (тактически), и именно это указывает, на что будет произведена атака (цели). ИБД ВОЭИ поможет выполнить обе эти задачи посредством их детализации на эмпирической основе.

В-третьих, нельзя избежать спорного вопроса «сбоя». Страны-потребители заинтересованы предоставить себе самим максимально возможные объемы информации, если сбой коммерческого характера приводит к значительному сбою в энергоснабжении. Коммерческие сбои могут иметь такие же масштабы последствий, как и технические сбои, аварии или террористические атаки. База данных, как механизм, основанный на практической информации, не предполагает в качестве результата определение политических факторов, которые ведут к определению дефекта в случае коммерческого спора. Отдельные пользователи могут прийти к своим собственным заключениям. ИБД ВОЭИ будет просто заносить данные о воздействии сбоя системы энергоснабжения на страны-производители, транзитные страны и страны-потребители в эмпирическом отношении.

В-четвертых, необходимо рассматривать и включать в базу данных об инцидентах вопрос кибер войны и атак, осуществляемых в отношении ИТ инфраструктур, которые контролируют энергетические системы. Франк Умбах и его коллеги из Центра стратегий европейской безопасности в Мюнхене детально исследовали кибер аспект проблем энергетической безопасности.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Франк отмечает: «Обеспокоенность западных правительств и компаний вопросом безопасности в плане увеличения числа кибер атак отдельными лицами, криминальными организациями и обеспокоенность правительств шпионскими или вредными программами, которые наносят ущерб процессам и активам жизненно важной инфраструктуры выросло в последние годы значительно. Эти кибер атаки достигли беспрецедентного уровня совершенства. Как следствие, значительно увеличилась уязвимость цифровых систем и сетей. Тем не менее, общественная осведомленность не шла в ногу с этими новыми угрозами и уязвимыми сторонами кибер пространства, что может иметь последствия для всех секторов государственной и частной жизни, национальных и международных компаний и даже для оборонных стратегий государств, многонациональных организаций, таких как ЕС» и, соответственно, ОБСЕ. Можно прийти к заключению, что ИБД ВОЭИ без информации о кибер атаках станет анафемой для полного анализа рисков, с которыми сталкиваются ВОЭИ в рамках существующих угроз.

Если энергетическая безопасность является темой, характерной для государств, коммерческих предприятий и политиков, занятых оценкой последствий сбоев важнейших объектов инфраструктуры и энергоснабжения для гражданского общества, тогда диалог и информированные действия должны иметь место для рассмотрения установленных угроз. Сам по себе диалог будет недостаточным. Большее наличие информации может сказать всем участникам об их индивидуальной роли и вкладе в укрепление данной среды безопасности во имя общего блага. Секретариат ОБСЕ, возможно, захочет принять данную рекомендацию к сведению.

Примечание: *Д-р Кевин Роснер является старшим исследователем Института анализа глобальной безопасности, Вашингтон, округ Колумбия, а также главным редактором онлайн журнала по энергетической безопасности*

Защита важнейшей энергетической инфраструктуры в секторе электроснабжения и газа: кибер угрозы в отношении центров энергетического управления

Д-р Франк Умбах, старший член-корреспондент, международная энергетическая безопасность, Центр европейских стратегий безопасности (CESS), Мюнхен-Берлин

Окружающая среда 21 века, представляющая собой угрозу для компаний и правительств

Хотя мировая энергетика и многие правительства обладают большим опытом в обеспечении промышленной безопасности, борьбы со стихийными бедствиями, профилактики нанесения ущерба энергетическим потокам и их нарушения, растущая изощренность мирового терроризма и рост кибернетических возможностей отдельных хакеров при совершении злоумышленных действий, организованная преступность и террористические группы представляют собой новые проблемы, в быстроизменяющейся системе мировой безопасности. Хотя необходимость в традиционных мерах безопасности («оружие, ограждение и охрана») пока не отпала, их недостаточно, чтобы справиться с новыми рисками и угрозами, появляющимися в результате быстрых изменений в окружающей среде, представляющей собой угрозу безопасности.

За последние годы, уязвимость цифровых систем и сетей росла по экспоненте, тогда как уровень осведомленности об этом широкой публики отставал от этих темпов появления новых угроз и уязвимостей в киберпространстве. Но эти угрозы могут оказывать потенциальное влияние на все секторы частной и общественной жизни, национального и международного бизнеса, и даже на политику безопасности государств и международных организаций, таких как ОБСЕ.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

В старой, как мир, борьбе между тем, кто нападает и тем, кто защищается, у нападающего преимуществ больше, чем когда-либо, ибо он лучше вооружен, сам выбирает силу нападения, а также цель, и больше не связан географическими расстояниями или границами. Эти угрозы бросают вызов традиционным допущениям и размышлениям как о национальной, так и о коллективной безопасности. Взять хотя бы, появление бот-сетей: заражение вирусом, находящимся в неактивированном состоянии и незамеченным Интернет-пользователями, который может быть активирован хакером в любой момент (троян), и в любой точке мира, позволяет преступникам или террористам запускать крупные враждебные операции, направленные на получение данных с помощью шпионажа, их фальсификацию, разрушение или изменение секретной информации с чрезвычайно вредными последствиями для промышленности, а также для жизненно важных национальных инфраструктур, а проводя границу между киберпреступностью, кибертерроризмом и кибератаками отдельных лиц, новые «несвященные союзы» преступных синдикатов, террористов или националистических движений и отдельных лиц увеличили угрозу «цифрового Перл-Харбора» при нанесении новой формы «ассиметричного удара» в 21 веке.

Усилия ЕС с 2004 года

С 2001 года в ЕС росло понимание необходимости защиты важнейшей инфраструктуры как существенного и увеличивающегося риска для национальной и международной безопасности, которой должны заниматься государства-члены ЕС как по отдельности, так и коллективно. Но препятствием стал тот факт, что отдельные государства-члены традиционно разрабатывали свои собственные индивидуальные подходы, учреждения и программы для того, чтобы справиться с этими новыми проблемами безопасности в целях защиты жизненно важной инфраструктуры, в том числе важнейшей информационной инфраструктуры (ВИИ), несмотря на понимание наличия общих рисков, угроз, уязвимых мест и стратегий по обеспечению жизненно важной (информационной) инфраструктуры. Кроме того, ЕС только ограничил возможности раннего оповещения и реагирования на инциденты - даже на уровне государств-членов ЕС. Равным же образом, не хватает общего управления в рамках Европы и государственно-частных партнерств (ГЧП).

Несмотря на эти недостатки, первый шаг к тому, чтобы обратить внимание на эти общие риски и уязвимые места, а также справиться с выходящим за границы отдельных государств влиянием поврежденной инфраструктуры или ее нарушенных процессов был сделан тогда, когда в 2004 году было образовано Европейское агентство по сетевой и информационной безопасности (ЕАСИБ) с целью улучшить европейскую координацию по информационной безопасности. Более широкая инициатива была проявлена Комиссией Европейского экономического сообщества в конце 2005 года при выпуске «Зеленой книги по Европейской программе защиты жизненно важной инфраструктуры». В декабре 2006г. Европейский Совет утвердил Европейскую программу защиты жизненно важной инфраструктуры (ЕПЗЖВИ), в которой давалось определение принципов, процессов и инструментов ее реализации. ЕПЗЖВИ легла в основу Плана мероприятий по ЕПЗЖВИ, предупредительной информационной системы жизненно важной инфраструктуры (CIWIN), использованию экспертных групп по ЗЖВИ на уровне ЕС, процессов обмена информацией по ЖВИ, процедуры по выработке общего подхода к оценке необходимости улучшения защиты таких инфраструктур и выявления и анализа взаимозависимостей между сильно различающимися жизненно-важными инфраструктурами.

На этом фоне со второй половины 2007 года Комиссия провела тендер на серию исследований по 7-й Рамочной программе ЕС для Генерального директората Европейской Комиссии по вопросам правосудия, свободы и безопасности (JLS), которые включают в себя исследования по инфраструктурам и активам конкретных отраслей.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

В Проекте Октавио, в котором принимало участие Общество центрально-евразийских исследований, ставилось три основных задачи: (1) обратить особое внимание на структуры, функциональные средства и безопасность жизненно-важных объектов (т.е. центров управления) в системах электроснабжения и газоснабжения; (2) обеспечить точную оценку (риска) в отношении центров управления энергетической отрасли по секторам природного газа и электричества и требований к их киберструктуре; и (3) разработать всесторонний подход к улучшению безопасности центров управления энергоснабжением на основе создания критериев и методик оценки, аудита и уменьшения риска для центров управления снабжением ЕС электричеством и природным газом и для их взаимозависимых структур ИКТ (информационно-коммуникационных технологий).

В отношении важнейшей энергетической инфраструктуры ЕС признал существование двух проблем, требующих решения:

Распространение ИКТ высвечивает многочисленные новые сферы безопасности во всех областях нашей жизни, где подразумевается наша от них зависимость. Либерализация рынка и приватизация принадлежавших государству операторов инфраструктуры, а также новые нормативно-правовые акты привели ко все увеличивающейся зависимости промышленности, находящейся в частных руках, и государственных органов от внешних поставщиков товаров и услуг, в том числе от имеющейся в продаже готовой продукции. В то же время почти каждая отдельная услуга прямо или косвенно зависит от бесперебойной поставки электричества. Физические, виртуальные или логические сети возросли по размеру и сложности. В результате роста взаимозависимости между различными важнейшими инфраструктурами, эта зависимость и влияние перебоев со снабжением или нарушений часто не являются очевидными, пока не наступает кризис и не нарушается связь. Даже сбои, отключения и нарушения меньшего масштаба могут иметь драматические последствия и непредвиденные каскадные явления в еще более сложной системе между различными важнейшими инфраструктурами, выходящими за пределы национальных границ («парадокс уязвимости»).

Ранее система энергоснабжения была децентрализованной, и в каждом регионе стояла своя электростанция и местная сеть электроснабжения, которая соединяла производителя с потребителями. Если электростанция выходила из строя, то весь регион оставался без электроэнергии. Когда региональные сети соединились сетями электропередач, безопасность снабжения улучшилась ввиду возможности обмениваться энергией между региональными сетями. Это также экономило финансовые ресурсы, в частности со стороны производителей. Сегодня эти региональные сети расширились за пределы границ отдельных государств, соединив отдельные государства-члены ЕС с перспективой создания общей системы. Это также сэкономило финансовые ресурсы, в частности со стороны производителей. Сегодня эти региональные сети расширились за пределы границ отдельных государств, соединив отдельные государства-члены ЕС с перспективой создания общего либерализированного энергетического рынка по всему ЕС. В то время как это справедливо для электроснабжения и газоснабжения, Европейская система поставки газа по газопроводу, воспринимаемая как “ахиллесова пята" безопасности энергоснабжения для ЕС, охватывает географическую территорию значительно большего размера, при наличии газопроводов, тянущихся на большое расстояние и соединяющих производителя, страны, через которые проходит транзит и страны-потребители.

Функциональные особенности энергетических центров управления и их уязвимость

Эксплуатационные процессы цепочек поставки электроэнергии и природного газа, как и их безопасность и управление, сильно зависят от инфраструктуры ИКТ. Центры управление энергетикой управляют работой электростанций, а также сетей.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Для обеспечения безопасности электроснабжения и газоснабжения и работы огромных сетей электроснабжения и газоснабжения, пересекающих границы стран, требуется руководство сетями и иерархия центров управления (главного, регионального и районного центра управления). Эффективность центров управления при применении методов сбора и обработки данных тесно связана с разработкой и применением ИКТ. Их задачей является:
Измерения и сбор информации с помощью датчиков, в том числе наблюдение со спутников и управление системами газопроводов, электростанций, насосных станций, хранилищ и сетей;
Получение информации: передача необходимой информации от сети в Центр управления и передача команд из Командных центров таким «эксплуатационным» компонентам, как подстанции;

Обработка, выведение на экран и архивирование информации от сетей, генерирование информации по управлению.

В отличие от прошлой вспомогательной функции по управлению работой электростанций и сетей, произошла ее трансформация в сложный инструмент централизованного характера, выполняющий центральную функцию в энергоснабжении. Без этой центральной функции любая операция в цепочках энергоснабжения и газоснабжения, начиная от производства и кончая распределением и снабжением, была бы невозможной. Эффективность и надежность этих Центров управления, в частности Системы командных центров и центров сетевого управления, является существенной и самой большой угрозой в случае физических и электронных нападений. Они могли бы вызвать далеко идущие последствия для других критически важных инфраструктур, а также могли бы привести к серьезным убыткам для компаний на бирже, а также для десятков тысяч потребителей.

Задачи сбора и обработки информации являются элементами SCADA (Системы диспетчерского контроля и сбора данных). С помощью SCADA центры управления могут определить неполадки и произвести их ремонт, предпринять необходимые меры централизованного ремонта и собрать данные по планированию и дальнейшим действиям. Первоначально у каждой электростанции был свой Центр управления, связанный с другими как часть сетевой иерархии. Развитие ИКТ улучшило возможность сочетать различные задачи командной структуры не только для иерархии сетей, но и для различных носителей, таких как электричество, газ, вода или районное отопление, в Центральном командном центре. Последние расширили свои возможности с помощью использования Географических информационных систем (ГИС) для обеспечения географически-ориентированной информации об установках, сетях, транспортных средствах или географических или политических подробностях. Современные системы SCADA используют стандартные интерфейсы и стандартные компоненты (компьютеров с ОС UNIX или Windows). Это улучшило связи в системе и ее эффективность, но также значительно увеличило уязвимость системы для внешних электронных атак.

Перспективы

В дополнение к новым формам террористических атак, отдельным хакерам и (транснациональным) преступным организациям, уязвимость различных отраслевых инфраструктур также возросла, ввиду того, что они гораздо более связаны друг с другом из-за быстрого роста информационных технологий. Инфраструктуры ИКТ в энергетике, транспорте, банковской и финансовой отраслях стали нервной системой нашего современного информационного общества. Нарушения, связанные с ИКТ, могут вызвать во много раз большие нарушения в других местах, отраслях или секторах и оказать воздействие, которое распространяется далеко от района первоначальной поломки, а также выйти за пределы границ государства-члена ЕС.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Их безопасность и устойчивость не может быть обеспечена и улучшена только в чисто национальных рамках нескоординированных стратегий отдельных государств. Кроме того, рыночные силы не стимулируют в достаточной мере частных операторов вкладывать средства в защиту важнейших инфраструктур. Фундаментальной и до сих пор недооцененной проблемой является то, что низкий уровень защиты в некоторых государствах-членах ЕС может увеличить уязвимость других, тогда как параллельно этому, недостаточно систематическое сотрудничество между государствами в Европе существенно уменьшает эффективность профилактических и своевременных контрмер. В то время как проект Октавио был первоначально призван определить угрозы физического и кибернетического характера и уязвимые места для центров управления энергетикой, а также для других инфраструктур в цепочках электроснабжения и газоснабжения, проводимый в настоящее время проект ЕС INSPIRE идет дальше: Он направлен на уменьшение угроз и усиление прочности, а также устойчивости центров управления в энергетике и других важнейших инфраструктурах больших комплексов с помощью повышения безопасности и улучшения охраны систем управления жизненно-важными инфраструктурами больших комплексов.

При ограниченности финансовых и кадровых ресурсов, имеющихся в наличии у операторов для защиты своих инфраструктурных систем, как энергетическая отрасль, так и ее руководство нуждаются в эффективном использовании всех имеющихся в наличии ресурсов с помощью оценки рисков и расстановки приоритетов для надлежащего управления риском. Пока нет возможности 100% защиты объектов и инфраструктуры инженерных сетей от физического нападения или кибернетической атаки, эти угрозы можно минимизировать без того, чтобы жертвовать производительностью или ежедневный эксплуатацией. Профессиональная безопасность и оценка рисков нуждается в оценке системы с точки зрения перспективы ее физической и кибернетической безопасности, SCADA и систем распределенного управления (СРУ), коммуникационной безопасности, безопасности энергетических систем, безопасности распределения, производства и вопросы биологической/химической безопасности в новых концепциях целостно интегрированной безопасности.

Безопасность международной энергетической инфраструктуры

Д-р Брюс Аврилл, основатель и старший партнер Strategic Energy Security Solutions LLC

Одной из основных обязанностей руководителей частных энергетических компаний является обеспечение непрерывности производства. Во многих странах одним из самых значительных рисков являются террористические атаки, которые могут резко снизить либо даже прервать производство на долгое время. Последний опыт в таких странах как Саудовская Аравия, Йемен и в Гвинейском заливе показал, что энергетические объекты представляют собой привлекательные цели для террористов. К сожалению, такие объекты часто легко уязвимы перед атаками террористов вследствие отсутствия связи между функцией промышленной безопасности, выполняемой частным сектором, и функцией внешней безопасности, выполняемой правительствами в стране местонахождения. Так как существенное и продолжительное прерывание производства и дохода от экспорта вследствие террористической атаки очевидно не в интересах ни энергетической компании, ни государства, в котором она находится, описанная выше ситуация далека от оптимальной.

В чем состоит реальный риск прерывания поставки энергии вследствие террористической атаки?

На этот вопрос нет общепринятого ответа. Скорее, ответ зависит от видения респондента, а также географического региона, в котором находится конкретный объект. На одном из полюсов – точка зрения, представленная в отчете Ernst & Young за 2009 г. о стратегических бизнес-рисках в нефтегазовой

«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 № 6/07***

индустрии, в котором «нарушение снабжения» находится на девятом месте в их списке десяти самых опасных рисков. События, которые могут предположительно послужить импульсом для нарушения снабжения, однако были изначально геополитическими, включая региональную незащищенность и нестабильность и/или намеренные прерывания экспортерами энергии в политических целях. Но в отличие от отчета 2008 года возможность атак на трубопроводы, оффшорные установки и танкеры была упомянута особенно, и также было отмечено, что «нефтяные установки [являются] привлекательной целью для недовольных». В отчете 2008 года только один из экспертов, собранных Ernst & Young, предположил, что следует рассматривать риск террористических атак на нефтяные объекты на Ближнем Востоке как часть «движения от символических объектов нападения к экономическим». И хотя осознание рисков террористических атак немного увеличилось, сообщение открытым текстом гласит, что корпоративному руководству не нужно уделять много времени и ресурсов в отношении этого риска.

В противовес этой довольно оптимистической точке зрения большинство сведущих обозревателей считают, что риск успешных террористических атак высок, особенно в отношении энергетических объектов, расположенных в некоторых географических регионах. Это мнение поддерживается тенденцией, заметной в заявлениях на веб-сайтах джихадских движений, а также недавними событиями.

За последние двенадцать лет произошло значительное изменение в заявлениях и публикациях на сайтах касательно мнения джихадистов об энергетических объектах в роли мишеней. Так, в августе 1996 года Усама бен Ладен распространил заявление, в котором ясно указывалось, что энергетические объекты исламского мира не подлежат нападению: «Я бы хотел предупредить своих братьев, моджахедов, сыновей нации, защищать это (нефтяное) богатство и не затрагивать его в битве, поскольку это великое богатство Ислама и большая экономическая сила, которая понадобится исламскому государству, которое мы скоро построим». Разрешалось атаковать иностранный персонал («крестоносцев» и «неверных»), но не саму энергетическую инфраструктуру. И наоборот, в декабре 2006 года Усама бен Ладен взывал к своим последователям сконцентрироваться на остановке добычи нефти любыми возможными способами: «Одной из основных причин, по которой наши враги завоевывают господство над нашей страной – это то, что они воруют нашу нефть; поэтому вы должны прилагать все усилия, чтобы остановить величайшее ограбление в истории природных ресурсов настоящего и будущего поколений…Сконцентрируйте свои операции на этом [добыче нефти], особенно в Ираке и зоне Персидского залива, и тогда из-за этого [нехватки нефти] они вымрут один за другим».

Такая распространяющаяся риторика о необходимости атаковать объекты энергетики отражается в фетвах и других сочинениях в различных источниках. Например, в июне 2004 г. шейх Абдулла Бен Насер аль-Рашид написал фетву под заголовком «Законы планирования ударов по интересам, связанным с нефтью, и обзор законов, относящихся к экономическому джихаду». К сожалению, на Западе не обратили на это внимание до тех пор, пока Аль-Каеда не привлекла к этому внимание в качестве оправдания неудавшейся атаке Абкаика в феврале 2006 г. Также в 2006 году был опубликован «Указ о планировании ударов по нефтяным объектам», который предоставлял всесторонние религиозные и политические аргументы в пользу атак на энергетические объекты. В 2007 году была опубликована статья под названием «Бен Ладен и нефтяное оружие», призывавшая к атакам на нефтяные объекты, поставляющих нефть в США, по всему миру. И наконец, в прошлом году «Указ о планировании ударов по нефтяным объектам» был снова размещен на нескольких джихадских веб-сайтах, а также появилась новая статья, «Аль-Каеда и битва за нефть», гласящая, что Аль-Каеда должна использовать атаки энергетических объектов, чтобы привести к повышению цен на нефть, что нанесет вред экономике США.

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

За тот же период времени цепочка террористических атак показывает, что распространяющаяся риторика пала зернами на благодатную почву. Атаки на энергетические объекты, фактически достигшие стадии исполнения (хотя с различными степенями успешности) включают: использование загруженной взрывчаткой шлюпки для атаки на французский танкер, M/V Limburg, недалеко от берегов Йемена в октябре 2002 г., что нанесло значительный ущерб судну; атака на поселок Оазис в Аль-Хобаре, Саудовская Аравия, в мае 2004 г., где погибли 19 иностранных сотрудников нефтяных компаний; предотвращенная в последний момент бомбовая атака двух автомобилей на крупнейшем в мире нефтяном объекте, Абкаик, Саудовская Аравия, в феврале 2006 г.; и провалившаяся атака на Йеменский НПЗ в сентябре 2006 г. Также несколько потенциальных атак были раскрыты и предотвращены на стадии планирования, включая: план атаки австралийской электросети в апреле 2004 г.; наблюдение за нефтехранилищами в Австралии и США в 2005 г. и 2006 г., соответственно; и угроза НПЗ Рас Танура в Саудовской Аравии и Бахрейне в октябре 2006 г. Скорее всего, еще несколько других таких угроз были раскрыты, но не афишировались, по очевидным причинам.

Конечно, энергетическая инфраструктура представляет собой потенциально привлекательную мишень для различных террористических групп, помимо тех, которые мотивированы джихадской риторикой. Как указывалось другими, относительно низкая стоимость такой атаки, как с материальной стороны, так и со стороны задействованного персонала, представляет собой хорошую возможность для небольшой группы нанести удар, несоизмеримый с размером их организации. Например, «Одна небольшая атака на нефтепровод в юго-восточном Ираке, выполненная примерно за $2 000, стоила правительству Ирака более $500 млн. в виде потерянной прибыли от продажи нефти. То есть доходность инвестиции составила 25 000 000%». Также, принимая во внимание большую протяженность энергетической инфраструктуры, такой как трубопроводы, фактически невозможно защищать их эффективно, что точно отражается в термине «мишень длиной в десять тысяч километров». Имеется огромное количество показательных примеров, таких как: постоянные атаки Движения за освобождение дельты Нигера (MEND) на нефтяную инфраструктуру и персонал в Гвинейском заливе; сотни атак Национальной освободительной армии (ELN) на трубопровод Каньо Лимон-Ковеньяс в Колумбии за последние двадцать лет; и организованные атаки на мексиканские трубопроводы, предположительно Народно-освободительной армией (EPR) в 2007 г. Также Курдистанская партия рабочих (PKK) взяла на себя ответственность за взрыв и последовавший за ним пожар на турецкой части трубопровода BTC в ноябре 2008 года, хотя турецкие власти утверждали, что происшествие стало результатом механической поломки.

Так как сущность террористических организаций, так же как и их факторы мотивации, ресурсы и возможности разнятся в зависимости от географического региона, невозможно сделать общие выводы о рисках террористических атак на каком-либо обобщенном энергетическом объекте. Вместо этого необходимо сконцентрировать внимание на специфических рисках для энергетической инфраструктуры в данном регионе, например, Канаде, Евразии, Индонезии, Латинской Америке и Северной Америке. Из всех перечисленных регионов только канадский анализ отразил мнение отчетов Ernst & Young, придя к заключению, что риски успешной террористической атаки на канадскую энергетическую инфраструктуру довольно низки.

Правительство США очевидно согласно с заключением, что крупные энергетические объекты в некоторых регионах подвержены значительному риску повреждения вследствие террористической атаки. В 2006 году оно утвердило Стратегию всемирной защиты жизненно важных объектов энергетической инфраструктуры (GCEIP). Целями Стратегии GCEIP являлись работа с правительствами выбранных стран в отношении усиления безопасности энергетических объектов, которые важны для всемирного энергетического рынка, а также являются возможными мишенями террористических атак. Хотя подробности программы и страны-партнеры держатся в секрете, понятно, что защита крупных энергетических объектов за рубежом являлась важным приоритетом для администрации Буша.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Расхождение между частной функцией промышленной безопасности и государственной функцией внешней безопасности

Поскольку в большинстве случаев на энергетических объектах имеются очень эффективные программы промышленной безопасности, в большинстве случаев силы безопасности частного сектора вряд ли смогут противостоять решительной атаке хорошо вооруженных террористов. На самом деле, в большинстве стран силы безопасности частных компаний обычно не имеют права носить оружие (помимо личного оружия, и то только в некоторых случаях), а в некоторых компаниях имеются строгие политики, запрещающие ношение оружия во всех помещениях и на территории. В реальности силы безопасности частных компаний сконцентрированы на промышленной безопасности, предотвращении происшествий и смягчении их последствий, контролируя, чтобы доступ к важным объектам имелся только у уполномоченного персонала, а также предотвращая воровство и кражи продукции. Следовательно, неудивительно, что в большинстве крупных энергетических компаний руководители подразделений безопасности отчитываются перед правлением по линии охраны труда, безопасности и окружающей среды (ОТБОС), при этом имеются несколько уровней управления между ними и правлением. При таких обстоятельствах безопасность – всего лишь один из конкурирующих приоритетов для руководителя высшего звена.
В результате почти во всех странах действительная защита от террористической угрозы предоставляется вооруженным персоналом, принадлежащим министерству или агентству страны местонахождения объекта, например, Министерству Внутренних дел. Эти силы несут ответственность за безопасность за периметром объекта и обычно контролируют доступ автотранспорта и людей на воротах. Обычно они работают в тесном сотрудничестве со службой государственной разведки, чтобы определять и уничтожать угрозы до того, как они приблизятся к периметру. В принципе, правительственные войска по периметру должны иметь персонал, оружие и быть обученными отражению атак решительной и хорошо вооруженной группировке террористов, использующих бомбы в машинах и грузовиках, автоматическое оружие и взрывчатые вещества. Однако на практике имеющийся опыт показывает, что правительственные войска редко применяются, даже в странах, которые очень серьезно относятся к риску террористических атак.

Вооруженные правительственные войска не могут предоставлять соответствующую защиту по нескольким причинам. Во-первых, большинство правительств стран, имеющих богатые углеводородные запасы, еще не выделили отдельное министерство или департамент, который бы нес ответственность за безопасность энергетических объектов, а также имел достаточные полномочия для реализации эффективных мер безопасности. Во-вторых, подача непроверенной информации и конкуренция между министерствами препятствует сотрудничеству и обмену информацией между всеми сторонами, участвующими в вопросах безопасности. В-третьих, полномочие принимать решения касательно реагирования на атаку обычно ограничено офицерами относительно высокого ранга, а не делегируются младшим офицерам или сержантскому составу, которые будут отражать всю тяжесть атаки. В результате никто не сможет или не примет решение в реальном времени, чтобы отразить атаку, эффективно парализуя защиту. В-четвертых, и в конечном итоге, необходимо побороть господствующие настроения «это не может случиться здесь», или «если это случится, такова воля божья, и ничего не поделаешь» (в некоторых мусульманских странах).

Следовательно, топ-менеджеры энергетических компаний, владеющих или управляющих зарубежными объектами со значительным риском нападения террористов, стоят перед дилеммой: они не могут принять эффективные действия в пределах периметра объекта, и при этом они знают, что силы за пределами периметра вряд ли будут эффективными. До тех пор, пока эти обстоятельства не изменятся, руководству придется полагаться только на удачу. Тем не менее, если произойдет успешная террористическая атака, менеджеры окажутся в затруднительной ситуации, так как им придется доказывать правлению и акционерам, что они продемонстрировали добросовестность и адекватно распорядились своей фидуциарной ответственностью.

«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 № 6/07***

Если все признают, что статус безопасности на многих энергетических объектах неудовлетворителен, почему это неудовлетворительное состояние дел никак не меняется? Что мешает или задерживает произвести значительные улучшения безопасности? В большинстве случаев можно определить несколько факторов. Во-первых, во многих странах частный оператор является партнером национальной нефтяной компании, и отношения между ними часто бывают деликатными и сложными. Предположение, что правительство не в состоянии обеспечить должный уровень безопасности представляется недипломатичным и возможно создаст больше проблем, чем решит. Во-вторых, руководители служб безопасности частного сектора часто чувствуют, что они «делают все, что могут», и что они жестко ограничены бюджетными рамками. Как указывалось выше, во многих компаниях безопасность конкурирует с охраной труда и окружающей среды за один источник ресурсов, и директор ОТБОС может легко отдать предпочтение другим вопросам. В-третьих, специалисты по безопасности имеют тенденцию полагаться на знакомые подходы и испытанные решения, и часто они внутренне не доверяют новому и неизвестному. Это может привести к печальной ситуации, когда «делается одно и то же, снова и снова, но ожидаются другие результаты» (содержательное определение безумия Альбертом Эйнштейном).

Использование государственно-частных партнерств для преодоления расхождения

Стратегия GCEIP США предлагает потенциальную модель развития государственно-частных партнерств для преодоления расхождения между частными и государственными силами безопасности, и повысить безопасность энергетических объектов во многих странах. Эта стратегия была основана на межправительственных договоренностях, стимулирующих государства, в которых есть жизненно важные энергетические объекты, повышать безопасность, предоставляемую как правительством, так и частным оператором, с помощью и консультациями USG, что гарантирует достижение результатов, т.е. повышения безопасности. Главным аргументом служило то, что долгосрочный простой крупного энергетического объекта не входит ни в интересы страны местонахождения объекта, ни в интересы США, а также то, что инвестирование небольшой части прибыли страны местонахождения от ископаемого топлива в повышение безопасности представляет собой эффективную политику страхования для минимизации риска потери этой прибыли. Такой подход оказался исключительно эффективным, и фактически все страны, к которым обратились с этим предложением, согласились понести большие расходы на повышение безопасности энергетических объектов, либо в сотрудничестве с USG, либо с частной охранной фирмой. Обычно страна местонахождения объекта ставила условием, что оператор объекта несет ответственность за физические усовершенствования безопасности периметра, а также безопасности в пределах периметра, в то время как государство несет ответственность за безопасность за пределами периметра, включая вооруженные силы, обеспечивающие защиту периметра.

Описанная выше модель разделения ответственности между операторами объекта и страной местонахождения объекта подходит многим другим странам, с небольшими видоизменениями, в зависимости от величины прибыли от экспорта углеводородов. В случае с крупными экспортерами, такими как Катар, Ангола и Казахстан, текущие или планируемые доходы от экспорта СПГ и нефти таковы, что вопрос о том, смогут ли эти страны позволить себе улучшение безопасности периметра на основных площадках, которые во многих случаях в настоящее время остаются незащищенными, даже не стоит.

И наоборот, такая страна как Оман, где чистый экспорт нефти составляет 700 000 баррелей в день, не считается крупным экспортером. Хотя доходы Омана от экспорта углеводородов значительно ниже, чем в вышеупомянутых странах, они, тем не менее, составляют 75% прибылей Султаната.

Такая ситуация – палка о двух концах: с одной стороны, у правительства Омана чистый доход, который можно инвестировать в повышение безопасности, меньше, но с другой стороны эта страна особенно уязвима в случае потери этого дохода.

«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 № 6/07***

Например, по текущим ценам, прерывание экспорта примерно 550 000 баррелей в день, которые Shell добывает в Омане, будет стоить Оману и Shell примерно $24 млн. и $14 млн. в день соответственно, в дополнение к расходам на восстановление, экологическую реабилитацию, и (для Shell) потенциальные потери от снижения стоимости акций. Хотя Shell будет продолжать получать деньги от своих операций в других странах, у Омана такой возможности нет, и продолжительное прерывание экспорта будет катастрофическим для Султаната. В таком случае, как с Оманом, никто не может предположить, что государство местонахождения объекта будет автоматически нести все расходы по повышению безопасности внутри и за пределами периметра объекта. Однако, принимая во внимание относительно открытые границы и общество Омана, и его соседство с потенциальными источниками терроризма, такими как Йемен, Саудовская Аравия и Иран, появляется очень сильный аргумент в пользу развития государственно-частного партнерства с целью повышения безопасности энергетического объекта в сотрудничестве с такими операторами как Shell. Детали разделения расходов необходимо обсуждать.

Основное требование к этому подходу – это присутствие функционального центрального правительства, способного вступить в такой договор и выполнять взятые на себя обязательства в отношении усовершенствований безопасности энергетической инфраструктуры. К сожалению, не все производители энергии соответствуют этим критериям. В качестве примера на ум приходит ситуация в Нигерии, где нефтедобывающие регионы в большинстве случаев неконтролируемы, а верховенство закона – под вопросом. Если нынешние попытки нигерийского правительства призвать к порядку мятежников MEND с помощью амнистии увенчаются успехом, а также, если оно сумеет обуздать коррупцию и дать региону эффективное управление, то, возможно, получится распространить концепцию государственно-частного партнерства на решение даже этой, ранее трудноустранимой, проблемы.

***Примечание**: Доктор Брюс Аврилл является бывшим старшим координатором Политики по защите жизненно важных энергетических объектов в Государственном Департаменте США. Эта статья была впервые опубликована в журнале «Journal of Energy Security» в октябре 2009 г.*

Тернистый путь к безопасной «интеллектуальной электросети»

Дэвид Бейкер, начальник отдела обслуживания компании IOActive

С внедрением технологии Smart Grid («интеллектуальная электросеть») схемы распределения электроэнергии быстро принимают более изощренный вид. «Интеллектуальная электросеть» позволяет экономить деньги и ресурсы и в то же время вести более качественный учет расхода энергии. Однако, как и в случае со всеми новыми технологиями, крайне важно рассмотреть все эффекты от использования «интеллектуальной электросети» и ее компонентов. Опыт показывает, что технологии, рано вышедшие на рынок, часто подвержены уязвимостям с точки зрения безопасности, что делает их основной целью атак.

«Интеллектуальная электросеть» подсоединяет местную систему электроснабжения к национальной энергетической инфраструктуре. Такая сеть распределения характеризуется двунаправленностью потоков электроэнергии и информации, что позволяет наблюдать за всеми ее компонентами: от электростанций от бытовых устройств отдельных пользователей. Используя преимущества технологий распределенных вычислений и отказоустойчивого обмена данными, такая сеть обеспечивает доступ к информации в режиме реального времени и позволяет практически мгновенно балансировать подачу электроэнергии на уровне отдельных устройств.

Важнейшим компонентом «интеллектуальной электросети» является расширенная измерительная инфраструктура, или сеть интеллектуальных датчиков, которая действует одновременно как средство распределения и как конечная точка в системе обмена данными и измерительных узлов. Интеллектуальные датчики обладают беспроводным сетевым интерфейсом и сетевым программным

«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 № 6/07***

обеспечением. Предприятия коммунального обслуживания могут автоматически обновлять программное обеспечение на этих устройствах, а также отключать от сети отдельных потребителей в удаленном режиме (т. н. дистанционное отключение).

Интеллектуальные датчики в перспективе помогут коммунальным службам и потребителям лучше управлять распределением, выработкой и использованием электроэнергии, а также обеспечат экономию и повысят качество предоставляемых услуг. В теории звучит отлично — однако насколько надежны такие датчики?

По сути, интеллектуальные датчики являются маленькими компьютерами. Однако на многих из них отсутствуют средства защиты и обеспечения безопасности, ставшие привычными на современных компьютерах и в сетях. Равно как и компьютеры с программами, разрабатывавшиеся годы назад, эти устройства создавались без учета требований к безопасности, что подтвердило исследование компании IOActive, в котором были рассмотрены некоторые из подобных интеллектуальных измерительных устройств.

Помимо стандартных видов уязвимостей, экспертам IOActive также удалось добиться выполнения на стандартных интеллектуальных датчиках концептуального программного червя. С учетом того, что радиоблок интеллектуального датчика является открытой разработкой, а в протоколах обмена данными отсутствуют функции проверки подлинности и авторизации, экспертам IOActive удалось воспользоваться этими уязвимостями (в числе других) и создать концептуальную программу-червь. Если бы злоумышленнику удалось установить вредоносную программу всего на один датчик, он смог бы заставить встроенную в датчик микропрограмму отправлять на смежные датчики команды, которые в конечном итоге привели бы к заражению этой программой всех датчиков в области действия.

Заразив червем некоторое количество датчиков, злоумышленник теоретически получает следующие возможности:

- подключение и отключение потребителей в заранее определенное время;
- изменение данных измерений и калибровочных констант;
- изменение частоты, на которой датчик производит обмен данными;
- перевод датчика в состояние непригодности.

После заражения действительно вредоносным червем датчиков в определенной области становятся возможными «хороший» и «плохой» варианты развития событий. Согласно «хорошему» сценарию, коммунальная компания отправила бы на все зараженные датчики по стандартной беспроводной сети обновление микропрограммы, которое перезаписало бы червь и вернуло датчики к нормальной работе.

По «плохому» сценарию, стандартный механизм обновления оказался бы недоступен либо была бы сбита калибровка датчиков. Если бы датчики поддерживали возможность дистанционного отключения, их можно было бы настроить на одновременное отключение от электросети всех потребителей. Чтобы возобновить подачу электроэнергии в их дома, коммунальной компании пришлось бы потратить время на то, чтобы выяснить причину проблемы, разработать исправление, а затем физически восстановить или заменить все датчики. Возобновление электроснабжения, вероятно, оказалось бы дорогостоящей и продолжительной процедурой — разорительной для компании и крайне неприятной для потребителей.

Если масштабировать эту ситуацию, с помощью «интеллектуальной сетки» террористы смогли бы отключить подачу электричества в большом районе, чтобы затем потребовать от поставщика коммунальных услуг «выкуп» либо даже выдвинуть политические требования. В более мелком масштабе этой уязвимостью могли бы воспользоваться преступники, отключая от электроснабжения отдельные дома и проникая в них либо просто доставляя хозяевам неудобства.

Несмотря на эти уязвимости, действительность такова, что расширенная измерительная инфраструктура пришла к нам надолго. Поэтому встает вопрос: как устранить все эти присущие ей недочеты в плане безопасности и воспользоваться преимуществами интеллектуальной системы электроснабжения?

Специальный бюллетень CTN

январь 2010

Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Важнейшая роль в обеспечении безопасности «интеллектуальной электросети» принадлежит поставщикам коммунальных услуг. Они в состоянии стимулировать конкуренцию на рынке малых датчиков и гарантировать использование лишь качественных и хорошо защищенных устройств.

Постоянно проверяя безопасность, качество и надежность интеллектуальных измерительных устройств в течение всего срока их службы, коммунальные компании будут способствовать дальнейшему совершенствованию их защиты.

Стремясь помочь изготовителям в разработке более защищенных датчиков, способных противостоять атакам, компания IOActive предлагает им внедрять технологию цикла безопасной разработки программного обеспечения (Safe Development Lifetime, или SDL). Эта технология реализует превентивный подход к вопросу обеспечения безопасности и задействует защитные средства на всех этапах разработки, а также предполагает финальную проверку перед окончательным выпуском программного продукта.

Внедрив технологию SDL и придерживаясь ее, изготовители датчиков смогут более успешно устранять проектные изъяны в интеллектуальных измерительных устройствах и реализовать основное правило безопасности: защита должна быть многоуровневой. Несколько уровней защиты обеспечивают большую безопасность благодаря тому, что при сбое одного механизма закрыть брешь в системе защиты помогают резервные средства. Многоуровневая система защиты крайне важна именно для датчиков, поскольку они находятся за пределами квартир и весьма слабо защищены физически. В отсутствие многоуровневой системы защиты любой достаточно любопытный злоумышленник, обладающий базовыми знаниями в области электроники, сможет выкрасть такое устройство, вскрыть его технологию и обнаружить уязвимости, которыми можно воспользоваться.

Надежное шифрование, проверка подлинности и авторизация — вот еще несколько уровней защиты, которые плохо реализованы во многих интеллектуальных измерительных устройствах. Эксперты компании IOActive выяснили, что во многих датчиках перед выполнением важных функций, таких как обновление ПО или отключение потребителя от сети, не используется шифрование либо отсутствует проверка подлинности. В тех датчиках, в которых алгоритмы шифрования присутствуют, эксперты IOActive обнаружили, что эти функции фактически неуправляемы: ключи часто лежат «на поверхности», являются крайне ненадежными либо могут быть получены с использованием простых методов взлома аппаратных устройств.

«Интеллектуальная электросеть» переносит концепцию сети Интернет на сети распределения электроэнергии, что в перспективе совершит переворот в системе электроснабжения и усовершенствует ее. Как и Интернет, «интеллектуальная электросеть» обещает огромные выгоды, однако в то же время ставит нас перед новыми проблемами в области безопасности. К счастью, благодаря непрекращающимся исследованиям работы по обеспечению безопасности инфраструктуры «интеллектуальной электросети» ведутся уже сегодня. Получая поддержку со стороны государства, а также ведущих экспертов в вопросах безопасности и защиты данных, компании-поставщики коммунальных услуг возлагают на изготовителей датчиков ответственность за обеспечение безопасности этих устройств с использованием формального цикла безопасной разработки программного обеспечения и с привлечением сторонних специалистов для проверки надежности продуктов.

Следуя передовым методикам обеспечения безопасности и конфиденциальности данных, коммунальные компании получают в свое распоряжение все преимущества «интеллектуальной электросети», в то же время надежно защищая эту важнейшую инфраструктуру.

Примечание. *Дэвид Бейкер - эксперт по вопросам информационной безопасности, нормативного соответствия услуг передачи и обработки данных, а также архитектур «интеллектуальных электросетей». Бейкер специализируется в области разработки требований к системам безопасности и поиска оптимальных способов управления важнейшими инфраструктурами и системами коммунального обслуживания. по вопросам инфраструктуры расширенных измерений. (www.ioactive.com)*

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Защита нефтяной инфраструктуры

Г-н Умберто Сакконе, начальник службы безопасности, ENI Spa

Сегодня угроза террористических актов, направленных против важнейших объектов инфраструктуры, привлекла внимание к стратегическому вопросу безопасности энергетического сектора и определению потенциально уязвимых мест отрасли. Защита важнейших объектов инфраструктуры на сегодняшний день является ключевой составляющей национальной безопасности нескольких стран, а после 11 сентября 2001 года данная проблема стала центральной темой дебатов по вопросам терроризма и внутренней безопасности в США.

Топливно-энергетические ресурсы как политически, так и экономически являются для нефтедобывающих стран и потребителей нефти стратегическими активами. Говоря о нефтепроводах, страны, в которых расположены такие активы (транзитные страны), считаются странами первостепенной стратегической важности международного уровня. После окончания Холодной Войны регионы богатые нефтью, такие как Персидский Залив, Каспийский бассейн и южное Китайское море приобретают все большую значимость в стратегическом смысле. В результате этой мутирующей геостратегической тенденции особое внимание уделяется защите ключевых ресурсов, в особенности, нефти и природного газа. Международный терроризм всегда покушался на нефтяные и газовые ресурсы, видя в них удобные политические и экономические мишени для террористических актов.

«Мир нефти» с его корпорациями, соответствующими объектами инфраструктуры и руководством - одна из мишеней, на которую нацелена Аль-Каида и его лидер Осама Бен Ладен. Фактически, свою стратегию Бен Ладен определил еще в 1997 году в интервью с пакистанским журналистом Хамидом Миром: *«Рост цен на нефть незначителен по сравнению с ценами на другие товары. С 1973 года цена на сырую нефть выросла только на 8 долларов США, в то время как цена на некоторые другие товары увеличилась в три раза. Пшеница в Соединенных Штатах, например, подорожала в отличие от цены на арабскую нефть в три раза. Мусульманский мир терпит убытки в 115 долларов США за баррель. Ежедневно 10 миллионов баррелей добывается только в одной Саудовской Аравии. Таким образом, ежедневный убыток составляет свыше одного миллиона долларов США, а общий убыток (включая другие арабские страны) – два миллиона долларов США. Мусульмане во всем мире гибнут в нищете из-за того, что США воруют нашу нефть."*

Принимая во внимание вышесказанное, стратегия Аль-Каиды, однако, столкнулась с дилеммой: как нанести удар по интересам нефтяных корпораций и при этом свести до минимума последствия теракта для интересов мусульманского мира. В своем «Объявлении войны против американцев» в 1996 году Бен Ладен дал четко понять, что моджахеды должны избегать участия в движении боевиков против основных топливно-энергетических ресурсов исламского государства.

Организация террористических актов на месторождениях (на которых зиждется экономика западных стран) в мусульманских странах является, таким образом, основной составляющей стратегии терроризма, которая, однако, вступает в противоречие с мнением, что непоправимый ущерб нефтяным месторождениям нанесет тяжелый урон экономике всего мусульманского сообщества.

Столкнувшись с такой дилеммой, Аль-Каида, таким образом, разработала стратегический план, который предусматривает необходимость избегать атак на нефтяные месторождения, но поощряет террористические акты, направленные против нефтеперерабатывающих объектов, трубопроводов, танкеров, нефтяных терминалов, а также покушения на руководство и сотрудников немусульманских нефтяных корпораций.

По всей видимости, террористический акт Аль-Каиды на нефтеперерабатывающем заводе Абкаик в Саудовской Аравии 24 февраля 2006 года ознаменовал начало новой и более

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Структурированной террористической стратегии, направленной против объектов нефтяной инфраструктуры. Фактически через два дня после теракта, шейх Абд-аль-Азиз бен Рашид аль-Анази, религиозный фанатик, связанный с Аль-Каидой, опубликовал в Интернете доктрину и религиозное обоснование терактов на нефтяных объектах в статье с заголовком «Религиозное правило при организации терактов на нефтяных объектах». Статья преследует цель признать обоснованность легитимного характера террористических актов с религиозной точки зрения, при условии что топливно-энергетические запасы мусульманского мира не испытают на себе последствия терактов. По словам Бен Ладена, саботаж является эффективным оружием, однако теракты на нефтяных месторождениях не допустимы. Разрешены три мишени:

- **Трубопроводы**: определены как «легкая мишень». Выгоды, полученные при уничтожении трубопровода, значительно превышают убытки, понесенные исламским населением.
- **Нефтеперерабатывающие заводы и соответствующие объекты (морские порты, танкеры, нефтяные терминалы)**: только объекты, принадлежащие мусульманам (а не совместным предприятиям) подлежат сохранности.

Личности, играющие выдающуюся роль в нефтяной индустрии: означены как «простейшая мишень». Излюбленная мишень.

Мусульмане не относятся к излюбленным мишеням, однако и они могут стать целью терроризма, если их уничтожение представляется необходимым или несет выгоды.

Ниже представлены некоторые наиболее уязвимые объекты, имеющие отношение к нефтяной отрасли

- **Места добычи и разработки**: зачастую расположены в отдаленных территориях с соответствующими сложными маршрутами и затрудненной коммуникацией с органами власти и структурами, связанными с безопасностью. Когда безопасность месторождения обеспечивается силами национальной безопасности, их численность значительно не дотягивает до числа террористов, к которым зачастую примыкает местное население. Таким образом, такие месторождения представляют собой удобную мишень для террористов.
- **Судна**: морские судна также подвержены риску стать излюбленной мишенью для террористов по ряду причин:
  - Меры безопасности для отражения возможных атак на борту зачастую ограничиваются водоструйными пушками или сиренами.
  - Численность персонала, ответственного за безопасность, как правило, незначительная.
  - Перевозимые материалы, преимущественно, легковоспламеняемы и опасны для окружающей среды.
  - В случае атаки, помощь извне возможна только спустя долгое время.
  - В итоге, танкеры считаются относительно легкими мишенями.
- **Трубопроводы**: транспортировка нефти и газа на большие расстояния осуществляется по трубопроводам. Последние пролегают на поверхности суши и, таким образом, визуально хорошо различимы, или - под землей, но и в этом случае, их местонахождение легко определить. Кроме того, соответствующее вспомогательное оборудование (например, компрессорные станции), как правило, остается незащищенным. На отдаленных территориях уязвимость такого оборудования для террористических актов значительно выше.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

- **Нефтеперерабатывающие заводы**: нефтеперерабатывающий завод представляет собой самый важный актив во всем нефтегазовом цикле. От бесперебойности его работы зависит все национальное энергообеспечение. Значимость нефтеперерабатывающего завода, сложность его вида деятельности, большое количество задействованных персоналий, а также вид продукции – все это является стимулом для развития мер безопасности.

Необходимо отметить, что международные террористические группы могут отвечать современным требованиями логистики для успешной организации терактов, направленных против всей системы розничной торговли нефтегазовой отрасли. Несмотря на то, что потенциальный ущерб для отдельного месторождения представляется незначительным, координированный теракт сразу по нескольким месторождениям может нанести существенный урон всей национальной экономике со всеми вытекающими социо-политическими последствиями.

Все субсекторы нефтегазовой отрасли разных уровней уязвимы для террористической угрозы, поскольку международный терроризм уже доказал свою способность успешно организовывать теракты на месторождениях, трубопроводах, нефтеперерабатывающих заводах и в системе розничной торговли конечного продукта.

Необходимость участия частного сектора в защите жизненно важных национальных объектов инфраструктуры

Дэвид Тейлор-Смит, Генеральный Директор G4S Secure Solutions
(Соединенное Королевство и Ирландия)

С ростом глобальных угроз безопасности защита жизненно важных национальных объектов инфраструктуры (ЖВНОИ) стала важной сферой, в которой государственный и частный секторы должны организовать более тесное сотрудничество. Значимость такого сотрудничества возросла, поскольку правительства уже не способны предоставить ту необходимую всецелую и быстродействующую поддержку, которую они могли обеспечить ранее. Другого выхода, кроме как привлечь в обеспечение безопасности объектов частный сектор, который уже давно занимается финансированием, строительством и производством на жизненно важных объектах инфраструктуры, нет.

Значимость ЖВНОИ подытожил в своем заявлении бывший Президент США, Билл Клинтон, по словам которого: «Жизненно важные объекты инфраструктуры настолько значимы, что их остановка или уничтожение катастрофически ослабит оборону или экономическую безопасность всей нации». Правительственный Центр по Защите Национальных Объектов Инфраструктуры Великобритании выделил девять секторов ЖВНОИ: коммуникации; органы по чрезвычайным ситуациям; энергетика; финансы; пищевая промышленность; органы власти; здравоохранение; транспорт и водоснабжение. Без этих структур любое государство может пострадать тяжелые последствия, в том числе, экономический ущерб, социальную нестабильность или даже человеческую трагедию национального масштаба.

В каждом секторе, особенно в странах, в которых частные финансовые инициативы имели успех, многие элементы ЖВНОИ на сегодняшний день находятся в зоне ответственности (и даже в собственности) частного сектора. Такой значимый сдвиг в контроле производства и в собственности демонстрирует ценность участия частного сектора в строительстве и управлении жизненно важными объектами инфраструктуры. Этот факт обязывает правительства пересмотреть свой подход к защите ЖВНОИ и отрасли и пробудить осознание того, что обеспечение безопасности этих объектов является жизненно важным.

январь 2010

Специальный бюллетень CTN
Защита важнейших объектов энергетической инфраструктуры от террористических актов

«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 № 6/07***

Террористические акты и действия боевиков остаются ключевыми угрозами и проблемами, которые пестреют в заголовках, особенно в свете последних событий в Мумбаи и Лахоре. Сложность взаимодействия с этими угрозами обусловлена их зависимостью от разнородных социальных структур на международных границах и трудностью вычленения тех структур, которые принимают участие в терактах.

Однако, чрезвычайно опасно, если все наши усилия и решения по распределению финансовых ресурсов будут продиктованы исключительно терроризмом. Компаниям необходимо принять во внимание более широкий набор рисков, с которыми они могут столкнуться, начиная со стихийных бедствий и заканчивая ростом преступной политической активности. Разрушения, причиненные ураганом Катрина, цунами в 2004 году или совсем недавними наводнениями во всей Великобритании, создали угрозу для жизнеспособности сообществ и инфраструктуры, от которой они зависят. Компании должны уже сейчас начать подготовку к эффективному отражению растущего распространения этих национальных и международных угроз.

Когда разражается бедствие, предполагается, что именно правительства и государственные органы должны безотлагательно предпринять необходимые меры, восстановить инфраструктуру, возобновить социальную и экономическую стабильность. Мы также склонны обвинять правительство в хаосе и нестабильности, являющимися следствиями событий, которые, как нам кажется, можно было предвидеть, избежать или предотвратить. Однако, в то время как правительства и в действительности оказываются подготовленными к таким событиям, принимая безотлагательные меры в большинстве случаев, реакция органов по чрезвычайным ситуациям и вооруженных сил зачастую оказывается замедленной в силу ограниченности деятельности и бюджета.

Все осложняется тем, что национальные правительства и государственные органы, кроме того, не всегда способны справляться с международными чрезвычайными ситуациями, что объясняется целым рядом причин, начиная от политических и заканчивая неспособностью. Таким образом, где же правительства и госорганы могут изыскать те дополнительные ресурсы, которые смогли бы не только защитить активы, но и обеспечить доступ к угрозам, которым подвергаются активы?

Очевидный ответ - сектор национальной безопасности, который имеет подготовленные ресурсы во всем мире и по роду деятельности - основное право на предотвращение и сведение до минимума последствий разрушений ЖВНОИ.

Компании в данной отрасли уже имеют опыт взаимодействия с подобными задачами, как внутри страны, так и, при необходимости, за рубежом. Мы обеспечиваем безопасность аэропортов, электростанций, водоочистных сооружений и банков во многих странах, а в некоторых из них мы помимо этого ведем строительство и осуществляем управление такими жизненно важными объектами инфраструктуры, как тюрьмы, колонии для несовершеннолетних и центры наличности. Будучи пользователем и одновременно обеспечивая защиту ЖВНОИ, мы можем оказать реальную поддержку правительствам, ищущим пути усиления национальной безопасности.

Итак, что необходимо сделать правительствам? Запустить процесс, который необходим, чтобы принудить все соответствующие организации частного сектора относиться к обеспечению безопасности ЖВНОИ более серьезно путем создания для собственников и управленцев эксплицитных обязательств по обеспечению безопасности своей инфраструктуры, подобные тем, которые правительство Великобритании уже вменило некоторым компаниям в авиационной промышленности и водоснабжении. Такие обязательства могут быть закреплены законодательно или регулятивно: однако в силу того, что они носят необязательный характер, некоторые компании продолжают игнорировать проблему по финансовым и производственным причинам.

«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 № 6/07***

Правительства могут также применить более прагматичный подход в использовании частного сектора для управления, обеспечения безопасности и роста участия в защите ЖВНОИ внутри страны и за рубежом.

В большинстве случаев гибкие, национальные и международные ресурсы частного сектора равнозначны или более ценны, чем ресурсы, которые находятся в распоряжении отдельных правительств, и как таковым им необходимо доверить участие в необходимых мерах безопасности.

Возьмем к примеру G4S. В Северной Америке мы уже доверили компании обеспечение безопасности 50 процентов коммерческих атомных электростанций и оказание помощи по защите значимо уязвимых организаций, таких как Пентагон и НАСА. В Европе мы обеспечиваем безопасность Европейского Парламента, штаб-квартиры НАТО, ряда охраняемых объектов Правительства Великобритании и растущего числа основных международных морских портов и аэропортов, таких как аэропорт Схипхол в Амстердаме и Хитроу Интернэшнл. Кроме того, мы охраняем Посольства и дипломатов Великобритании, США и других суверенных государств в особо опасных точках во всем мире, а также осуществляем своевременный, чрезвычайный трансграничный сервис, который во многом оказался более эффективным, чем усилия отдельных государственных структур.

В дополнение, с учетом того, что государственные органы вынуждены обеспечивать все более точные и упредительные разведданные, организации частного сектора с их мириадой международных сетей предлагают новые пути для обеспечения необходимой разведки, и зачастую предоставляет данные быстрее, чем на то способны отдельно взятые нации. В конечном счете, частный сектор на протяжении уже многих лет пользуется услугами частных агентств безопасности в целях коммерческой разведки. Обеспечение доступа к разведывательным сетям частному сектору диктуется простым здравым смыслом.

Таким образом, частный сектор уже доказал весьма реальные преимущества его участия в предоставлении услуг, имеющих отношение к ЖВНОИ, которые прежде считались исключительной прерогативой частного сектора. В действительности, другой альтернативы, кроме как сотрудничество государственного и частного секторов в вопросах обеспечения безопасности и осуществления строительства жизненно важных объектов инфраструктуры, не существует. Правительства, которые сделали выбор в пользу сохранения *status quo,* а не в пользу привлечения частного сектора в обеспечение безопасности ЖВНОИ, неоправданно рискуют и, в конечном счете, испытывают нехватку собственных ресурсов, и подвергают ЖВНОИ потенциальной угрозе терроризма.

ПРИМЕЧАНИЕ: *Настоящая статья впервые опубликована в журнале GIT Security+Management, издание 5 (апрель 2009 г.)*