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




ОБСЕ Организация по безопасности и сотрудничеству в Европе

ISBN 978-92-9235-022-2

Дизайн: HiSolutions AG
Макет: OTHERVIEW, Watrowicz & Watrowicz GbR
Печать: Ueberreuter Print GmbH
Источник фотографий: fotolia.com / Kanea, B., Wylezich, wellphoto, panomacc

Финансовую поддержку проекту
предоставила Делегация США в ОБСЕ.

Антитеррористическое подразделение Департамента
по противодействию транснациональным угрозам
Секретариата ОБСЕ
Wallnerstrasse 6
A-1010 Vienna
Austria
Телефон: +43 1 514 360, atu@osce.org

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

ОБСЕ Организация по безопасности и сотрудничеству в Европе

Содержание

Вступительное слово

Перед вами Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства. Данное руководство разработано рядом экспертов, представляющих государственный и частный сектор государств — участников ОБСЕ, при участии экспертов из Европейского Союза и Организации североатлантического договора.

Значение мер по обеспечению энергетической безопасности и безопасности энергетической инфраструктуры невозможно переоценить. На сегодняшний день вопросы обеспечения энергетической безопасности и безопасности энергетической инфраструктуры находятся в числе самых насущных проблем, связанных с обеспечением безопасности, защитой экономики и охраной окружающей среды. В последние годы тема защиты важнейших объектов энергетической инфраструктуры от терроризма привлекает все большее внимание международного сообщества. Важнейшие объекты энергетической инфраструктуры являются источником топлива, обеспечивающим развитие глобальной экономики и жизнь общества. Мы зависим от этой инфраструктуры, что делает ее объекты идеальной мишенью для совершения террористических актов. Нарушение инфраструктуры и разрушение ее объектов может оказать серьезное воздействие на защиту, безопасность, экономическое благосостояние и здоровье отдельных людей и общества в целом.

Вопрос защиты важнейших объектов энергетической инфраструктуры от террористических актов представляет особую важность для Организации по безопасности и сотрудничеству в Европе (ОБСЕ), поскольку в эту организацию, представленную 57 государствами-участниками и 11 партнерами по сотрудничеству, входят крупнейшие производители и потребители энергии, а также многие страны, имеющие стратегическое значение при транзите энергии. В ноябре 2007 года государства — участники ОБСЕ одобрили Решение Совета министров о защите важнейших объектов энергетической инфраструктуры от террористических актов [MC.DEC/6/07], приняв на себя обязательства по сотрудничеству и улучшению координации, а также по рассмотрению всех необходимых мер на национальном уровне для обеспечения адекватной защиты жизненно важной энергетической инфраструктуры от террористических актов.

Во исполнение Решения Совета министров MC.DEC/6/7 Антитеррористическое подразделение Департамента по противодействию транснациональным угрозам (АТП ДПТНУ) ОБСЕ провело Экспертный семинар по вопросам государственно-частного партнерства в области защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов, который состоялся в Вене 11-12 февраля 2010 года.

В поддержку реализации решения Антитеррористическим подразделением Департамента по противодействию транснациональным угрозам был инициирован Проект защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов, и было опубликовано настоящее Руководство по передовой практике.

Цель публикации заключается в том, чтобы повысить осведомленность всех заинтересованных сторон о риске террористической киберугрозы, которому подвержены важнейшие объекты неядерной энергетической инфраструктуры, в частности, промышленные системы управления и объекты киберинфраструктуры. Другой ее целью является способствование внедрению передовой практики защиты такой инфраструктуры. В настоящем Руководстве определены основные вопросы и сложности, связанные с реализацией мер по обеспечению безопасности, а также представлены избранные примеры передовой практики в качестве возможных решений. Руководство призвано стать справочным документом, содержащим основную информацию для лиц, разрабатывающих государственную политику, для государственных органов, ответственных за защиту важнейших объектов энергетической инфраструктуры, для владельцев и операторов объектов неядерной энергетической инфраструктуры и для прочих заинтересованных сторон в государствах — участниках ОБСЕ и в партнерах по сотрудничеству.

В этой публикации представлена структура для стимулирования разработки и внедрения приемлемых мер, а также для обеспечения институционального управления вопросами кибербезопасности в отношении важнейших объектов неядерной энергетической инфраструктуры на основе сотрудничества и комплексного подхода (с учетом всех опасностей), построенного на рассмотрении рисков, с особым акцентом на готовности к реагированию на инциденты, общей устойчивости инфраструктуры и надежности энергоснабжения. Рассмотренные вопросы включают: оценку рисков, физическую безопасность, кибербезопасность, планирование действий при чрезвычайной ситуации, государственно-частные партнерства, вовлечение общественности (в том числе особый вклад женского сообщества) и международное/трансграничное сотрудничество.

Алексей Лыженков

Координатор деятельности по противодействию транснациональным угрозам

Выражение признательности

Антитеррористическое подразделение Департамента по противодействию транснациональным угрозам ОБСЕ и его руководитель по антитеррористическим вопросам Томас Вухте выражают свою благодарность следующим государствам — участникам ОБСЕ, экспертам и сотрудникам за их вклад в подготовку Руководства:

Государствам — участникам ОБСЕ, внесшим вклад в подготовку Руководства:

Беларусь, Хорватия, Франция, Германия, Венгрия, Литва, Нидерланды, Румыния, Словакия, Словения, Швеция, Швейцария, Таджикистан, Турция, США

Европейскому Союзу и Организации Североатлантического договора за их поддержку

Членам Консультативной группы заинтересованных сторон, внесшим вклад в подготовку Руководства:

Марио д'Агостини, Федеральное управление сырьевого обеспечения национальной экономики (FONES); руководитель подразделения секретариата по электроснабжению и питьевой воде; швейцарский национальный представитель в Группе промышленных ресурсов и коммуникационных услуг [IRCSG, промышленность] в рамках программы «Партнерство ради мира», Совет евроатлантического партнерства (НАТО); председатель специальной рабочей группы по защите важнейших объектов инфраструктуры в сфере энергетики

Брэд Дэвидсон, аналитик по международным отношениям, Управление по защите инфраструктуры, Министерство национальной безопасности США

Витаутас Бутримас, главный советник по вопросам кибербезопасности Министерства обороны Республики Литва

Шарри Р. Кларк, сотрудник по международным отношениям, Бюро по борьбе с терроризмом, Государственный департамент США

Вильям Флинн, заместитель помощника секретаря, Управление по защите инфраструктуры, Министерство национальной безопасности США

Петра Хохманнова, руководитель CSIRT.SK, DataCentrum – Министерство финансов Словацкой Республики

Хосе Антонио Ойос-Перес, сотрудник по политике, Защита важнейших объектов энергетической инфраструктуры, Европейская комиссия, Главный директорат по энергетике

Даниэль Ионита, CERT-RO Румыния

Мерибет Келлихер, сотрудник по международным отношениям, Бюро по борьбе с терроризмом, Государственный департамент США

Данка Кубикова, старший государственный советник Министерства экономики Словацкой Республики, Словацкая Республика

Ян Лукачин, ABB, s.r.o. Менеджер по продажам, Словацкая Республика

Ричард Прозен, сотрудник по международным отношениям, Бюро по европейским отношениям, Государственный департамент США

Пауль Рейтер, OMV AG, руководитель по корпоративной безопасности и устойчивости

Консультанты проекта:

Хейко Борхерт, управляющий директор, Sandfire AG, Швейцария

Энно Эверс, управляющий консультант по безопасности систем, HiSolutions AG, Германия

Каролин Гримм, консультант по управлению корпоративной безопасностью, HiSolutions AG, Германия

Матиас Кеппе, консультант по управлению корпоративной безопасностью, HiSolutions AG, Германия

Робин Кроха, директор по управлению корпоративной безопасностью, HiSolutions AG, Германия

Александр Папитч, старший консультант по безопасности систем, HiSolutions AG, Германия

Ина Райфферсбергер, консультант по управлению корпоративной безопасностью, HiSolutions AG, Германия

Гордон Шварцер, управляющий консультант по управлению корпоративной безопасностью, HiSolutions AG, Германия

Сотрудники ОБСЕ

Антон Денгг, советник по вопросам борьбы с терроризмом, Департамент по противодействию транснациональным угрозам /Антитеррористическое подразделение, редактор данного издания

Селин Фрейдл, помощник по проекту, Департамент по противодействию транснациональным угрозам /Антитеррористическое подразделение

Мехди Кнани, младший сотрудник по программам, Департамент по противодействию транснациональным угрозам /Антитеррористическое подразделение

Александр Малышев, старший помощник по управлению информацией, группа координации, Департамент по противодействию транснациональным угрозам

Неманья Малишевич, сотрудник по кибербезопасности, группа координации, Департамент по противодействию транснациональным угрозам

Рейнхард Ухриг, заместитель начальника и координатор программ, Департамент по противодействию транснациональным угрозам / Антитеррористическое подразделение

Ласло Сюч, сотрудник по программам, Департамент по противодействию транснациональным угрозам /Антитеррористическое подразделение, редактор настоящего издания

Ричард Вилер, старший сотрудник по программам, энергетическая безопасность, Бюро Координатора экономической и экологической деятельности ОБСЕ

Антитеррористическое подразделение Департамента по противодействию транснациональным угрозам ОБСЕ также выражает благодарность правительству США за финансовую поддержку данного проекта.

1. Краткое содержание

1. Краткое содержание

Объекты национальной и коммерческой инфраструктуры всегда рассматривались противниками в качестве потенциальных мишеней. В древнем мире[1] нападению подвергались пути снабжения городов и стран, а иногда и сами склады запасов. С целью ослабить армию атаковались также пути военных поставок. В прошлом противник совершал атаки, чтобы отрезать доступ к продовольствию и водным запасам или разрушить военные объекты, но в эпоху индустриализации у него появилась новая мишень — энергоснабжение.

В сегодняшнем высоко индустриализованном мире мало что может работать без энергии. Та жизнь, которую мы знаем, не могла бы существовать без энергетической отрасли и была бы обречена на гибель, прервись энергоснабжение на длительный срок. Нашим потенциальным врагам известно об этом.

Поэтому внедрение мер, гарантирующих постоянное наличие энергии, в том числе электричества, является важной обязанностью стран и секторов энергетики. Эту обязанность должны взять на себя и государства — участники Организации по безопасности и сотрудничеству в Европе (ОБСЕ). ОБСЕ является уникальной общеевропейской и трансатлантической организацией, в которую входят высоко индустриализованные и развитые государства — участники и страны — партнеры по сотрудничеству от Северной Африки до Австралии. Эта организация способна решать вопросы безопасности энергетической инфраструктуры, в частности, те из них, которые связаны с угрозами террористических актов и с угрозами, исходящими из киберпространства.

В этом Руководстве рассказывается о значении важнейших объектов неядерной энергетической инфраструктуры для стран и потребителей энергии, и определяются угрозы для такой инфраструктуры. Особое внимание уделяется террористическим актам, исходящим из киберпространства. В руководстве не совершается попытка дать всесторонний анализ угроз или подробно объяснить все меры защиты. Здесь также не рассматривается вопрос о фактической уязвимости или о степени уязвимости определенных стран или операторов важнейших объектов неядерной энергетической инфраструктуры к таким угрозам, поскольку это можно определить только на индивидуальной основе. Скорее, в этом руководстве освещаются методологические вопросы, которые необходимо принимать во внимание при обеспечении защиты важнейших объектов неядерной энергетической инфраструктуры, а также приводятся примеры передовой практики снижения потенциальных уязвимостей.

Примеры передовой практики, представленные здесь, в первую очередь призваны помочь странам в выявлении угроз террористических актов, исходящих из киберпространства, а также в противодействии им. Однако приведенные меры можно адаптировать, расширить и/или применить и в отношении других угроз и других секторов. Такая возможность учитывается по всему тексту руководства.

Далее последует подробный анализ угроз с приведением рекомендаций по повышению готовности и устойчивости к ним. Ниже приведен ряд выявленных нами положительных практик, применение которых можно рекомендовать всем странам и компаниям, эксплуатирующим важнейшие объекты неядерной энергетической инфраструктуры:

1. Повышение осведомленности о значении важнейших объектов неядерной энергетической инфраструктуры и о степени угроз террористических актов, исходящих из киберпространства, а также о других видах потенциальных угроз.

2. Развитие национального и международного сотрудничества между государственными органами и владельцами и операторами важнейших объектов неядерной энергетической инфраструктуры перед лицом угрозы кибератак.

3. Упрощение информационного обмена между государственными органами и операторами важнейших объектов неядерной энергетической инфраструктуры в отношении способов противодействия угрозам кибератак.

4. Обсуждение совместных мер по повышению осведомленности, информационно-разъяснительной работе, партнерству с представителями отрасли и, в соответствующих случаях, установлению адекватных регулирующих стандартов путем использования существующих национальных и международных форумов и, в соответствующих случаях, создания стандартизированных

1 Michael J. Assante: „Infrastructure Protection in the Ancient World: What the Romans can tell us about their Aqueducts – What we may apply to our modern infrastructures", Proceedings of the 42nd Hawaii International Conference on System Sciences (2009), стр. 4

национальных и международных форумов и процессов противодействия террористическим актам в киберпространстве, направленным на важнейшие объекты неядерной энергетической инфраструктуры.

ОБСЕ играет в этих процессах особую роль, поскольку эта организация может действовать в качестве посредника между такими международными организациями, как Европейский Союз (ЕС) и Организация североатлантического договора (НАТО), а также владельцами и операторами важнейших объектов неядерной энергетической инфраструктуры.

2. Террористические акты в киберпространстве, направленные на важнейшие объекты неядерной энергетической инфраструктуры

ОБСЕ Организация по безопасности и сотрудничеству в Европе

2. Террористические акты в киберпространстве, направленные на важнейшие объекты неядерной энергетической инфраструктуры

Точно так же, как существуют разные определения терроризма, существуют и разные определения «кибертерроризма». Реальный вызов для стран и компаний состоит в том, чтобы обнаружить угрозы и выявить преступников, поскольку для жертв обычно важны последствия. Поэтому неудивительно, что попытки определить этот термин концентрируются на последствиях. Ниже приведены два примера определения термина «кибертерроризм»:

«Под кибертерроризмом обычно понимают незаконные атаки и угрозы атаки на компьютеры, сети и на хранящуюся в них информацию в целях устрашения или принуждения государства или его населения и реализации определенных политических или социальных целей». [2]

«Кибертерроризм означает использование инструментов компьютерной сети для нанесения вреда важнейшим объектам национальной инфраструктуры (таких как энергетика, транспорт, государственная деятельность) или прекращения их работы».[3]

В этих определениях упомянуты только атаки на инфраструктуру киберпространства и атаки с использованием киберинструментов. Между тем, термин «кибертерроризм» используется и в более широком контексте. В следующих разделах мы будем определять кибертерроризм как терроризм, связанный с киберпространством, а конкретнее (с учетом наших целей) — как террористические акты, направленные на киберинфраструктуру, в частности, на системы управления важнейшими объектами неядерной энергетической инфраструктуры. Особое внимание мы уделим глобальному и национальному значению важнейших объектов неядерной энергетической инфраструктуры, а также общим и конкретным киберугрозам для них, включая угрозы, связанные с террористическими актами.

2.1 Важнейшие объекты инфраструктуры

Инфраструктура крайне важна для высокоразвитых и эффективных современных обществ, а развитие инфраструктуры является основным показателем экономической конкурентоспособности. В основе процветания и прогресса стран в глобальном мире лежит обеспечение конкурентоспособности, для сохранения которой необходимо защищать важнейшие объекты инфраструктуры.

Защита важнейших объектов инфраструктуры является основной задачей национальной и корпоративной безопасности и всегда должна занимать центральное место в политике безопасности страны. Отсутствие мер по защите важнейших объектов инфраструктуры может иметь серьезные последствия. «Важнейшие объекты инфраструктуры представляют собой организации и предприятия, имеющие большое значение для общества. Нарушения или перебои в их работе могут привести к долгосрочным нарушениям функционирования системы снабжения, значительному

2 Mehmet Nesip Ogun: Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes, Journal of Applied Security Research (2012), стр. 209

3 Gabriel Weimann: Cyberterrorism: The Sum of All Fears?: Studies in Conflict & Terrorism, стр. 130

ущербу государственной безопасности или другим серьезным последствиям».[4]

ЕС определяет важнейшие объекты инфраструктуры как «активы, системы или их части, находящиеся в государствах — членах (и имеющие фундаментальное значение для поддержания жизненно важных социальных функций, здоровья, безопасности, защиты, экономического или социального благополучия), сбои в работе или разрушение которых оказали бы существенное воздействие на государства — члены (в результате невозможности поддержания этих функций)».[5]

Министерство национальной безопасности США определяет важнейшие объекты инфраструктуры как «системы и активы — физические и виртуальные, — значение которых столь велико, что ограничение их дееспособности или их разрушение может привести к ослаблению безопасности, экономики, социального благополучия или социальной безопасности, нанесению ущерба окружающей среде или какому-либо сочетанию этих неблагоприятных явлений в любой федеральной юрисдикции, юрисдикции штата, региональной, территориальной или местной юрисдикции».[6]

Все эти определения весьма схожи по своей сути — они отсылают к значительному воздействию на общественную и государственную безопасность, экономическое процветание и социальное благополучие. Особое значение имеют такие дополнительные свойства важнейших объектов инфраструктуры как межотраслевая взаимозависимость и далеко идущие последствия изменений в их работе. Перебои в работе одного важнейшего сектора инфраструктуры могут оказать воздействие на другие секторы. Особенно четко это видно при рассмотрении энергетического сектора, поскольку энергия необходима для нормального функционирования всех прочих отраслей. Кроме того, сбой, возникший в одной географической области, может иметь региональные или даже международные последствия. Так, авария в системе электроснабжения, произошедшая в 2003 году в Нью-Йорке, затронула более 55 миллионов человек в США и Канаде и повлекла за собой последствия для других отраслей, включая транспортный сектор и сектор здравоохранения, что привело к нескольким смертельным случаям. Энергия необходима для работы всех секторов, поэтому аварии в системе электроснабжения почти неизбежно сказываются на функционировании различных объектов. В качестве примера можно рассмотреть бензозаправочные станции, которые обычно не оснащаются аварийными источниками электропитания высокой емкости, а значит, отключение электропитания может привести к ограничению или даже к остановке их работы. Далее, бензозаправочные станции могут оказаться не в состоянии обеспечивать топливом транспортные средства и аварийные генераторы, необходимые для работы других важнейших объектов инфраструктуры, тем самым затрагивая работу энергетического и транспортного сектора. Без резервного, постоянного и/или альтернативного энергоснабжения больницы, банки и государственные учреждения могут оказаться не в состоянии продолжить свою работу, а значит, будут затронуты сектор здравоохранения, финансовый и страховой сектор, сектор государственного управления и администрирования.

Каскадный эффект

Термин используется в качестве метафоры процессов, постепенно переходящих из одной стадии в другую, как водопад [итал.: cascata].

4 Nationale Strategie zum Schutz Kritischer Infrastrukturen, стр. 4, Федеральное министерство внутренних дел Германии, URL: http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf (11/13/2012, перевод автора)

5 Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection (2008/114/EC)

6 National Infrastructure Protection Plan (NIPP), стр. 109: Министерство национальной безопасности США, URL: https://www.dhs.gov/national-infrastructure-protection-plan (11/13/2012)

К важнейшим объектам инфраструктуры принято относить следующие секторы и отрасли:[7]

Секторы	Отрасли
Энергетика	• Электричество • Природный газ • Нефть
Информационные и коммуникационные технологии (ИКТ)	• Телекоммуникации (включая спутники) • Телерадиовещательная сеть • Программное обеспечение, аппаратное обеспечение и сети (включая Интернет)
Транспорт и транспортные перевозки	• Судоходство • Авиация • Железнодорожный транспорт • Автодорожный транспорт • Логистика
Здравоохранение	• Здравоохранение • Лекарства и вакцины • Лаборатории
Водоснабжение	• Дамбы • Склады • Очистные и распределительные сети
Финансы и страхование	• Банки • Фондовые биржи • Страховые компании • Финансовые услуги
Государственное управление и администрация	• Правительство • Парламент • Правовые институты • Аварийно-спасательные службы
Пищевая промышленность и сельское хозяйство	• Торговля продуктами питания • Сельское хозяйство
Средства массовой информации и культурные активы	• Радио • Пресса • Символические здания

Таблица 1: Важнейшие секторы инфраструктуры[7]

7 National Infrastructure Protection Plan (NIPP), стр. 109: Министерство национальной безопасности США, URL: https://www.dhs.gov/national-infrastructure-protection-plan (11/13/2012)

Для поддержания работы важнейших объектов инфраструктуры исключительно важно сохранять стабильность в энергетическом секторе и других важнейших инфраструктурных отраслях (например, необходимо постоянно поддерживать стабильную работу электросетей, поскольку в случае сбоев последствия могут проявиться в считанные секунды). Сбои в системе электроснабжения часто имеют серьезные последствия из-за каскадного эффекта — неизбежно затрагивая другие секторы и их инфраструктуру. В этом отношении трансформаторным подстанциям и высоковольтным линиям электропередачи часто придается большее значение, чем электростанциям, поскольку сбои в работе электростанции обычно можно компенсировать[8], в то время как аварию сети или аварию на критических участках сети компенсировать невозможно.

В ЕС, в частности, объекты нефтяной инфраструктуры рассматриваются как менее важные по сравнению с объектами электрической и газовой инфраструктуры. Нефть является ресурсом, имеющим первостепенное значение для функционирования транспортных сетей, однако поскольку рынок глобализован, распределение нефти в рамках ЕС представляет собой относительно гибкий процесс. Кроме того, государства — члены ЕС обладают значительными запасами нефти. Каждое государство — член ЕС по закону должно обладать запасами нефти, достаточными для удовлетворения внутреннего спроса в течение не менее 90 дней.[9] Текущего стратегического нефтяного запаса США, который составляет 694,9[10] миллионов баррелей нефти, хватит на 36 дней.[11]

2.2 Важнейшие объекты неядерной энергетической инфраструктуры

Согласно данным Международного энергетического агентства (МЭА), в мировом производстве энергии в 2010 году использовались следующие энергоносители:[12]

Топливо [13]	В абсолютном выражении в МТНЭ[14]	Доля, %
Уголь	3 475,77	27,3
Сырая нефть	4 159,37	32,7
Нефтепродукты	-51,93	-0,4
Природный газ	2 727,61	21,4
Ядерная энергия	718,96	5,7
Гидроэнергия	295,62	2,3
Биотопливо и отходы	1 278,03	10,0
Прочее	113,71	0,9
Итого	12 717,16	100

Таблица 2: Мировое производство энергии в 2010 г.[15]

94,3 % процента мирового энергопроизводства приходится на неядерные энергоносители. Поэтому объекты неядерной энергетической инфраструктуры представляют собой привлекательную, хотя и не всегда уязвимую, цель для всякого рода диверсий и атак.

Важнейшая неядерная энергетическая инфраструктура включает разведку, добычу, хранение, переработку, подготовку и распределение ископаемого топлива, системы вспомогательной инфраструктуры, такие как электроснабжение, а также добычу и переработку новых источников энергии.

8 Как вариант, это можно сделать на национальном уровне путем импорта электроэнергии.

9 МЭА, URL: http://www.iea.org/publications/freepublications/publication/EPPD_Bochure_English_2012_02.pdf (Статус: 03/20/2013)

10 Cf. Strategic Petroleum Reserve Inventory, URL: http://www.spr.doe.gov/dir/dir.html (12/07/2012)

11 При объеме среднего дневного использования, составляющем 19,15 миллионов баррелей; см. URL: https://www.cia.gov/library/publications/the-world-factbook/fields/2174.html (13/02/2013)

12 Международное энергетическое агентство, Key World Energy Statistics 2012; более новые сравнительные данные на международном уровне отсутствуют

13 Более подробные объяснения можно найти в следующих источниках: Международное энергетическое агентство, Key World Energy Statistics 2012, стр. 17

14 1 миллион тонн нефтяного эквивалента (м.э.) = 11 630 гигаватт-часов (ГВт-ч).

15 Международное энергетическое агентство, Key World Energy Statistics 2012.

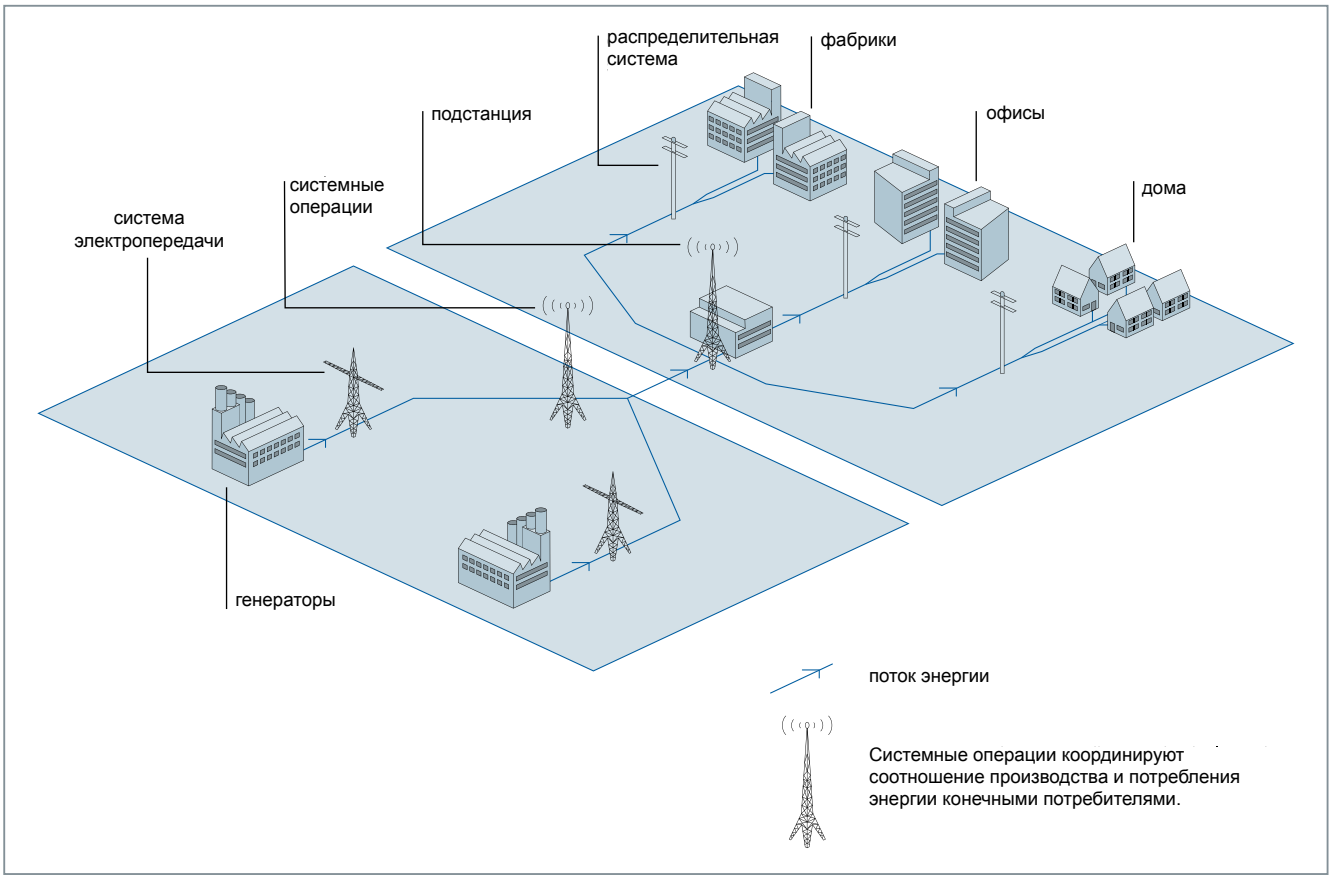


Рис. 1: Функции электроэнергетической промышленности

Полная цепь поставок неядерной энергетической инфраструктуры включает разведку энергонесущего сырья, производство электроэнергии, ее передачу и распределение, хранение и окончательное потребление[16].[17] Кроме того, цепь поставок также включает торговлю различными источниками энергии и самой энергией, а также персонал и организации, осуществляющие управление цепью поставок и коммерческой деятельностью.

➥ Рис. 1: Структура электроэнергетической промышленности[18]

- Энергия производится путем преобразования энергоносителя в электрическую мощность. К энергоносителям относятся продукты, содержащие уголь, [19] а также солнечную, ветровую и гидроэлектрическую энергию.

- Передачу и распределение энергии можно разделить на два этапа. На первом этапе передается энергоноситель (например, по трубопроводу, на судах и автотранспорте); на втором – сама электроэнергия.

- Хранение энергии, по примеру ее передачи и распределения, также можно разделить на два этапа. Первый этап состоит в хранении энергоносителя;[20] второй – в хранении электроэнергии.

- Часть генерируемой энергии используется в цепи поставок неядерной энергетической инфраструктуры (например, для производства электроэнергии). Однако гораздо большая часть используется конечным потребителем (предприятиями, частными домохозяйствами и т.д.).

- Торговля энергоносителями и энергией обычно осуществляется на торговых платформах. Наличие торговых платформ является обязательным условием для осуществления международной торговли энергией. Для создания и обслуживания торговых платформ используются информационные технологии. Торговые платформы играют важную роль в установлении цен на

16 При расчете окончательного потребления электроэнергии не учитывается энергия, необходимая для производства, передачи и распределения энергии. Международное энергетическое агентство, Energy Statistics Manual 2012, стр. 27

17 Примеры юридических определений этих элементов цепи поставок: Директива 2009/72/EC (7/13/2009) и директива 2009/73/EC (7/13/2009), Статья 2 в обоих случаях.

18 Примеры юридических определений этих элементов цепи поставок: Директива 2009/72/EC (7/13/2009) и директива 2009/73/EC (7/13/2009), Статья 2 в обоих случаях.

19 Ископаемое и прочее топливо, такое как сельскохозяйственные, промышленные и бытовые отходы

20 Ископаемое и прочее топливо, такое как сельскохозяйственные, промышленные и бытовые отходы

энергию — на них происходит сопоставление спроса и предложения. Как следствие, цены на энергоносители и энергию колеблются.

- Для обеспечения функционирования всей цепи поставок требуются меры администрирования. Для этого создаются группы управления, службы персонала, осуществляются сервис и техническое обслуживание.

Конечные потребители энергии потребляют уже произведенную энергию. Однако существуют и потребители, использующие энергию для производства другой энергии.[21] Производить и хранить энергию конечные потребители сегодня могут, например, с помощью фотоэлектрических установок и аккумуляторов. Среди новых форм децентрализованного хранения энергии — такие инновационные разработки как аккумуляторы электромобилей. Слияние ролей конечного потребителя и производителя энергии создает новую сложность для энергетических компаний, когда речь заходит о гарантии безопасности и надежности соответствующих элементов инфраструктуры. Глобальный показатель конечного потребления первичной энергии [22] в 2010 году составил 8 676,63 м.э.,[23] что эквивалентно приблизительно 2/3 произведенной энергии.

Для конечных потребителей энергии значение имеют два фактора:

1. Затраты на энергию

2. Наличие энергии[24]

Затраты конечных потребителей на энергию могут варьироваться. Их значение определяется долей затрат на энергию в общих затратах на производство товаров или услуг и зависит от стандартов жизни населения. В энергоемких отраслях энергозатраты являются выше, чем в секторе услуг. В Германии их доля колеблется от 0,2 процента в сегментах услуг производственных отраслей до почти 10 процентов в химической промышленности и в производстве и переработке металлов.[25] При расчете потребления первичной энергии на душу населения показатель потребления составляет от 142 кг ROE в Эритрее до 16 844,1 кг ROE в Исландии.[26]

Ранее мы отмечали, что экономические показатели страны зависят от наличия энергии.[27] Во-первых, наличие энергии имеет прямую связь с экономическим развитием и занятостью населения. Во-вторых, надежность энергопоставок и конкурентоспособность цен на энергию выгодны для экономики страны и обеспечивают ее привлекательность как промышленной зоны для различных отраслей, в особенности для энергоемких. Как следствие, надежность энергопоставок[28] все чаще становится важным критерием при выборе компаниями мест для инвестиций, а высокая инвестиционная привлекательность способствует росту и процветанию страны.

Заинтересованные лица, представляющие государство и отрасль, также обращают внимание на надежность энергопоставок и вклад энергетического сектора в благосостояние и рост экономики страны.

Экономический вклад энергетического сектора[29] колеблется от страны к стране. В Австрии в энергетике занято 28 300 человек, работающих приблизительно в 1570 компаниях, и эта отрасль приносит стране 5,3 миллиарда евро[30].[31] В Германии сектор энергоснабжения в 2010 году принес 408,5 миллиарда евро,[32] обеспечив занятостью 221 264 человек в 1722 компаниях.[33]

Распространенное представление о том, что между уровнем потребления энергии в стране и ее экономическим состоянием существует прямая взаимосвязь, сегодня во многом устарело. Благодаря разработкам в области повышения эффективности энергопользования национальное потребление энергии не всегда повышается при экономическом росте[34].[35] Ослабление взаимосвязи также объясняется структурными изменениями, направленными на снижение энергоемкости производства или увеличение сектора услуг, переносом компонентов производства энергии за границу, [36]а также изменениями в росте численности населения. В отдельных случаях экономические показатели могут расти при сокращении потребления энергии.

21 Например, угольные электростанции, требующие большого количества энергии для производства электричества. Этот тип использования энергии не считается конечным потреблением энергии.

22 Total Primary Energy Supply (TPES), International Energy Agency, Key World Energy Statistics 2012, стр. 63

23 International Energy Agency, Key World Energy Statistics 2012

24 ifo Schnelldienst 07/2011, стр. 10ff

25 Федеральное статистическое управление Германии, Energieverbrauch des Verarbeitenden Gewerbes nach ausgewählten Wirtschaftszweigen 2010.

26 Федеральное статистическое управление Германии, Basisdaten Primärenergieverbrauch 2009/2010.

27 Например, ifo Schnelldienst 07/2011, стр. 10ff

28 Надежность энергопоставок является важным понятием. С национальной и корпоративной точки зрения в это понятие вкладывается потребность в гарантии бесперебойного потока ресурсов для производства необходимой продукции. Энергозатраты также играют важную роль, как можно видеть из идущих в настоящее время в Европе дебатов о субсидиях на возобновляемые источники энергии и на разработку нефтяных месторождений и месторождений сланцевого газа в США. В настоящем руководстве эта важная тема упоминается, но не рассматривается подробно.

29 Включая ядерную энергию. Данные без учета ядерной энергии отсутствуют.

30 Валовая продукция

31 Kuratorium Sicheres Österreich (KSÖ), Cybersicherheit in Österreich, стр. 29, URL: http://www.kuratorium-sicheres-oesterreich.at/uploads/tx_ksothema/Cyberrisikoanalyse.pdf (04/12/2013)

32 Валовая продукция

33 Федеральное статистическое управление Германии, Fachserie 4, Reihe 6.1 Produzierendes Gewerbe, стр. 16ff

34 Валовая продукция часто используется как параметр.

35 ifo Schnelldienst 07/2011, стр. 12

36 Взаимозависимость стран также создает риск при импорте.

При обеспечении надежности энергопоставок особое значение уделяется важнейшим объектам неядерной энергетической инфраструктуры, поскольку именно в энергетическом секторе, а также в секторе телекоммуникаций, сбои могут вызвать каскадный эффект и/или эффект домино. Каскадный эффект наблюдается тогда, когда два сектора зависят друг от друга в такой степени, что сбой в одном из них сказывается на функционировании другого. Эта взаимозависимость может привести и к эффекту домино — когда сбой в одном секторе незамедлительно или с небольшой задержкой приводит к сбою в зависимом от него секторе. Небольшие задержки дают возможность для реализации мер безопасности (например, привлечения групп специалистов по обеспечению непрерывности деятельности или управлению кризисными ситуациями, реализации их планов или активации аварийного электропитания для защиты цепи поставок).[37]

Страны, которым такие эффекты известны, в случае нарушения в одном важном инфраструктурном секторе всегда стремятся расширить программу кризисного и экстренного управления для охвата других (не затронутых нарушением) секторов и учесть эти секторы при планировании антикризисных мер. При подготовке к возможным кризисам необходимо повысить устойчивость[38] отдельных секторов, чтобы они могли максимально долго продолжать свою деятельность даже при возникновении сбоев в других секторах. Таким образом, для компенсации различий в уровне жесткости мер безопасности, принимаемых в отдельных важнейших инфраструктурных секторах, крайне важны межотраслевые меры по предотвращению кризисных ситуаций и антикризисному управлению.

Защита важнейших объектов неядерной энергетической инфраструктуры является не только национальной, но и общемировой задачей. Нарушения в работе важнейших объектов неядерной энергетической инфраструктуры снижают доступность и надежность энергопоставок и могут угрожать стабильности регионов и государств, а также влиять на ценовую конъюнктуру международных энергетических рынков. Террористические акты, стихийные бедствия и технические или организационные угрозы могут нанести вред населению, а также привести к серьезным повреждениям имущества и негативным экономическим последствиям. От таких сбоев может серьезно пострадать доверие общества к поставщику энергии и к способности государственного сектора управлять кризисными ситуациями.[39]

Мы уже упомянули о том, что нарушение в энергетической инфраструктуре одной страны или одного региона может вызвать каскадный эффект, в результате которого возникнут нарушения в инфраструктуре других стран или глобальные сбои. Чтобы предотвратить возникновение каскадного эффекта, превентивные меры и меры антикризисного управления, применяемые для защиты важнейших объектов неядерной энергетической инфраструктуры, необходимо согласовывать на международном уровне. В некоторых странах правительства разрабатывают специальные отраслевые планы. В США специальные отраслевые планы разработаны для каждого сектора, включая энергетический сектор и сектор коммуникаций.[40]

2.3 Террористические угрозы в киберпространстве, направленные на важнейшие объекты энергетической неядерной инфраструктуры

Как показали многочисленные нападения групп боевиков на наземные нефте- и газопроводы в таких странах как Колумбия, Ирак и Нигерия, энергетические сети могут быть уязвимы для предварительно спланированных атак. Трубопроводные сети часто имеют протяженность в тысячи километров, поэтому отслеживание их состояния становится непростой задачей, а значит, и надлежащее обеспечение их безопасности представляет собой сложный, дорогостоящий процесс[41]

В последние годы энергетическая цепь поставок стала более автоматизированной и, как следствие, более зависимой от компьютерных систем контроля. Это обеспечивает более эффективное и надежное функционирование современной энергетической инфраструктуры, но в то же время повышает уязвимость сети, поскольку современные сети становятся все более связанными друг с другом и все чаще управляются удаленно. Несмотря на то что использование открытых стандартов программного обеспечения позволяет снизить затраты на эксплуатацию сетей, оно также делает энергетическую сеть более уязвимой для кибератак, поскольку злоумышленники получают доступ к известному или открытому исходному коду, а значит, могут использовать его в собственных целях.[42]

37 Более подробно об этом см. Главу 4.

38 Устойчивость является термином, который используется для описания способности противостоять неблагоприятному воздействию или изменению условий, поглощать их, восстанавливаться после их воздействия или успешно адаптироваться к ним (Министерство национальной безопасности США, 2009 г., Национальный план защиты инфраструктуры, стр. 111).

39 Почему важна защита важнейших объектов инфраструктуры? Министерство национальной безопасности США, URL: http://www.dhs.gov/critical-infrastructure-sectors (16/11/2012)

40 Специальный отраслевой план по энергетике, Министерство национальной безопасности США, URL: http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf (2010); и Специальный отраслевой план по коммуникациям, Министерство национальной безопасности США, http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf (2010)

41 В Главе 7 представлены дополнительные документы, в которых разъясняется, как этот вопрос решается в других важнейших инфраструктурных секторах (транспортном секторе, секторе водоснабжения, сектор ИКТ и др.), перед которыми стоят аналогичные задачи.

42 Critical Energy Infrastructure Protection: The Case of the Trans-ASEAN Energy Network, URL: http://www.ensec.org/index.php?option=com_content&view=article&id=205:critical-energy-infrastructure-protection-the-case-of-the-trans-asean-energy-network&catid=98:issuecontent0809&Itemid=349 (11/20/2012)

Угрозы важнейшим объектам неядерной энергетической инфраструктуры, можно классифицировать различным образом в зависимости от цели угроз, участия людей и иных критериев.[43]

Открытые стандарты программного обеспечения
Открытые стандарты программного обеспечения доступны всем участникам рынка и просты в использовании. Кроме того, в случае необходимости любой из участников рынка всегда может самостоятельно выполнить разработку на основе этих стандартов. На правовом уровне зачастую наблюдается стремление к формулированию требований по открытости нового программного обеспечения. Как показывает пример SSL (протокол шифровки информации в Интернете) или TCP/IP (сетевые протоколы), Интернет-стандарты обычно соответствуют всем требованиям к открытости. Открытые стандарты дешевле в использовании, поскольку за них не взимается лицензионный сбор. Для усовершенствования программ и исправления программных ошибок не требуется участие разработчика.

Террористические акты в киберпространстве, которые являются основной темой настоящего руководства, — это намеренные угрозы, исходящие от людей. Существует множество других угроз, опасностей и сложностей, способных привести к критическим ситуациям и хаосу, которыми могут воспользоваться террористы, однако эти угрозы не являются темой настоящего документа. Среди угроз для важнейших объектов неядерной энергетической инфраструктуры — угрозы, возникающие в связи с геологическими условиями или окружающей средой (например, экстремальные погодные условия или стихийные бедствия); угрозы для здоровья людей (например, пандемии); геостратегические угрозы (например, политическая нестабильность или пиратство); сложности, связанные с регулированием (например, нормативные положения и платформы ценообразования); и организационные сложности (например, использование субподряда/зависимость от других организаций и «скрытая зависимость»[44]в рамках цепи поставок).

Технические сбои, как непреднамеренные (например, ставшие следствием человеческого фактора),[45] так и преднамеренные, представляют собой другой вид угроз и могут иметь серьезные последствия. Кроме того, неустранимые уязвимости вместе с возрастающей сложностью технических компонентов и систем — это факторы, всегда означающие возможность возникновения новых рисков. В качестве примеров может служить сбой всей системы банковских карт Европейской комиссии в Швейцарии, произошедший в 2000 году в результате ошибки в центре обработки данных, или авария в системе электроснабжения США и Канады, случившаяся в 2003 году.

Технические сбои могут иметь множество причин. При этом зачастую поиск причины требует слишком высоких затрат, не может быть проведен в разумные сроки или невозможен в связи с правовыми барьерами. В результате многие меры направляются на предотвращение или сведение этих угроз к минимуму, а не на устранение непосредственных и долгосрочных последствий угрозы. Технические угрозы могут быть осложнены организационными особенностями или сложностью бизнес-процессов — факторами, которые затрудняют обнаружение человеческой ошибки/действия или технического сбоя.

Даже если технический сбой является непреднамеренным или случайным, технические уязвимости могут эксплуатироваться террористами при кибератаке или физическом нападении. Однако эти виды нападений существенно отличаются по планированию и организационной сложности от других видов атак.

Способы нивелирования этих угроз могут включать:[46]

a. Развертывание разных систем и разделение систем в целях предотвращения ситуации, когда сбои в работе одной системы наносят ущерб всей макросистеме; недопущение зависимости от одного источника.

b. Включение в контракты положений об ответственности за ущерб в результате технических неполадок, позволяющих в случае сбоев получить компенсацию от поставщика[47].

c. Постоянный обмен [48] информацией об обнаруженных ошибках и уязвимых местах с поставщиками и другими компаниями для максимально быстрого устранения или исправления этих проблем.

Терроризм и прочие угрозы, исходящие от людей, могут привести к значительным финансовым, материальным и человеческим потерям. Подобные угрозы могут исходить от внутренних или внешних нарушителей. Внутренние нарушители, как правило, лучше информированы, чем внеш-

43 В дополнение к этой классификации существуют и другие, например, разделение BSI на природные и антропологические угрозы. Cf. URL: http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/threats/threats_node.html (02/13/2013)

44 Скрытая зависимость может возникнуть, когда несколько поставщиков используют один источник снабжения. В этом случае у компании фактически существует только один поставщик. В случае сбоя в его работе компания оказывается зависимой от объемов запасов поставщика.

45 Хотя термин «ошибка» подразумевает непреднамеренные действия, он рассматривается здесь в рамках преднамеренных угроз, поскольку во многих странах халатность считается преступлением.

46 Индивидуальные меры более подробно описаны в Главах 4 и 5.

47 В этом контексте при выборе поставщика необходимо убедиться, что он в состоянии выплатить компенсацию. Иными словами, многие мелкие и незначительные с финансовой точки зрения компании не следует даже рассматривать в качестве потенциальных поставщиков.

48 Например, ассоциации, специализированные СМИ или национальные учреждения, такие как группы по реагированию на чрезвычайные и кризисные ситуации

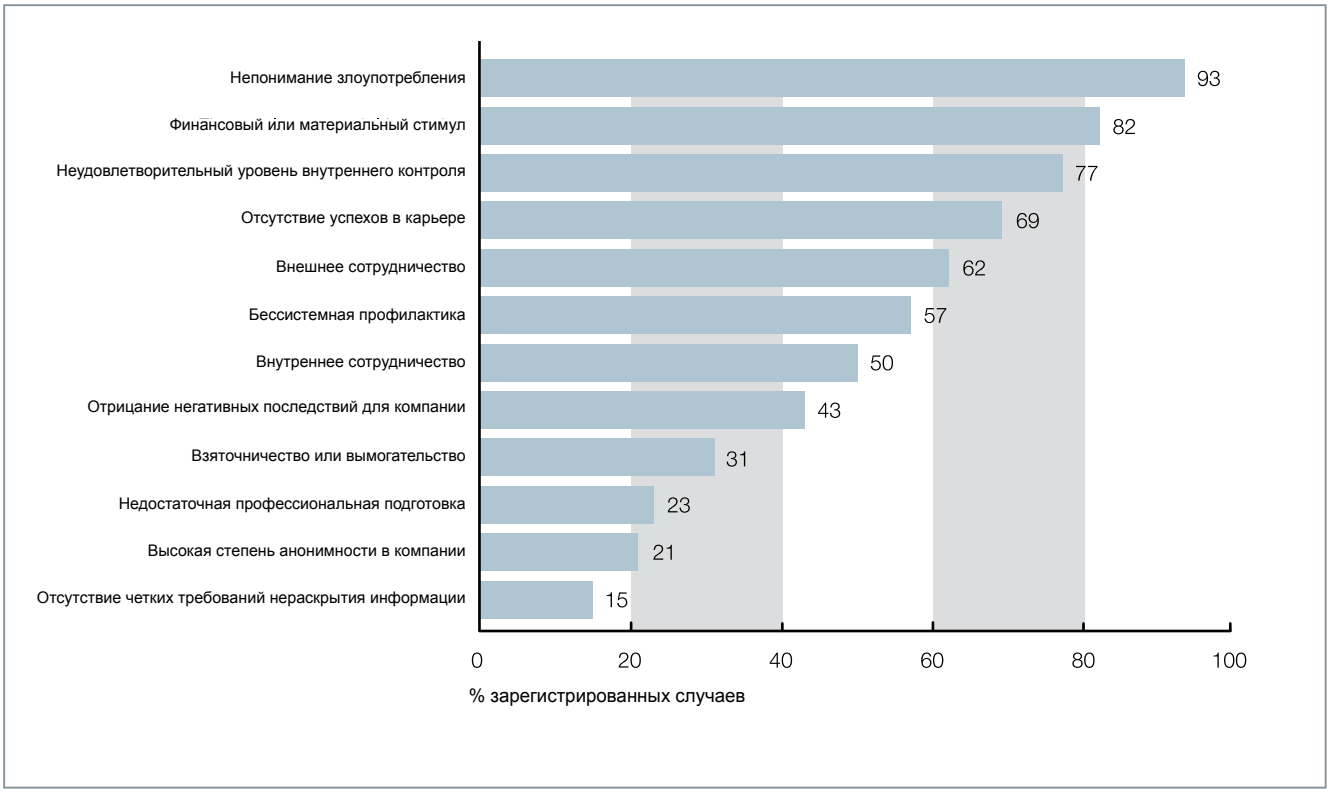


Рис. 2: Мотивы внутренних нарушителей[50]

ние, и статистически представляют собой более серьезную угрозу. Внутренние нарушители являются сообщниками или основными участниками преступного сговора в большинстве происшествий и в случаях с наиболее существенными потерями.[49] Этот факт имеет особое значение, поскольку компаниям доступен самый эффективный и простой способ снижения данной угрозы — начать противодействие ей на раннем этапе. Примеры угроз, исходящих от людей, включают использование продукции в собственных целях и кражу данных, а мотивация таких действий может быть самой разной — от саботажа до терроризма. Выявив мотивы внутренних нарушителей, можно обнаружить способы ограничения ущерба. В следующей диаграмме представлены 12 основных мотивов.

Для снижения воздействия таких факторов как «неудовлетворительный уровень внутреннего контроля», «бессистемная профилактика», «недостаточная профессиональная подготовка», и «отсутствие четких требований нераскрытия информации» могут быть приняты следующие меры:[51]

a. Профессиональная подготовка, обучение и повышение осведомленности персонала и отдельных контрагентов;

b. Внедрение комплексных концепций обеспечения безопасности (использование шифровальных технологий, засекречивание уникальных процессов, контроль доступа, мониторинг важных областей и т.д.);

c. Публикация руководств по этике и кодексов поведения;

d. Введение принципа служебной необходимости при доступе к специальной информации[52]; и

e. Внедрение системы анонимных сообщений о нарушениях для выявления внутренних нарушителей.

Определенные мотивы для совершения террористических актов могут быть как у внутренних, так и у внешних нарушителей. Для выявления и устранения потенциальных проблем необходимо выполнять проверки биографических данных сотрудников и четко регламентировать рабочий процесс.

Несмотря на некоторые разногласия по вопросам разграничения и определения различных видов киберпреступлений и кибертерроризма, существует единое мнение о том, что эти угрозы относятся к категории намеренных, поскольку они предполагают эксплуатацию различных уязвимых мест отдельными людьми

49 SiFo-Studie 2009/2010, стр. 64ff

50 SiFo-Studie 2009/2010, стр. 61

51 Индивидуальные меры более подробно описаны в Главах 4 и 5. Все выдержки, представленные здесь, взяты из SiFo-Studie 2009/2010, стр. 76ff и Best Practice, журнала для клиентов компании T-System, выпуск 04/2011.

52 Конфиденциальная информация предоставляется только тому персоналу, которому она необходима для работы.

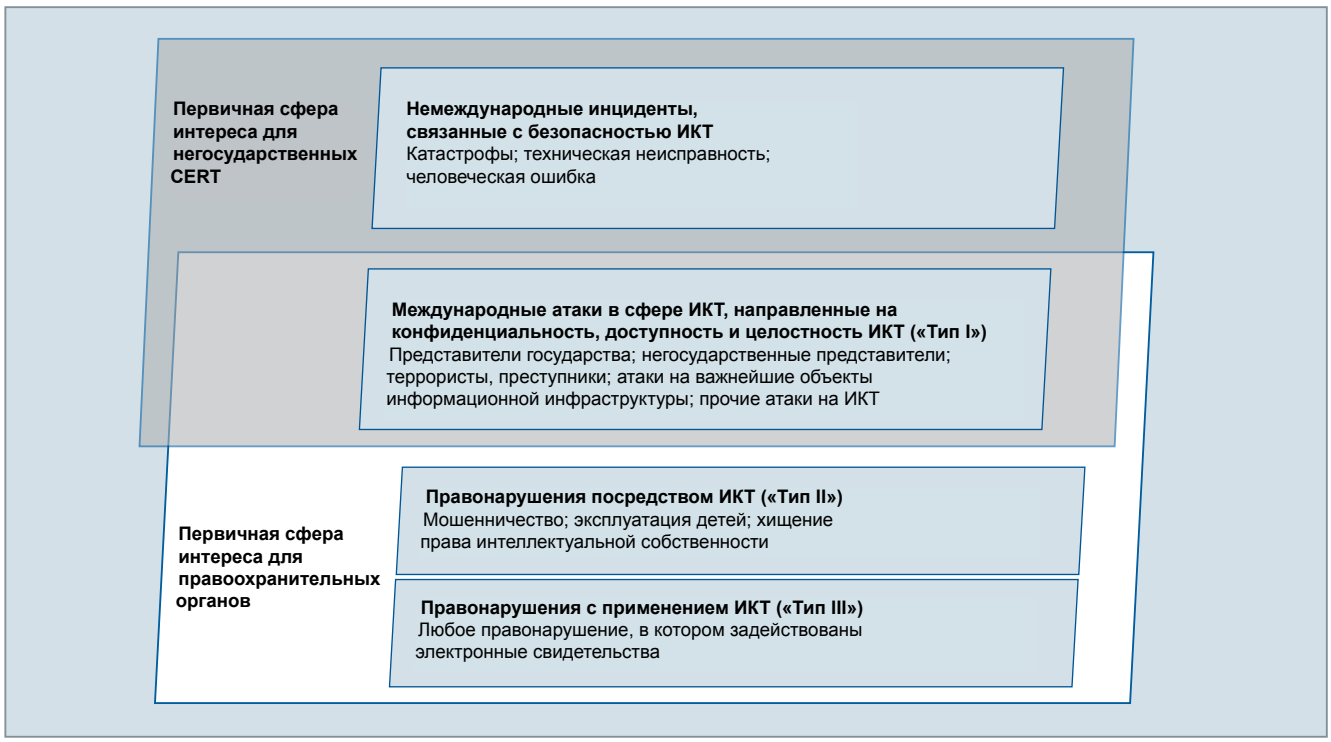


Рис. 3: Характеристика киберпреступности и нарушений кибербезопасности

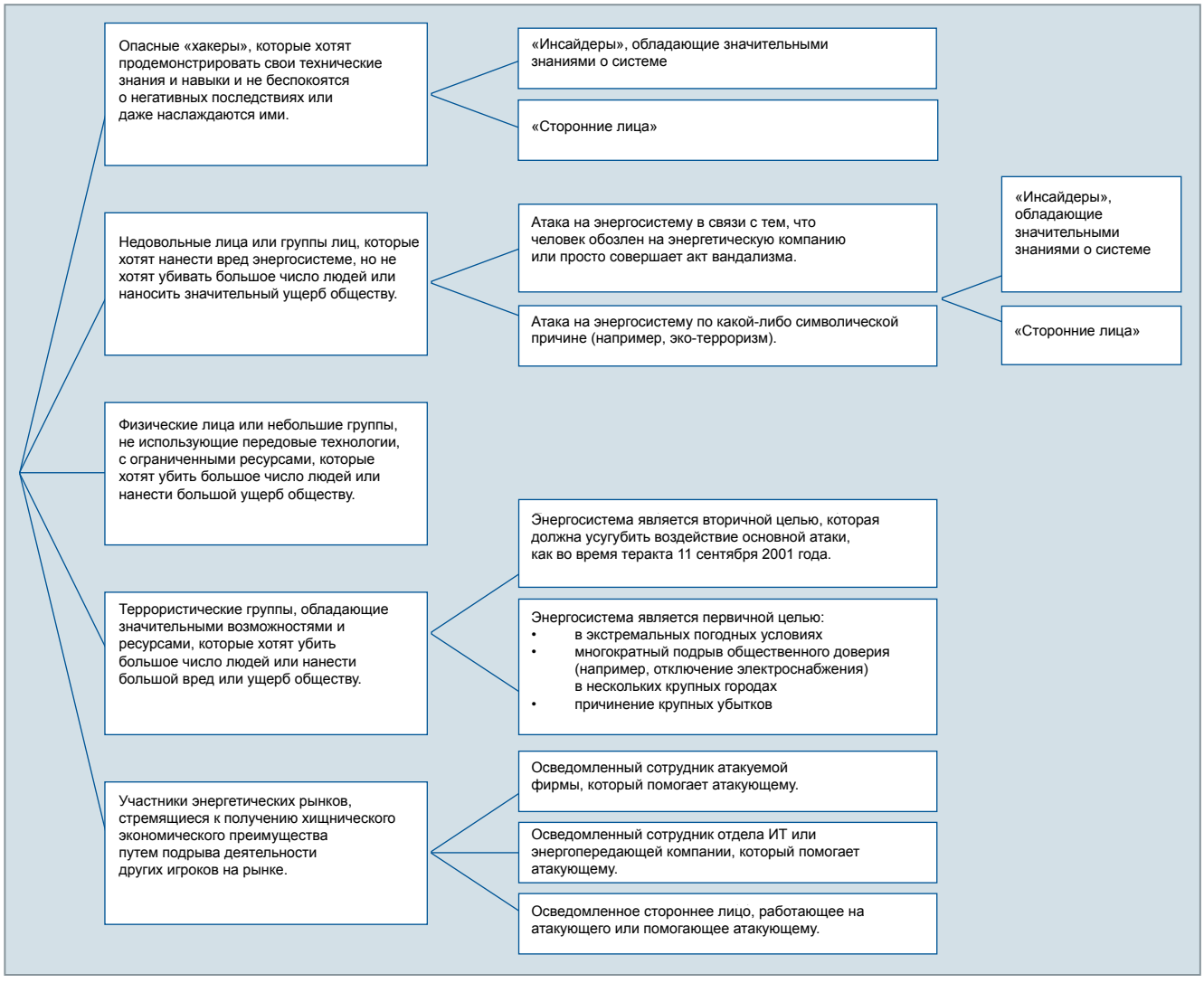


Рис. 4: Простая классификация потенциальных нарушителей, которые могут атаковать энергетическую систему

или группами в целях нанесения ущерба. По мере развития технологий потенциальный спектр возможных векторов уголовных и террористических кибератак становится все шире.

На основании Статей 2–9 Конвенции Совета Европы по киберпреступлениям 2001 года[53] (также известной под названием «Будапештская Конвенция») была разработана весьма простая для понимания типология, охватывающая различные аспекты безопасности систем ИКТ. Классификация проста: в ней формулируется различие между формами технологических нарушений и преступлениями в сфере ИКТ. Руководство по передовой практике получения доказательств с помощью компьютерных технологий Ассоциации руководителей полицейских служб Великобритании (2009 г.) придерживается аналогичного подхода: «компьютеры могут использоваться при совершении преступления [Тип II]; они могут содержать доказательства преступления [Тип III] и могут быть целями преступления [Тип I]».[54] На Рис. 3 ниже представлены различия и сходства между полномочиями Группы быстрого реагирования на нарушения компьютерной безопасности и правоохранительных органов в контексте данной классификации и возможных нарушений.

➥ Рис. 3: Характеристика киберпреступности и нарушений безопасности в киберпространстве[55]

Оператору важнейших объектов неядерной энергетической инфраструктуры трудно определить намерения атакующих, поэтому при изучении киберпреступления или террористического акта в киберпространстве важно проанализировать, каких последствий желал добиться злоумышленник, атакуя цель. Этот анализ не важен на первом этапе реагирования, когда основное внимание направлено на максимально быстрое восстановление работы систем. На нем имеет смысл сосредоточиться только при последующем анализе действий злоумышленника.[56]

➥ Рис. 4: Простая классификация потенциальных нападающих на энергетические сети[57]

Террористы могут использовать для совершения киберпреступления любой подход, поэтому крайне важно, чтобы операторы важнейших объектов неядерной энергетической инфраструктуры были осведомлены о векторах атаки и о вероятных сценариях киберпреступления.

2.4 Потенциальные террористические акты, основанные на использовании информационных технологий и направленные против важнейших объектов неядерной энергетической инфраструктуры

Представленная ниже диаграмма иллюстрирует нападения на важнейшие объекты неядерной энергетической инфраструктуры, которые не могут быть классифицированы как терроризм, но могут быть использованы террористическими группами в своих целях. Соответствующие защитные меры, направленные на избежание или сокращение ущерба, будут представлены ниже в настоящем руководстве.

В диаграмме приведен пример кибератаки на электрическую сеть и представлены возможные последствия этой атаки.

➥ Рис. 5: Влияние кибератаки на электрическую сеть[58]

В 2007 году ученые Национальной лаборатории Айдахо представили наглядную демонстрацию последствий атаки на электростанцию. Министерство национальной безопасности США заказало у лаборатории демонстрацию получения доступа к системе управления электростанции и управления ею извне для вызова физического сбоя путем введения ложных данных. Во время демонстрации, названной «Тест генератора Аврора», в работе генератора сначала произошла заминка, затем из него пошел белый пар, и после этого он перестал работать. Демонстрация показала не только то, что хакеры способны преодолеть системы защиты и получить контроль над генератором, но и то, что генератор может быть физически разрушен. Уничтожение генератора или турбины может привести к длительному простою, поскольку для замены этих компонентов необходимо заново изготовить и установить детали. Репортаж об этом эксперименте можно было наблюдать на канале CNN.[59]

Другой эксперимент, в ходе которого была смоделирована кибератака на электрическую сеть США, был проведен в 2010 году. Хакеры получили доступ к электронному оборудованию нескольких подстанций и нацелились на системы, поддерживающие стабильность напряжения в линиях электропередач. Эти системы оказались слабым звеном. В случае настоящей

53 Council of Europe: Convention on Cybercrime (2001), URL: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (10/15/2012)

54 ENISA: Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime(2012), стр. 12

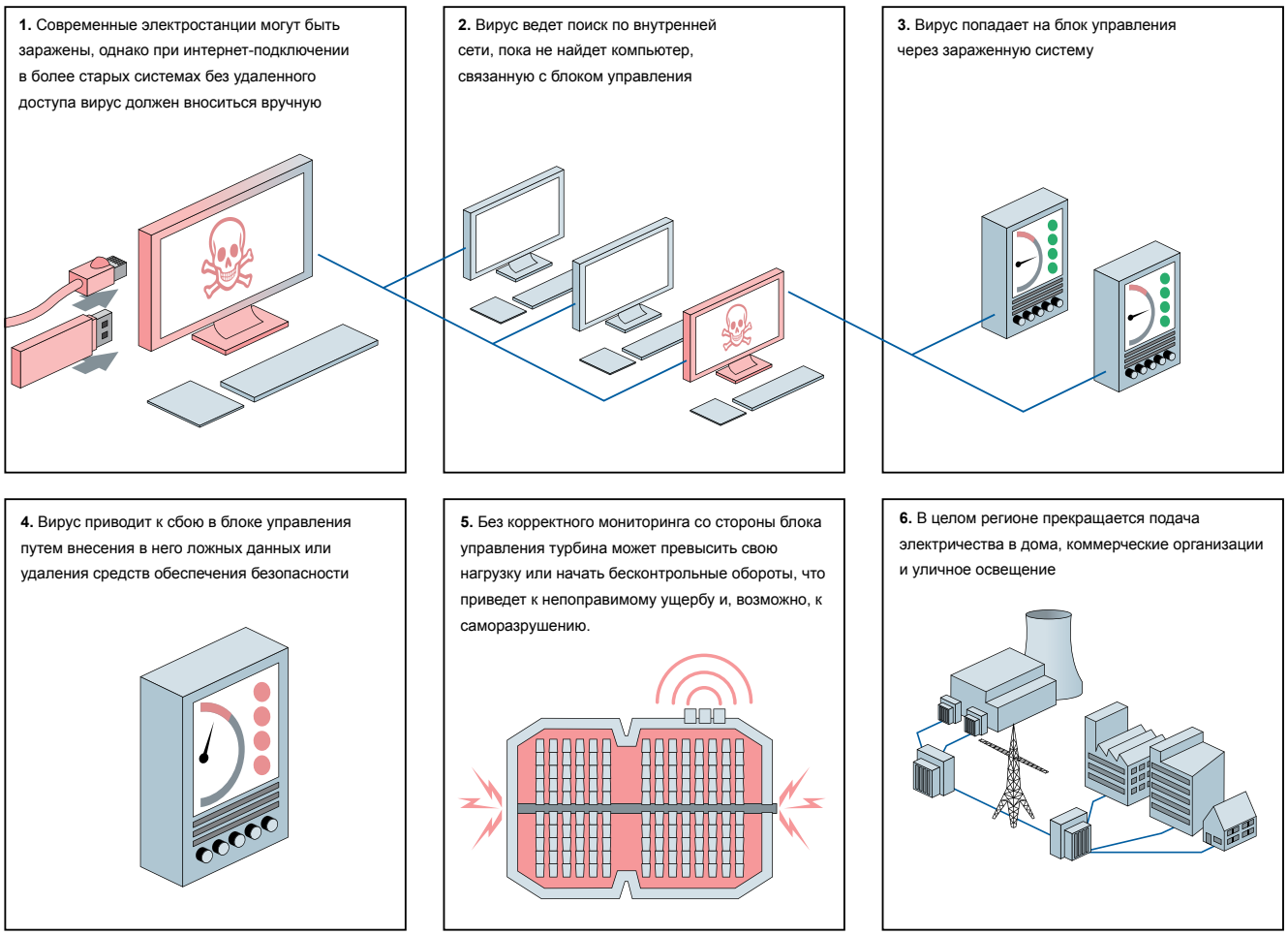
55 Европейское агентство по сетевой и информационной безопасности (ENISA): Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime (2012), стр. 13

56 Эту задачу может упростить письменное заявление о принятии ответственности, (при наличии такового). Однако таким заявлениям не всегда можно доверять, поскольку киберпреступники также могут фальсифицировать их для выполнения своих целей.

57 NAP: Terrorism and the Electric Power Delivery System (2009), стр. 15.

58 Financial Times, URL: http://www.ft.com/cms/s/0/00148d60-c795-11e0-a03f-00144feabdc0.html#axzz2EBla2YKG (12/05/2012)

59 Staged cyber attack reveals vulnerability in power grid: CNN U.S., URL: http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US (11/21/2012)



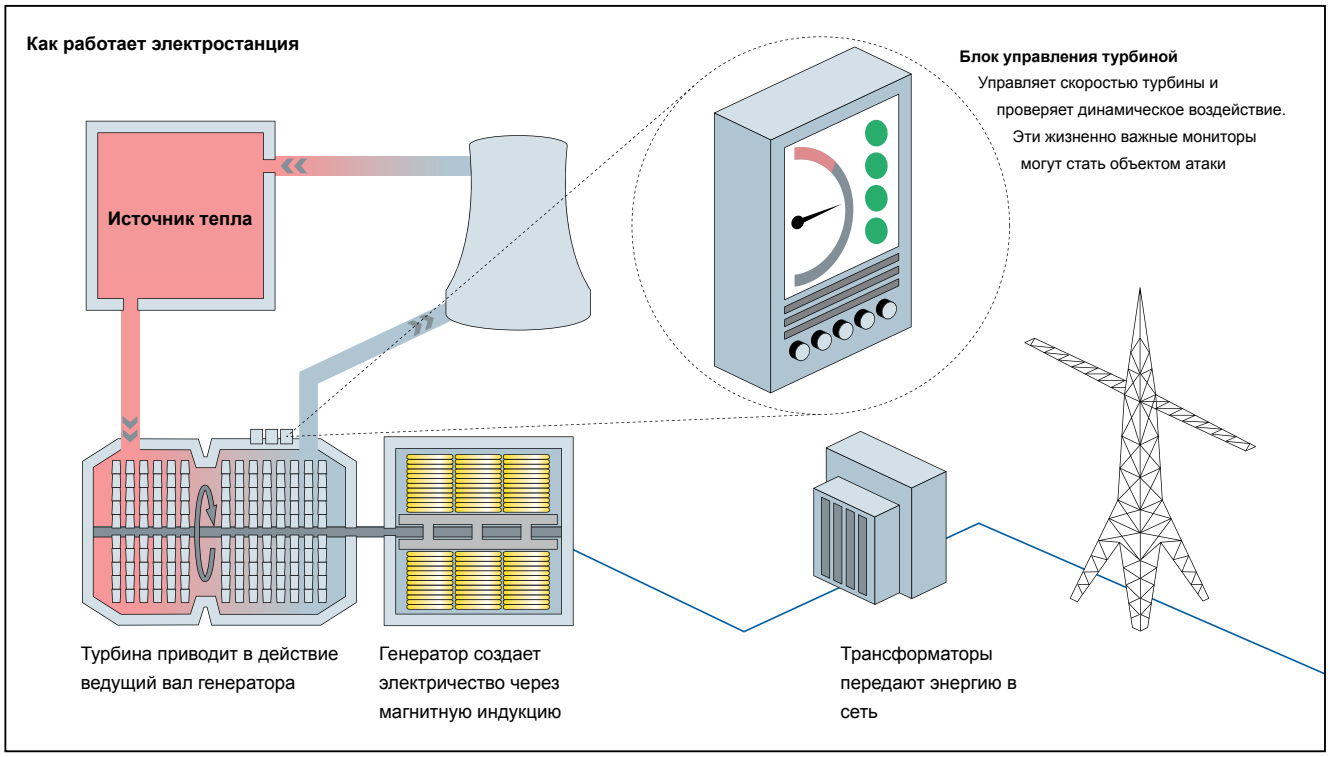


Рис. 5: Как кибератака может повлиять на сеть

атаки шесть таких устройств были бы разрушены, и целый штат остался бы без электричества на несколько недель.[60]

В результате другого происшествия в феврале 2011 года выяснилось, что китайские хакеры атаковали информационные системы нефтяных и газовых компаний, похитив конфиденциальные данные.[61] Эти атаки были направлены на компьютеры нефтяных и газовых компаний в США, на Тайване, в Греции и в Казахстане. Нападавшие использовали известные уязвимости операционных систем. Приведенные выше инциденты не были террористическими атаками, но террористы могут с легкостью применять эти методы для достижения своих целей.

Эксперты обнаружили другие атаки на центры обработки данных установок нефтяных и газовых компаний на Ближнем Востоке в октябре 2012 года. В августе 2012 года более 30 000 компьютеров, принадлежащих саудовской нефтяной компании Saudi Aramco, были парализованы и выведены из строя вредоносной программой (известной как "Shamoon"). Тот же вирус был использован против информационных систем катарской компании RasGas.[62]

В ноябре 2012 года была осуществлена атака на интернет-инфраструктуру компании 50Hertz, оператора сети передачи электроэнергии на севере и востоке Германии. Неустановленные взломщики провели DDoS-атаку на веб-сайты компании и ее систему электронной почты с помощью бот-сети.[63] В этом случае система подачи электроэнергии не была затронута напрямую, однако она легко могла стать целью нападения.

2.5 Резюме и рекомендации

От функционирования инфраструктуры в целом и важнейших инфраструктурных объектов в частности зависит нормальная жизнь стран и обществ, четкое функционирование отдельных отраслей и всей экономики. Кибератаки становятся главным вызовом для операторов важнейших объектов инфраструктуры и все чаще – для операторов важнейших объектов неядерной энергетической инфраструктуры. В то же время спрос на энергию постоянно растет. Как заявило правительство Германии, «необходимо найти новые решения, способствующие переходу к либерализованным рынкам, децентрализованным и гибким структурам энергоснабжения и к электромобильности, при этом обеспечивая максимальный уровень экономичности, надежности энергопоставок и экологичности».[64] В данном контексте безопасность важнейших объектов инфраструктуры является ключевым вопросом диалогов и политических мер, посвященных национальной, международной и корпоративной безопасности.

Угрозы, актуальные для операторов важнейших объектов инфраструктуры, можно классифицировать различными способами, но угроза терроризма очевидно является намеренной угрозой. Повышение взаимозависимости и интеграции компьютерных систем управления упрощает эксплуатацию инфраструктуры[65], но приводит к росту риска зловредного использования и целевых атак – кибератак в том числе. Угрозы, связанные с кибербезопасностью, особенно опасны для операторов важнейших объектов неядерной энергетической инфраструктуры, поскольку хорошо скоординированная кибератака, особенно при наличии каскадного эффекта, может нанести гораздо больший ущерб, чем физическая атака. Как следствие, важнейшие объекты энергетической инфраструктуры становятся привлекательной мишенью для террористов, стремящихся нанести как можно больший ущерб и вызвать максимальный общественный резонанс, в отличие от тех преступников, которые преследуют исключительно экономическую выгоду. Тесные связи в системах и каскадный эффект — это два слагаемых, за счет которых кибератаки на важнейшие объекты неядерной энергетической инфраструктуры потенциально способны привести к долговременным нарушениям работы систем энергоснабжения.

Поскольку в последнее время кибератаки на важнейшие объекты энергетической инфраструктуры становятся все более успешными, повышению защищенности таких объектов придается первостепенное значение. Угроза, исходящая изнутри, всегда является наиболее потенциально разрушительной. Вероятно, некоторые недавние атаки были осуществлены не без участия сотрудников. Быстро развивающиеся технологии и их растущая сложность, потенциальное использование прокси-серверов и арендуемых бот-сетей, а также рост взаимозависимости физической и виртуальной систем безопасности — все это повышает сложность угрозы и сложность защиты от нее.

60 Attack on the power grid in Spectrum der Wissenschaft, URL: http://www.spektrum.de/alias/energie-versorgung/angriff-auf-das-stromnetz/1123846 (11/21/2012)

61 Cf. McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), URL: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf (12/02/2013)

62 RasGas, new cyber attack against an energy company, URL: http://securityaffairs.co/wordpress/8332/malware/rasgas-new-cyber-attack-against-an-energy-company.html (01/29/2013)

63 European renewable power grid rocked by cyber-attack: EurActiv, URL: http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541 (12/10/2012)

64 Федеральное министерство экономики и технологии Германии (BMWi), URL: http://www.e-energy.de/958.php (12/04/2012)

65 Без компьютеризированных систем управления мониторингом инфраструктуры, ее систем и процессов занимается большое число сотрудников.

Государства могут помочь при защите инфраструктуры, но во многих странах основная часть ее важнейших объектов принадлежит частным компаниям. Именно поэтому сотрудничество между государством и частным бизнесом имеет неоценимое значение. Компании, владеющие важнейшими объектами неядерной энергетической инфраструктуры, могут применять различные защитные меры — от внутренних мер (обучения, повышения осведомленности и принятия концепций комплексной защиты), направленных на противодействие внутренним нарушителям, до мер при поддержке государства, таких как реализация концепции защиты, обеспечивающей одновременный контроль за всеми важнейшими объектами инфраструктуры и снижающей взаимозависимость и каскадный эффект. Компаниям, владеющим важнейшими объектами неядерной энергетической инфраструктуры, также следует сосредоточиться на определении степени зависимости их объектов от других объектов инфраструктуры — управляя этой степенью и, возможно, уменьшив ее, компании смогут обеспечить свою безопасность при сбоях в работе, возникающих у деловых партнеров, или при обнаружении вредоносного программного обеспечения или других неполадок в установленной системе. Эти меры имеют особую важность при обеспечении безопасности Систем дистанционного управления и сбора данных (SCADA).

3. Передовая практика в рамках управления рисками ИКТ для снижения рисков терроризма в киберпространстве

ОБСЕ Организация по безопасности и сотрудничеству в Европе

3. Передовая практика управления рисками ИКТ в целях снижения рисков терроризма в киберпространстве

В данной главе рассматривается создание организационной системы управления рисками ИКТ в энергетическом секторе. В первую очередь мы рассмотрим общую роль ИКТ и их важность для решения различных подзадач в энергетическом секторе, а также определим основные компоненты, зависимые от ИКТ. Исходя из этого, мы в общих чертах обрисуем проект системы управления рисками ИКТ, разработанный с учетом соответствующих международных стандартов и определенных подходов к управлению рисками, связанными с энергетической инфраструктурой. Завершается эта глава резюме и рекомендациями по снижению рисков, связанных с киберугрозами в неядерном энергетическом секторе.

3.1 Роль и значение ИКТ в энергетическом секторе

Зависимости существуют во многих областях работы важнейших объектов неядерной энергетической инфраструктуры. В частности, можно выделить зависимость между поставщиками нефти и производителями первичной энергии. Для добычи или доставки сырья поставщику требуется энергия, а производителю энергии нужны поставщики. Конфликт интересов может произойти, если, например, поставщик запросит высокую цену за поставляемую нефть, одновременно претендуя на закупку электроэнергии по низкой цене. Если поставщик потребует от производителя первичной энергии выполнения обоих требований, то, возможно, производитель не сможет сохранить рентабельность. Следовательно, ключевую роль в общем успехе играет способность обеих сторон к сотрудничеству. Это также относится к применению мер для защиты от кибератак и реагирования на возникающие атаки. Компаниям, владеющим важнейшими объектами неядерной энергетической инфраструктуры, необходимо интегрировать всю цепь поставок важнейшей неядерной энергетической инфраструктуры в свою систему управления рисками ИКТ.

Поскольку электроэнергия генерируется и потребляется одновременно, для эксплуатации электроэнергетической системы требуются системные операторы, способные постоянно обеспечивать баланс между производством электроэнергии и спросом на нее.[66] Такие системные операторы контролируют электрические цепи и управляют производством, передачей и распределением электроэнергии с помощью информационных сетевых систем управления и контроля, используемых для мониторинга важнейших процессов и функций. Эффективное функционирование электроэнергетической промышленности во многом зависит от работы этих систем.

По мере развития электроэнергетической промышленности и появления новых технологий некоторые поставщики энергии обновляют свои электросети.[67] Они используют современные технологии и дополнительные информационные системы и сети, в особенности в системах передачи и распределения. Такое развитие позволило отрасли и государству разработать концепцию более надежной и эффективной электросети, позволяющей интегрировать альтернативные формы производства энергии. Использование интеллектуальных сетей требует более широкого использования информационных систем, сетей и взаимозаменяемых средств коммуникаций для автоматизации процессов и действий, который сейчас выполняются системными операторами вручную.

↪ Рис. 6: Основные компоненты интеллектуальной сети[68]

66 Главное бюджетно-контрольное управление США (US GAO), 2011 г., Electricity Grid Modernization, p. 3 f

67 US GAO 2011, стр. 4

68 US GAO 2011, стр. 6

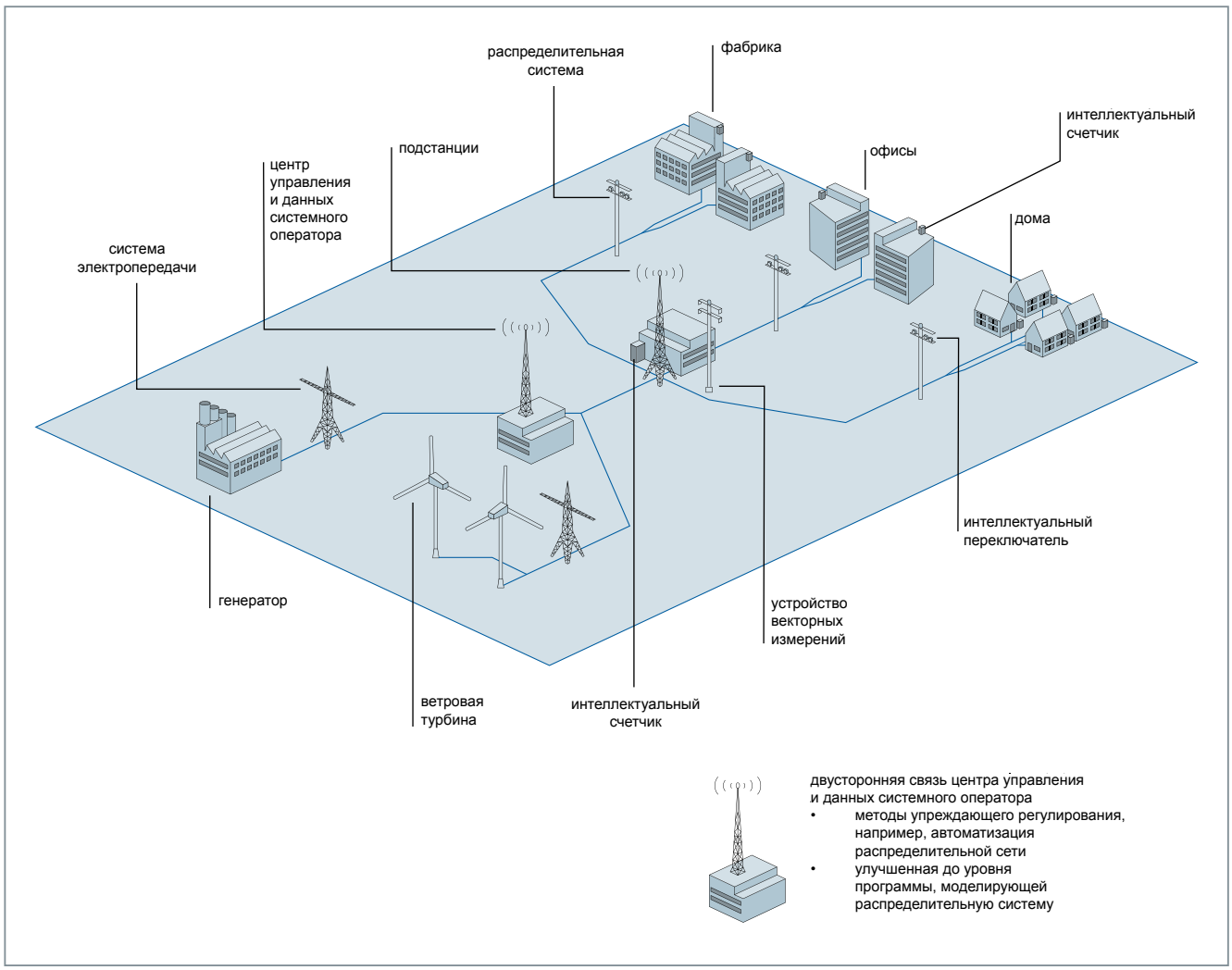


Рис. 6: Основные компоненты интеллектуальной сети

В будущем использование интеллектуальных сетей может выйти за пределы подзадач передачи и распределения; такие сети могут способствовать росту эксплуатации информационно-коммуникационных технологий в сфере хранения и торговли.[69]

Практически все участники рынка сходятся во мнении, что интеллектуальные сети необходимы, однако государственные органы и отрасль придерживаются абсолютно разных подходов к их созданию. Отчасти это объясняется различиями в целях и мотивации, но свою роль также играют технологические и правовые ограничения: то, что технически осуществимо, не всегда разрешено законом.

В целом государства нацелены на обеспечение надежности энергоснабжения и максимизацию вклада важнейших объектов неядерной энергетической инфраструктуры в национальную экономику. Цели компаний, владеющих важнейшими объектами неядерной энергетической инфраструктуры, как правило, полностью лежат в экономической плоскости и заключаются в получении максимальной прибыли. Третья сторона — конечные потребители электроэнергии — задействована здесь лишь косвенно. Потребители в целом заинтересованы в более низкой стоимости электроэнергии и надежности энергоснабжения. Эти разные цели могут как дополнять друг друга, так и противоречить друг другу. В настоящее время перед государством и операторами важнейших объектов неядерной энергетической инфраструктуры стоит задача найти эффективные и действенные пути взаимодействия. Возможно, имело бы смысл собрать заинтересованные стороны для дискуссии за круглым столом, сформировав рабочие группы на национальном уровне.[70] В рамках подобной группы стороны смогли бы встретиться и под руководством государства определить предпочтительный подход путем голосования.

69 US GAO 2011, стр. 6

70 В ФРГ была создана подобная рабочая группа, призванная оптимизировать переход от ядерной энергии к возобновляемым источникам энергии: Plattform Erneuerbare Energien, созданная Федеральным министерством экологии, защиты природы и ядерной безопасности (BMU). Cf. URL: http://www.erneuerbare-energien.de/ (02/13/2013)

ИКТ играют центральную роль в построении интеллектуальных сетей и управлении важнейшими объектами неядерной энергетической инфраструктуры. В следующих разделах рассматриваются и анализируются другие роли ИКТ. Объекты инфраструктуры ИКТ, как и объекты энергетической инфраструктуры, часто классифицируются правительствами и представителями отраслей как важнейшие объекты инфраструктуры.[71] В современной инфраструктуре все чаще используются связанные системы ИКТ. Это делает ее более уязвимой для цепной реакции, при которой первоначальная ошибка или сбой в одной системе может привести к прекращению функционирования многих других систем.

Системы ИКТ используются в энергетическом секторе для следующих целей:

- Для мониторинга и распределения
- Для покупки и продажи энергии и топлива
- Для сообщения об ошибках
- В качестве автоматической защитной системы для выявления сбоев и, в случае необходимости, оперативного отключения системы от сети
- Для передачи данных общего характера, включая данные о фактическом и прогнозируемом спросе, информацию по установке и т.д.

Системы SCADA имеют ключевое значение для надежной эксплуатации всех объектов в энергетическом секторе. Эти системы фиксируют данные с помощью датчиков, представляют информацию и сохраняют ее для обеспечения мониторинга объекта. Они входят в состав автоматизированной системы управления технологическими процессами, которая используется, помимо прочего, для измерения показателей передачи и распределения электроэнергии или давления внутри газопровода. Преимущества систем SCADA включают возможность вести мониторинг нескольких процессов одновременно и осуществлять упреждающее управление.[72] Однако преимущества единой точки управления и масштабных сетей, охватывающих все системы, сопровождаются риском, что такие точки и сети могут стать целью террористических актов, исходящих из киберпространства.

Проведя анализ кибербезопасности, Федеральное управление по информационной безопасности Германии (BSI) подготовило список наиболее серьезных угроз для Промышленных систем управления (ICS), включая системы SCADA. Угрозы классифицируются с учетом таких факторов как группы нарушителей, распространение, простота использования уязвимых мест, а также возможные технические и экономические последствия атаки. Для получения необходимых сведений были также проанализированы базы данных реальных происшествий.

➥ Таблица 3: 10 основных угроз для Промышленных систем управления [73]

3.2 Потенциальные уязвимые стороны ИКТ

Успех кибератак возможен только в том случае, если приведенные выше угрозы способны поразить уязвимые стороны информационных систем и сетей. Большинство уязвимостей возникают в системах на этапе разработки или позднее, во время внедрения. В рамках исследования, выполненного компанией McAfee в 2011 году, был проведен опрос 200 руководителей важнейших предприятий энергетической инфраструктуры из 14 стран по темам, связанным с практикой и политикой в области безопасности. 80 процентов опрошенных сообщили, что в течение последнего года их компании подвергались широкомасштабным DoS-атакам. Годом ранее эта цифра составила чуть менее 50 процентов. Как утверждает McAfee, «85% респондентов заявили, что в их сети проникали посторонние лица».[74] Кроме того, значительно выросло количество случаев кибершантажа. В течение одного года число затронутых компаний выросло на четверть. Случаи шантажа равномерно распределены по важнейшим секторам инфраструктуры.

Многие руководители служб безопасности узнали об угрозах, исходящих от других стран, в 2010 году, когда вредоносное программное обеспечение было обнаружено в информационных системах иранских атомных электростанций. Более половины опрошенных допускают, что атаки на важнейшие объекты инфраструктуры в их странах совершались с участием государственных органов.[75] От этого допущения недалеко до логического заключения о том, что террористы также могут воспользоваться известными уязвимыми сторонами важнейших объектов инфраструктуры для причинения огромного ущерба. Эксперты сходятся во мнении, что атаки на важнейшие объекты инфраструктуры могут быть более эффективны,

71 Европейская комиссия: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), URL: http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_risk_governance_report.pdf (03/13/2013)

72 Информация о неполадках поступает практически в режиме реального времени, что позволяет крайне быстро реагировать на них, не допуская перерастания ошибки в чрезвычайную ситуацию или кризис. Обычно это называют упреждающим управлением.

73 BSI-A-CS 004, (2012)

74 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), p. 6

75 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), p. 9

чем нападения на военные объекты. При этом отмечается, что эти атаки не вызывают такую эмоциональную реакцию, как фотографии последствий взрывов на гражданских объектах. Однако рано или поздно руководство террористическими организациями перейдет в руки нового поколения, которому информационные технологии могут быть ближе, чем действующим лидерам. Это может привести к существенному увеличению количества кибератак со стороны террористов.[76]

Чтобы получить полную картину уязвимых сторон, угроз и следующих из них рисков, управление рисками необходимо осуществлять в соответствии с методикой, предложенной в Главе 3.4. Этап выявления риска, очевидно, необходим для обнаружения уязвимостей и поэтому имеет большое значение при определении векторов будущих атак. Эти уязвимости приведут к ущербу, только если ими воспользуются для реализации соответствующей угрозы,[77] поэтому они не всегда

№	Угроза	Объяснение
1	Несанкционированное использование точек доступа дистанционного технического обслуживания	Точки доступа для технического обслуживания —специально созданные внешние входы в сеть ICS, которые часто бывают недостаточно безопасными.
2	Сетевые атаки через корпоративную сеть	Офисные ИТ обычно подключены к сети несколькими способами. В большинстве случаев также существуют сетевые связи между офисами и сетью ICS, которые нарушители также могут использовать для получения доступа к сети.
3	Атаки на стандартные компоненты, используемые в сети ICS	Стандартные компоненты ИТ (готовые коммерческие продукты (COTS)), такие как системное программное обеспечение, сервер приложений или баз данных, часто содержат недостатки и уязвимости, которыми могут воспользоваться нарушители. Если эти стандартные компоненты также используются в сети ICS, то риск успешной атаки на сеть ICS повышается.
4	(D)DoS-атаки	(Распределенная) атака типа «отказ в обслуживании» может негативно сказаться на работе сетевых соединений и важнейших ресурсов, а также вызвать сбой систем, например, для того, чтобы прервать работу ICS.
5	Человеческая ошибка и саботаж	Преднамеренные действия — как со стороны внутренних, так и внешних нарушителей — представляют собой массовую угрозу для всех защищаемых объектов. Большую угрозу также представляют халатность и человеческая ошибка, особенно в отношении защиты конфиденциальности и доступности объектов.
6	Запуск вируса через съемный носитель и внешние устройства	Использование съемных носителей и мобильных ИТ-компонентов внешнего персонала всегда связано с высоким риском заражения вирусом. См., например, случай с Stuxnet.
7	Чтение и запись новостей в сети ICS	Большинство компонентов контроля в настоящее время использует протоколы незашифрованного текста, таким образом, данная коммуникация остается незащищенной. Это упрощает чтение и ввод команд управления.
8	Несанкционированный доступ к ресурсам	Внутренним нарушителям и нападающим, чьи атаки следуют за первоначальным внешнем проникновением особенно просто добиться успеха, если сервисы и компоненты в сетевой схеме процесса не используют методы аутентификации и авторизации, или если эти методы являются ненадежными.
9	Атаки на компоненты сети	Нападающие могут манипулировать компонентами сети, чтобы провести атаку с применением технологии «незаконный посредник» или, например, упростить анализ трафика.
10	Технические сбои или форс-мажор	Сбои в результате экстремальных погодных условий или технических неполадок могут произойти в любое время — в таких случаях можно только минимизировать риск и потенциальный ущерб.

Таблица 3: 10 основных угроз для Промышленных систем управления

76 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), p. 15

77 См. Главы 2.3 и 2.4.

требуют срочных корректирующих действий. Первоначально их необходимо лишь выявить и постоянно отслеживать на предмет изменений.[78]

Уязвимые стороны могут находиться в следующих областях:[79]

- Организация
- Процессы и процедуры
- Практика управления
- Персонал
- Физическая среда
- Конфигурация информационной системы
- Аппаратное, программное или коммуникационное обеспечение
- Зависимость от сторонних организаций

В следующей таблице представлены примеры ресурсов, относящихся к ИКТ, и предположения о том, как нападающие могут нацеливаться на эти ресурсы и использовать их.

Актив	Описание возможных уязвимых мест и векторов атаки
Программное обеспечение	В приложения или в системное программное средство могут быть случайно или намеренно введены ошибки, и они могут использоваться для нарушения цели, для которой была предназначена данная программа.
Аппаратное обеспечение	Уязвимые места могут быть обнаружены в оборудовании, включая микропроцессоры, микроконтроллеры, монтажные платы, блоки питания, периферийные устройства, такие как принтеры или сканеры, устройства хранения данных и коммуникационное оборудование, включая сетевые карты. Манипуляции с этими компонентами могут тайным образом изменить предполагаемую функциональность компонента или предоставить возможности для ввода вируса.
Стыки между аппаратным и программным обеспечением	Примером такого стыка может быть перепрограммирование постоянной памяти компьютера (программируемого оборудования), которая может быть перепрограммирована ненадлежащим образом и тайно.
Каналы связи	Каналы коммуникации между системой или сетью и внешним миром могут использоваться злоумышленниками разными способами. Нарушители могут притворяться правомочными пользователями канала, создать затор в нем, и таким образом предотвратить его использование обычными пользователями или подслушать канал с целью получения информации, которая считается конфиденциальной или тайной.
Конфигурация	Большинство систем предоставляет различные варианты конфигурации, которые пользователи могут устанавливать на основании своих собственных представлений о сочетании безопасности и удобства. Поскольку удобство часто ценится больше безопасности, многие системы на практике конфигурированы небезопасно.
Пользователи и операторы	Полномочные пользователи и операторы системы или сети могут подвергнуться обману или шантажу, в результате которого они будут действовать по указанию злоумышленника или могут продавать свои услуги.
Поставщики услуг	Многие вычислительные центры полагаются на внешние стороны, которые оказывают им услуги, связанные с применением компьютерной техники, такие как техническое обслуживание или интернет-услуги. Злоумышленник может быть в состоянии убедить поставщика услуг совершить какие-то действия от его имени, например, установить агрессивную программу на целевой компьютер.

Таблица 4: Уязвимые стороны в киберпространстве[80]

78 Cf. ISO/IEC 27005, стр. 16

79 Cf. ISO/IEC 27005, стр. 16

80 На основании работы Фреда Шриера On Cyberwarfare, стр 48

Зависимость интеллектуальных сетей от информационных систем и сетей делает их особенно уязвимыми к атакам, при которых целенаправленно используются потенциальные уязвимые места.[81] Некоторые новые сложности обеспечения безопасности интеллектуальных сетей вызваны следующими факторами:

- Зависимость функционирования от сигналов датчиков
- Большая область для атаки

Кроме того, современные энергетические установки также в значительной степени зависят от высокоскоростных коммуникаций и автоматизированного и централизованного контроля над установками и устройствами. В энергетических системах особое значение имеют системы SCADA.[82]

3.3 Системы управления рисками, связанными с ИКТ, при управлении важнейшими объектами неядерной энергетической инфраструктуры

Эксплуатацию важнейших объектов инфраструктуры все чаще осуществляют частные, а не государственные организации (хотя данное утверждение справедливо не для всех стран). Это обстоятельство дополнительно повышает важность достижения совместного понимания по вопросам безопасной эксплуатации важнейших объектов неядерной энергетической инфраструктуры. Это единственный способ обеспечить разработку приемлемых механизмов — включая, при необходимости, механизмы регулирования — для обеспечения информационного взаимодействия и сотрудничества, а также для поддержания безопасности поставок. Обеспечение безопасности важнейших объектов энергетической инфраструктуры требует совместного понимания в отношении всех существующих требований, а также уязвимых мест всех компонентов, влияющих на цепь поставки энергоресурсов. Одним из методов решения этих вопросов является введение системы управления рисками.

Когда угрозы становятся рисками…

«Угроза несет в себе потенциал нанесения ущерба таким активам как информация, процессы и системы, а, значит, и организациям в целом».[83]

3.3.1 Принципы управления рисками

Риск — это абстрактное и сложное понятие, которое подробно рассматривается в ходе стандартизации. В общих чертах можно принять определение риска как воздействие неопределенности на цели.[84] Согласно другим подходам, риск определяется как сочетание вероятности происшествия и масштаба ущерба, который оно может причинить,[85] или как сочетание вероятности и воздействия какого-либо события.[86]

Термины «угроза», «уязвимая сторона» и «риск» часто путают, а иногда даже употребляют как синонимы. Однако для обеспечения соответствия стандартам управления рисками требуется четко понимать различия между данными терминами, что может быть затруднительно из-за различий между стандартами (см. следующее далее сравнение между стандартами ISO 31000 и ISO 27000). Таким образом, важно принять одно определение и последовательно использовать его.

➥ Таблица 5: Сравнение стандартов ISO 31000 и ISO 27000[87]

Национальный институт стандартов и технологии США (NIST) приводит дополнительный пример, в котором используется термин «угроза» (определение данного термина представлено в Главе 2.3). В этом определении учитываются уязвимые стороны, а также последствия, упомянутые выше.[88] В этом контексте оценку риска определяет результат взаимодействия угрозы, уязвимых сторон и последствий. Допущения, лежащие в основе этой модели, особенно подходят для иллюстрации опасности терроризма, поскольку здесь также учитывается степень воздействия.

➥ Рис. 7: Типичная модель риска[89]

Стандарт ISO/IEC 27032 определяет общие концепции управления рисками и представляет концепции уязвимых сторон, угроз и рисков в их общем контексте.

➥ Рис. 8: Определение концепций в стандарте ISO 27032[90]

Для успешного управления рисками организации требуются различные принципы и меры. Чтобы применить к управле-

81 US GAO 2011, стр. 9
82 NAP: Terrorism and the Electricity Power Delivery System (2012), стр. 2
83 ISO/IEC 27005:2011
84 Cf. ISO 31000:2009
85 Cf. ISO Guide 51:1999
86 Cf. ISO/IEC Guide 73
87 Cf. ISO 31000:2009 и ISO/IEC 27000:2009
88 NIST США 2010 г., стр. 9
89 NIST США, стр. 9
90 ISO 27032

	ISO 31000	ISO 27000
Угроза	-	Потенциальная причина нежелательного инцидента, который может вызвать нарушение в работе системы или организации
Уязвимость	-	Недостаток актива или системы контроля, который может использоваться для угрозы
Риск	Воздействие неопределенности на задачи	Сочетание вероятности события и его последствий

Таблица 5: Сравнение стандартов ISO 31000 и ISO 2700087

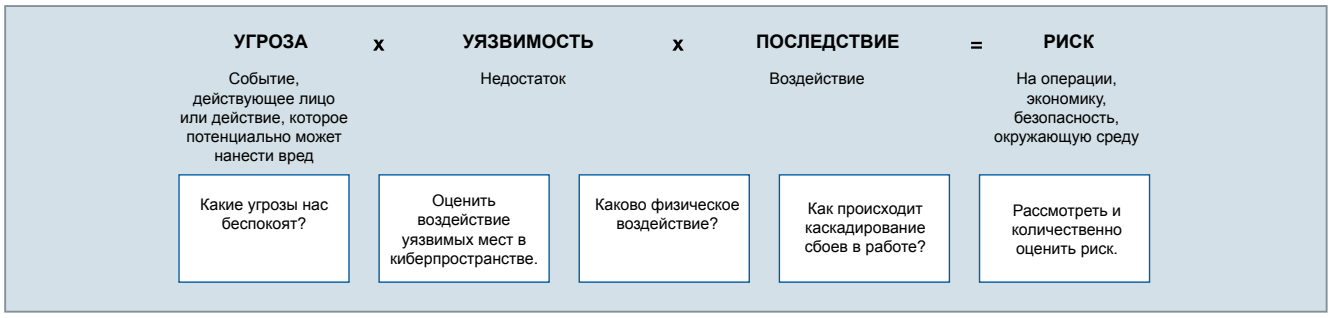


Рис. 7: Типичная модель риска

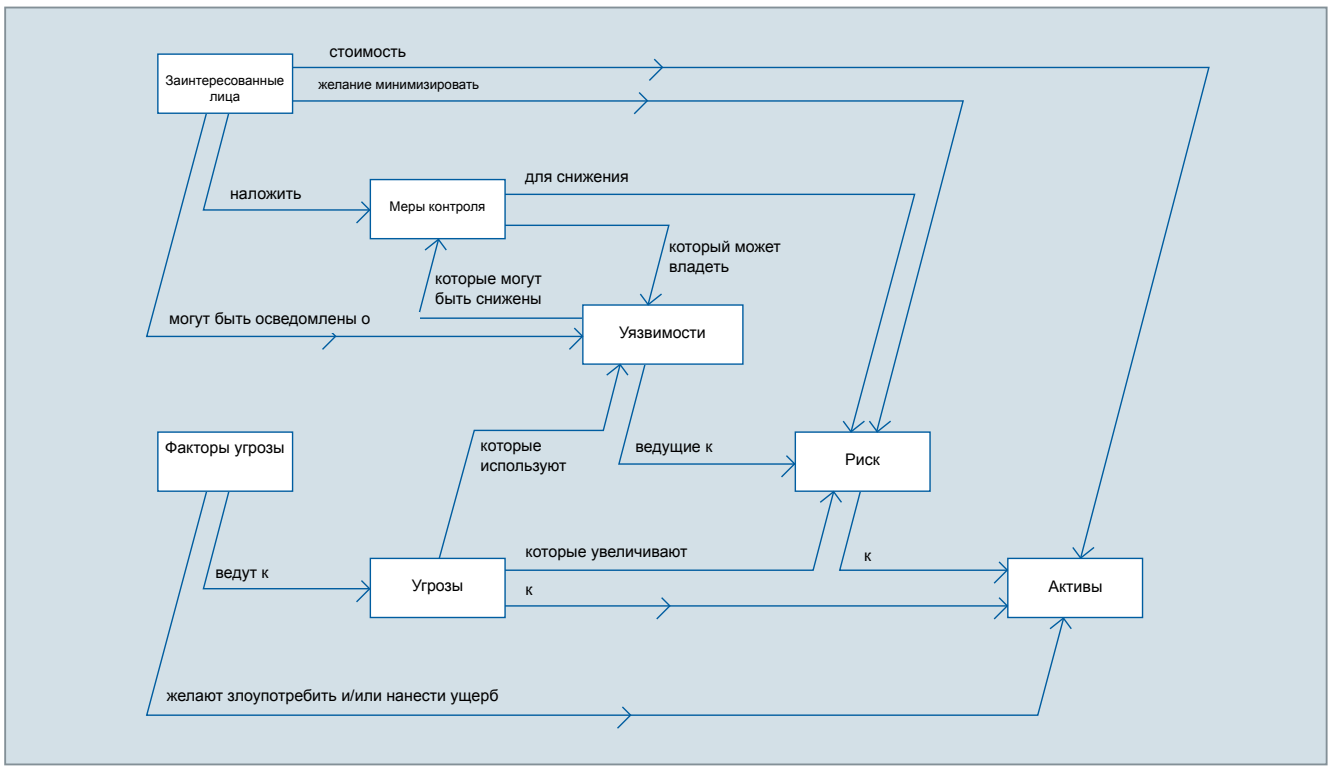


Рис. 8: Определение концепций в стандарте ISO 27032

нию рисками структурированный подход, необходимо объединить все требуемые аспекты и описать их в рамках одной комплексной системы, предназначенной помочь организациям в эффективном управлении рисками. Индивидуальная структура системы управления рисками будет зависеть от размера организации и сложности ее организационной структуры, ее подверженности риску, юридических норм, а также от уже имеющихся элементов управления рисками или систем управления.

В разных странах существуют различные подходы и стандарты построения системы управления рисками.[91] На международном уровне организационная структура и процесс управления рисками были описаны Международной организацией по стандартизации (ISO) в стандарте ISO 31000. Процесс управления рисками основан на принципе «Планирование, реализация, контроль, корректировка» (Plan, develop, control, action; PDCA) [92] и определяется как «набор компонентов, формирующий основу и организационную структуру для разработки, внедрения, мониторинга, проверки и постоянного усовершенствования управления рисками во всей организации».[93] Фактические методы построения системы управления рисками описываются как процесс, состоящий из пяти этапов.

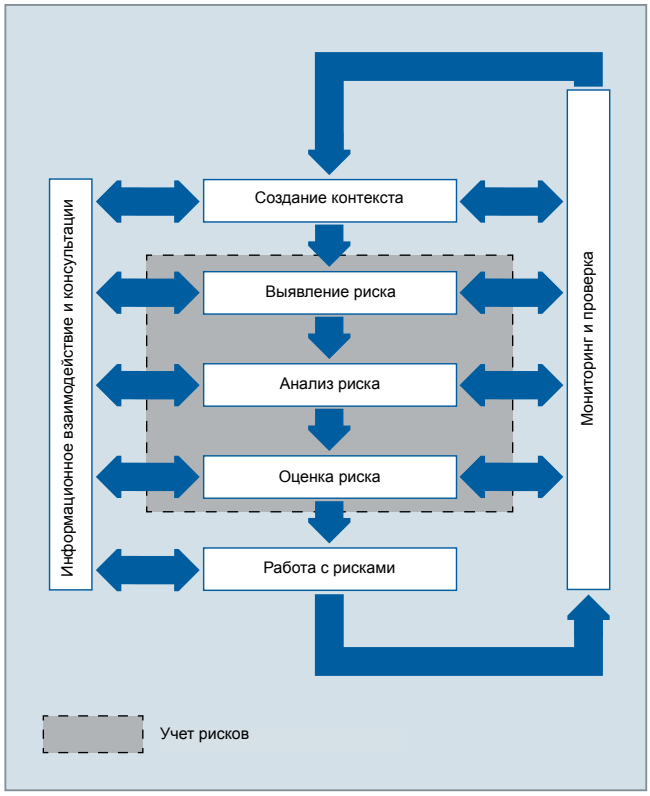


Рис. 9: Обзор процесса управления рисками[94]

Стандарты серии ISO 27000 распространяются исключительно на системы информационной безопасности и используются для адаптации к ним процесса управления рисками. Стандарт ISO/IEC 27005 соответствует общему подходу к управлению рисками, изложенному в стандарте ISO 31000, и применяет его принципы к сфере информационной безопасности. Исходя из описания управления рисками информационной безопасности, описанное внедрение системы управления рисками ИТ обеспечивает приемлемую основу для развития системы управления рисками, связанными с ИКТ.

Первый шаг заключается в том, чтобы установить общий контекст, учитывая при этом цели и определения внутренних и внешних параметров. Затем следует оценка рисков, которая представляет собой весь процесс выявления, анализа и определения степени риска. Значительная часть этого процесса приходится на определение потенциальных опасностей, событий, изменений или сценариев, которые могли бы препятствовать достижению организацией своих целей. В результате этого шага должен быть получен всеобъемлющий перечень рисков. Этот шаг особенно важен, поскольку все риски, не учтенные на данном этапе, будут исключены из всех последующих шагов. По этой причине особенно важно регулярно проводить мониторинг и анализ ситуации. Эти процедуры должны планироваться как существенная часть процесса управления рисками и включать регулярный мониторинг отдельных шагов процесса. В контексте выявления рисков также важно регулярно или по необходимости обновлять описание ситуации, включая в него новые угрозы, чтобы учитывать перспективы развития или изменения в среде риска.

После того как риски будут установлены, требуется получить основу для их оценки, определив вероятность их наступления и их потенциальное воздействие. В этот момент принимаются решения о том, с какими рисками необходимо бороться, и какие меры в этой борьбе являются приоритетными. Существуют различные способы управления рисками, включая их избегание, снижение, перенос или принятие.

При этом надо понимать, что риски не статичны. Угрозы, уязвимые стороны, вероятность наступления и последствия могут меняться быстро и непредсказуемо. Чтобы обеспечить полный и актуальный обзор ситуации с рисками и своевременно выявлять изменения, необходимо вести постоянный мониторинг и регулярно пересматривать риски. Как и с «петлей обратной связи» в структуре управления рисками

91 Поскольку настоящее руководство предназначено для международной аудитории, мы не перечисляем в нем национальные стандарты. Вместо этого мы сосредоточимся на международных стандартах, установленных Международной организацией стандартизации (ISO).

92 Цикл PDCA, также известный как цикл Деминга, описывает циклический четырехэтапный процесс решения проблемы («Планирование, реализация, контроль, корректировка»). Система стандарта ISO 31000 следует этой модели, по сути состоящей из этапов проектирования, внедрения, мониторинга и постоянного усовершенствования. Здесь мы сосредоточимся на этапе внедрения, поскольку в нем дается характеристика фактического процесса управления рисками.

93 Cf. ISO 31000:2009, стр. 2

94 ISO/IEC 27005:2011

NIPP США,[95] результаты мониторинга и пересмотра можно вносить обратно в систему как вводные данные на различных шагах процесса управления рисками в целях постоянного его усовершенствования.

При адаптации подхода, представленного здесь, к определенной организации или к определенному сектору, необходимо учитывать, что приведенный подход прежде всего является типовым и учитывает самые базовые функции. В него необходимо включить оценку рисков, характерных для организации или соответствующего сектора. При установлении общего контекста процесс следует переоценить и, возможно, пересмотреть, чтобы обеспечить его соответствие особенностям соответствующей организации или сектора.

Стандартное описание обзора и терминологии	
ISO/IEC 27000	Обзор и словарь
Стандартное описание общих требований	
ISO/IEC 27001	Требования
ISO/IEC 27006	Требования органов сертификации
Стандартное описание общих руководящих принципов	
ISO/IEC 27002	Кодекс профессиональной этики
ISO/IEC 27003	Внедрение
ISO/IEC 27004	Измерение
ISO/IEC 27005	Управление рисками
ISO/IEC 27007	Руководство по аудиту ISMS
Стандартное описание руководящих принципов для сектора	
ISO/IEC 27011	Руководящие принципы ISMS для телекоммуникационных организаций
ISO/IEC 27031	Руководящие принципы по готовности информационных и коммуникационных технологий к непрерывности деятельности
ISO/IEC 27032	Руководящие принципы для кибербезопасности
ISO/IEC 27033	Руководящие принципы для сетевой ИТ-безопасности

Таблица 6: Обзор компонентов серии стандартов ISO/IEC 27000[96]

3.3.2 Основные элементы серии стандартов ISO/IEC 27000

Серия стандартов ISO/IEC 27000 — это набор соответствующих стандартов информационной безопасности с охватом терминологии, требований, а также общих и конкретных указаний. Эта серия включает рекомендации по передовой практике для отдельных компонентов Системы управления информационной безопасностью (ISMS) верхнего порядка.

3.3.3 Подходы к управлению рисками в энергетической инфраструктуре

Европейская комиссия поручила разработку системы управления рисками компаниям Risk Solution и AEA Technology. Эта система предназначена для выявления и ликвидации уязвимых сторон в энергетическом секторе и секторе ИКТ. Она должна обеспечить ответственным сторонам в энергетическом секторе стандартизированный подход к количественной оценке рисков и управлению ими при международных поставках электроэнергии. Система управления рисками основана на анализе мер, уже используемых операторами в энергетическом секторе и правительствами государств-членов, а также действий, которые потребуются в будущем для ликвидации существующих пробелов в безопасности системы. Иными словами, она задает минимальный стандарт, но при этом может быть адаптирована отдельными государствами и операторами в соответствии с их потребностями и особенностями.

Система управления рисками построена таким образом, чтобы быть как можно более полезной максимальному числу заинтересованных сторон. Для этого она была сделана достаточно гибкой и позволяет каждому заинтересованному лицу учитывать риски, существующие в его собственной зоне ответственности. Например, на уровне ЕС основным преимуществом использования данной системы является управление рисками при международных поставках электроэнергии. На уровне государств-членов сетевому оператору может потребоваться выполнять управление рисками через

95 NIPP 2009, стр. 4

96 ISO/IEC 27000

другие, не обязательно государственные, границы. Эта система может использоваться на каждом уровне, поэтому до ее применения необходимо установить, на каком из следующих уровней она будет применяться.[97]

- На трансграничном уровне в пределах ЕС: В случаях, когда функциональный сбой в системе ИКТ ведет к перерыву в подаче энергии от одного государства-участника к другому государству-участнику, или когда нарушенный поток энергии передается транзитом через государство-участника по направлению к конечному пункту назначения.

- На трансграничном уровне за пределами ЕС: В случаях, когда функциональный сбой в системе ИКТ в стране, не входящей в ЕС, сказывается на подаче энергии в государство-участника.

- На национальном уровне государства-участника: В случаях, когда функциональный сбой в системе ИКТ в одной части национальной инфраструктуры страны сказывается на подаче энергии значительной части населения внутри одного государства-участника.

- На межорганизационном уровне: В случаях, когда функциональный сбой в системе ИКТ в одной организации сказывается на деятельности другой организации в результате сбоя в подаче энергии внутри одного государства-участника.

- На внутриорганизационном уровне: В случаях, когда функциональный сбой в системе ИКТ одной энергетической компании приводит к перерыву в подаче энергии внутри государства-участника, в котором находится эта компания.

Общий подход к управлению рисками, разработанный Международным советом по управлению рисками (IRGC), основывается на шаблонной структуре этого процесса. Этот шаблон разбивает деятельность в рамках процесса на следующие пять элементов:[98]

- Предварительная оценка для получения общего представления о риске.

- Оценка для определения знаний, необходимых для вынесения суждений и решений.

- Определение и анализ для оценки приемлемости риска.

- Управление для определения ролей участников процесса.

- Коммуникация для разработки процесса обмена информацией.

Как объясняется в исследовании Европейской комиссии, «система управления рисками в энергетике/ИКТ включает четыре этапа: предварительную оценку, оценку, определение и анализ, управление. На каждом этапе она напоминает пользователям о необходимости учитывать пятый элемент, коммуникацию. Эти шаги можно повторять, чтобы обеспечить основу для постоянного усовершенствования».[99]

➥ Рис. 10: Система управления рисками IRGC[100]

Кроме того, в рамках этой системы каждой стране и организации рекомендуется назначить эксперта, ответственного за внедрение системы управления рисками и реализацию ее целей для ликвидации выявленных уязвимых сторон. Примеры передовой практики для организации могут включать следующее:[101]

Поддержка этой деятельности и предоставление необходимых полномочий внутри организации директором или представителем старшего руководства.

- Наличие специалиста по управлению рисками, являющегося экспертом в данной области и способного выступить в роли внутреннего консультанта. Как правило, этот специалист также принимает на себя ответственность за ведение основной версии реестра рисков, отслеживая ход работ по согласованным действиям, направленным на управление возникающими рисками, а также за представление результатов по оценке рисков другим заинтересованным лицам, включая другие организации, имеющие отношение к выявленным трансграничным или межфункциональным нюансам. Теоретически специалист по управлению рисками может отвечать за взаимодействие с Европейской комиссией.

- Специалисты по инфраструктуре энергетики и ИКТ должны отвечать за выявление и анализ рисков

97 В контексте ОБСЕ к сообществу государств — участников ОБСЕ могут применяться следующие положения, относящиеся к ЕС.

98 Европейская комиссия: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), стр. 41

99 Европейская комиссия: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), стр 41

100 Европейская комиссия: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009)

101 Европейская комиссия: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), стр 42

Рис. 10: Система рисков IRGC

совместимости с помощью этой системы. Эту работу лучше всего проводить в рамках коллективных действий, например, путем проведения ряда специализированных семинаров, к ведению которых можно при необходимости привлечь специалиста по управлению рисками.

- Если в государстве-участнике проводится более подробный анализ воздействия и последствий (или рисков), экспертам может быть поручено провести полную количественную оценку политических, экономических и социальных последствий сбоев в подаче энергии. Это выходит за пределы качественной градации рисков, предложенной в настоящем документе.

- В случаях, когда в определенных ключевых областях взаимодействия требуются дополнительные меры по снижению риска, ответственность за исполнение согласованного плана действий должно нести то лицо, которое способно реализовать его наилучшим образом.

Индивидуальные задачи каждого этапа кратко представлены в Главе 3.5. Дополнительные предложения в отношении дальнейших действий можно найти в приложении к исследованию "Study on Risk Governance of European Critical Infrastructure in the ICT and Energy Sector".

При внедрении системы управления рисками также следует рассмотреть аспект, связанный с государственно-частными партнерствами (ГЧП).[102] В сентябре 2010 года Антитеррористическое подразделение (АТП ДПТНУ) [103] Секретариата ОБСЕ опубликовало тематический обзор, [104] в котором кратко представлены основные рекомендации для важнейших объектов энергетической инфраструктуры. Эти рекомендации были разработаны на проведенном под эгидой ОБСЕ семинаре государственно-частных экспертов «Protecting Non-Nuclear Critical Energy Infrastructure from Terrorist Attacks» («Защита важнейших объектов неядерной энергетической инфраструктуры от террористических атак»). ОБСЕ подчеркивает, что эти рекомендации не всегда предполагают согласие всех государств — участников ОБСЕ или Секретариата ОБСЕ с предлагаемыми мерами.

Основные рекомендации:

1. **Следовать комплексному подходу, основанному на оценке рисков.**
   Меры по защите энергетической инфраструктуры должны быть динамичными и основанными на актуальной и регулярно обновляемой оценке всех опасностей.

2. **Расширять рамки многостороннего сотрудничества.**
   Комплексный подход к защите важнейших объектов энергетической инфраструктуры, как указано выше, подразумевает координированное участие

102 См. Главу 5.1.

103 Cf. OSCE, URL: http://www.osce.org/atu (02/13/2013)

104 Cf. Protecting Critical Energy Infrastructure from Terrorist Attacks, URL: http://www.osce.org/atu/73638 (02/13/2013)

многочисленных заинтересованных сторон, представляющих различные государственные органы, государственный и частный сектор, а также зарубежные заинтересованные стороны.

3. **Разрабатывать гибкие меры по обеспечению безопасности, гарантирующие защиту на минимальном надлежащем уровне.**
   Уязвимые стороны и среда риска каждого важнейшего объекта энергетической инфраструктуры имеют свою специфику и динамику; их необходимо учитывать при обеспечении безопасности, чтобы обеспечить экономичность защиты и ее соответствие установленным рискам.

4. **Уделять больше внимания обеспечению готовности и общей устойчивости.**
   Готовность требует предварительного планирования действий в экстренной ситуации, тестирования и контроля, включая разработку планов информационного взаимодействия с широкой публикой/потребителями и энергетическими рынками. Для обеспечения большей устойчивости необходимо увеличить инвестиции в межсетевое взаимодействие и альтернативные маршруты поставок, а также в увеличение емкости хранилищ/стратегических запасов.

5. **Определить и устранить уязвимые места энергетического сектора в киберпространстве.**
   На сегодняшний день в мире, все более компьютеризованном и зависимом от ИКТ, традиционных мер физической безопасности («вооружение, ограждение и охрана») уже недостаточно. Необходимо в значительной мере повысить уровень общественной и корпоративной осведомленности и понимания вопросов кибербезопасности. Кроме того, должно поощряться развитие специальных навыков в вопросах обеспечения кибербезопасности.

6. **Развивать эффективное государственно-частное партнерство (ГЧП).** Необходимо четко определить роли и обязанности заинтересованных сторон в частном секторе и органов государственной власти в области обеспечения безопасности. Партнерство может развиваться в целях совместной оценки безопасности важнейших объектов энергетической инфраструктуры, пересмотра мер безопасности, разработки планов действий в чрезвычайных ситуациях и подготовки к реагированию на инциденты.

7. **Укреплять трансграничное/международное сотрудничество.**
   Последствия сбоя в работе одного энергетического инфраструктурного комплекса могут распространяться далеко за пределы государственных границ страны, где он расположен, будь то прекращение подачи или другой ущерб, включая экономический (например, рост цен на нестабильных рынках сбыта энергии) или экологический. Странам следует внимательно рассмотреть эти прямые и косвенные зависимости, что приведет к обоснованной заинтересованности в сотрудничестве с целью обеспечить целостность энергетической инфраструктуры.

Некоторые другие страны и организации разработали свои системы управления рисками. Например, система управления рисками США является неотъемлемой частью NIPP США.[105]

3.4 Резюме и рекомендации

В настоящей главе рассматривалась передовая практика применения систем управления рисками ИКТ с учетом возможных рисков терроризма. Рассмотренные здесь темы включают роль и значение ИКТ, основные компоненты, зависящие от ИКТ, системы управления рисками, векторы будущих атак и роль государств.

Резюмируя, можно сказать, что энергетические системы становятся все более сложными, а потому и все более восприимчивыми к перебоям в работе. Системный оператор управляет циклом электроснабжения с помощью информационных сетевых систем управления, которые используются для мониторинга особо важных процессов и функций. В будущем интеллектуальные сети все чаще будут заменять существующие электроэнергетические сети, автоматизируя ручные процессы и действия, совершаемые системными операторами, и повышая координацию выработки и хранения электричества. В то же время это приведет к возникновению новых уязвимых мест.

Инфраструктура ИКТ крайне важна. При этом вероятность цепной реакции в инфраструктуре ИКТ выше за счет взаимосвязи внутренних элементов. Системы SCADA входят в состав систем управления производственными процессами и дают возможность контролировать несколько процессов одновременно. Однако единая точка управления и тесно связанная сеть также являются причиной большей уязвимости к возможным атакам.

105 Краткое описание Системы управления рисками NIPP США представлено на сайте http://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf

Защита важнейших объектов инфраструктуры в целом и взаимосвязь важнейших объектов инфраструктуры и систем ИКТ имеют особое значение как для государственных властей, так и для компаний частного сектора. В целом необходимо помнить, что в области кибербезопасности проявляется все больше уязвимых мест, и осведомленность о потенциальных угрозах, а также готовность к противодействию им приобретают все большее значение. Внедрение системы управления рисками предусматривает единый метод выявления и устранения уязвимых мест.

Система управления рисками, представленная в Главе 3.4.3, состоит из нескольких этапов. В описании каждого этапа перечислены задачи, выполнение которых способно упростить внедрение системы. Ниже перечислены задачи, которые необходимо выполнить на каждом из этих этапов:[106]

Этап предварительной оценки

1. Определите взаимосвязи между системами энергетики и ИКТ, которые являются потенциальными целями и должны быть учтены в процессе управления рисками. Между системами энергетики и ИКТ существуют взаимосвязи, нарушение которых может привести к сбоям международных поставок электроэнергии.

2. Определите основных действующих лиц, которые должны быть включены в процесс оценки рисков, и их зоны ответственности в рамках рассматриваемых систем.

3. Определите основные документы, стандарты и регулирующие положения, относящиеся к рассматриваемым системам.

4. Рассмотрите вопрос о том, могли ли изменения на рынках, в цепях поставок и технологиях привести к повышению уровня рисков сбоя поставки энергии в энергетическом секторе и секторе ИКТ.

Этап оценки

1. Используя список потенциальных целей, полученный на этапе предварительной оценки, рассмотрите воздействие функционального сбоя каждой системы и оцените каждое из воздействий в соответствии с согласованной шкалой.

2. Пересмотрите оценку вопросов в отношении угроз сбоя в поставках энергии из-за нарушений взаимосвязи между энергетическим сектором и ИКТ.

3. Для каждой из систем, определенных как потенциальные цели в задаче 1, перечислите наиболее вероятные угрозы, которые могут привести к нарушению функционирования системы и вызвать сбой, учитывая действующие в настоящее время меры обеспечения безопасности.

4. Определите вероятность успешной реализации угрозы для каждой системы с оценкой критичности.

5. Классифицируйте каждое событие риска в соответствии с качеством имеющейся информации.

Этап определения и анализа

1. Поместите каждое установленное событие риска в матрицу приемлемости риска. Используйте показатели воздействия и уязвимости, полученные при выполнении предыдущих задач.

2. Проверьте полученные результаты, чтобы установить нехватку информации или скрытые события риска.

3. Опишите события риска по приоритетам с соответствующим обоснованием.

Этап управления

1. Рассмотрите имеющиеся варианты управления приоритетными рисками и выберите наиболее эффективные из них. Сформируйте стратегию управления рисками.

2. Определите лиц, ответственных за реализацию мероприятий, направленных на управление рисками, и получите их согласие.

3. Оцените ход работы по управлению рисками и, при необходимости, внесите улучшения в программу.

Вся система управления рисками и примеры контрольных листов и шаблонов представлены в приложении к документу Европейской комиссии.[107]

106 Европейская комиссия: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), стр. 43 ff

107 Европейская комиссия: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009)

4. Передовая практика мер безопасности в ИКТ по снижению рисков терроризма в киберпространстве

ОБСЕ Организация по безопасности и сотрудничеству в Европе

4. Передовая практика реализации мер безопасности в ИКТ по снижению рисков терроризма в киберпространстве

В данной главе рассматриваются образцы передовой практики реализации мер безопасности в ИКТ в связи с угрозами терроризма в киберпространстве. Здесь также рассматриваются применимые стандарты и стратегии.

4.1 Применение стандартов, относящихся к ИКТ

В других секторах уже существуют общепринятые стандарты, содержащие требования к безопасности и меры, которые могут применяться к важнейшим объектам неядерной энергетической инфраструктуры и системам ИКТ.[108] В настоящее время ведется работа по усовершенствованию этих стандартов и по разработке дополнительных стандартов. Перечисленные ниже стандарты особенно актуальны при обеспечении кибербезопасности систем ИКТ на важнейших объектах неядерной энергетической инфраструктуры:

- В первую очередь следует упомянуть стандарт серии ISO 27000. В нем содержится описание операционных и технических требований к управлению информационной безопасностью. Стандарт управления информационной безопасностью ISO 27001 обеспечивает основу, которая затем развивается в стандарте ISO 27002. Стандарты с более высокими номерами – многие из них еще находятся на стадии активной разработки – применяются к внедрению с учетом особенностей сектора.

- Один из последних стандартов этой серии, ISO 27032,[109] особым образом сосредоточен на проблемах, возникающих в связи со сложным взаимодействием между интернет-безопасностью, сетевой безопасностью и безопасностью приложений. Таким образом, в нем рассматриваются системы контроля для всех заинтересованных лиц в киберпространстве (организации потребителей и поставщиков). Уникальность заключается в том, что здесь однозначно определены такие темы как контроль, направленный

CIP-002	Выявление важнейших киберактивов
CIP-003	Меры контроля над управлением безопасностью
CIP-004	Персонал и профессиональная подготовка
CIP-005	Электронный периметр безопасности
CIP-006	Физическая безопасность киберсистем BES
CIP-007	Управление безопасностью систем
CIP-008	Представление информации об инцидентах и планирование ответных мер
CIP-009	Планы восстановления деятельности для киберсистем BES

Таблица 7: Отдельные стандарты NERC CIP (требования)[117]

108 Европейская комиссия: WP 2.2 Inclusion of effective security measures for smart grid security and resilience (2012)

109 Руководство BS ISO/IEC 27032:2012 по кибербезопасности

на предотвращение психологических атак, готовность к кибербезопасности и осведомленность. Особенно важно то, что в этот стандарт включена структура распространения информации и координации.

- Стандарт IEC 62351 направлен непосредственно на обеспечение информационной безопасности для функционирования диспетчерского пункта энергосистемы. В основном он обеспечивает внедрение стандартов безопасности, влияющих на протоколы передачи данных, определенные рабочей группой IEC TC 57, в частности, серия IEC 60870-5, серия IEC 60870-6, серия IEC 61850, серия IEC 61970 и серия IEC 61968. Эти стандарты в основном применяются к производителям. Группа M/490 SGIS[110] намерена расширить эти стандарты, включив в них особые технические аспекты для обеспечения кибербезопасности интеллектуальных сетей.
- Стандарты серии IEC 62443 (созданные на основе ISA-99[111]) охватывают вопросы безопасности для Промышленных систем автоматизации и управления (IACS). Основное внимание уделяется операционной передовой практике. Этот стандарт был разработан по инициативе подрядчиков и конечных пользователей различных отраслевых секторов, включая крупные нефтяные и газовые компании.[112] Он предназначен для владельцев активов, системных интеграторов и поставщиков запасных частей и содержит отдельные подстандарты. При разработке стандарта IEC 62443 была предпринята попытка включить в него существующие стандарты и обеспечить его соответствие им, в особенности это касается стандартов NISTIR 7628 и ISO 27001/2. После опубликования этой серии[113] было объявлено о запланированных крупных изменениях, с проектом

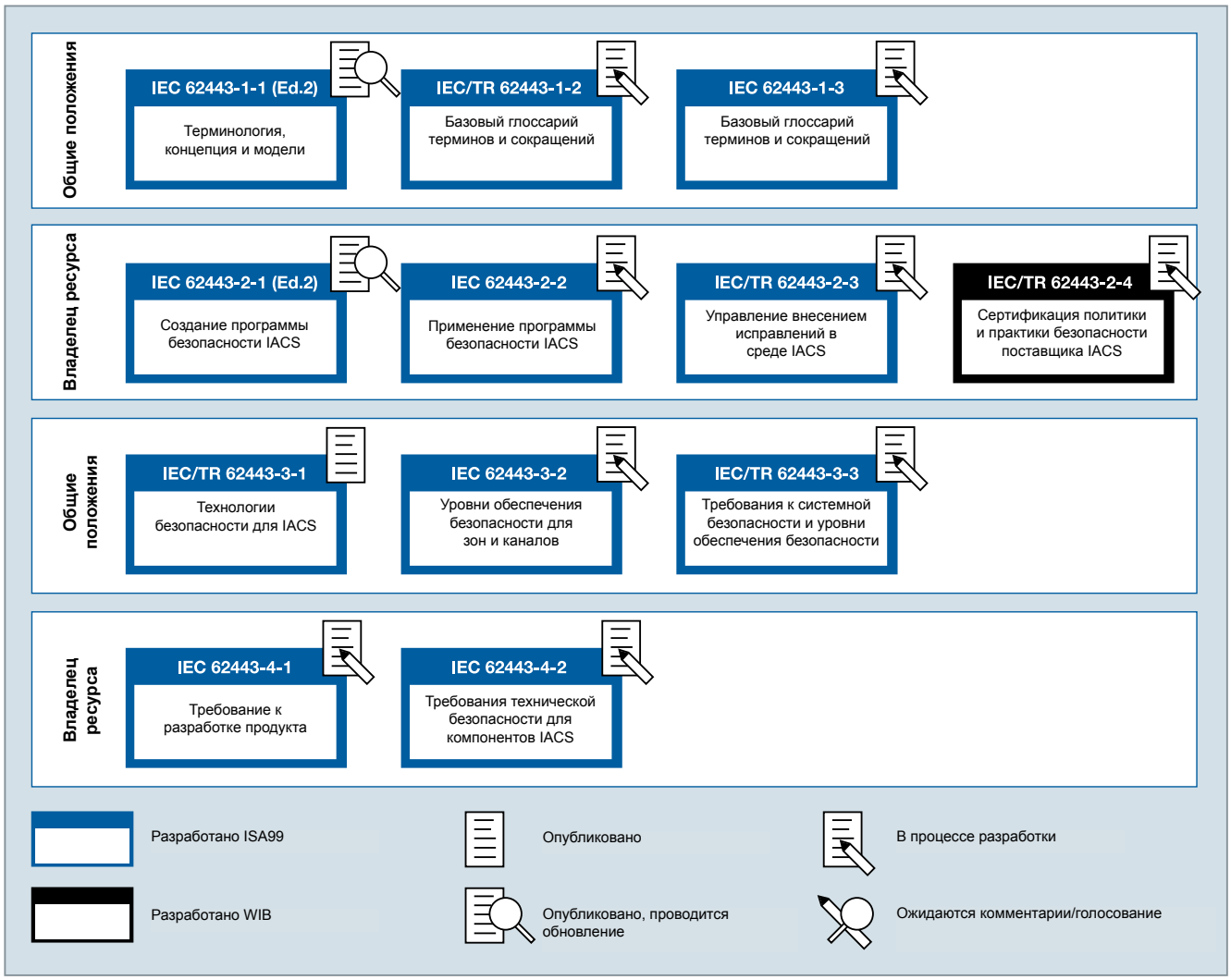


Рис. 11: Стандарт серии IEC 62443

110 Европейская комиссия EG-ENERGY, мандат M/490, рабочая группа SGCG-SGIS

111 ISA-99: Безопасность промышленных систем автоматизации и управления, серия стандартов Международного общества автоматизации (ISA)

112 IEC 62443-2-4 A Baseline Security Standard for Industrial Automation Control Systems, URL: http://ics-cert.us-cert.gov/icsjwg/presentations/fall2011/D2-24-0200pm_Track1_Ahmadi-Holstein_rr_Title-BaseSecStandIndAuto.pdf (02/14/2013)

113 Самые важные разделы были завершены в период с 2009 по 2011 годы.

которых уже можно ознакомиться. Ожидается, что текущий этап будет завершен в начале 2013 года.

- Специальная публикация NIST 800-39 «Managing Information Security Risk – Organization, Mission, and Information System View» является базовым документом для стандартов безопасности и руководств, имеющих отношение к FISMA,[114] и разработанных NIST, в котором даются ссылки на все дополнительные публикации, относящиеся к NIST. В отношении системы ISMS в ней даются ссылки – как и в других публикациях NIST – на стандарты ISO 27000 и ISO 31000 / ISO 27005 (управление рисками). В нем рекомендуется единый подход к управлению рисками.

- Стандарт NISTIR 7628 (Руководство по кибербезопасности интеллектуальных сетей) предназначен для обеспечения кибербезопасности инфраструктуры электроэнергетики. Главное внимание в отчете уделяется требованиям к безопасности. В Части 1 перечислены общие требования к безопасности и даны многочисленные ссылки на другие стандарты NIST в отношении конкретных требований. Здесь определено семь областей интеллектуальных сетей (операции, распределение, передача и т.д.) и определены логические категории интерфейсов (например, интерфейсы между системами управления внутри одной и той же организации и между разными организациями). Затем к этим категориям интерфейса применяются требования к безопасности (например, целостность, аутентификация, пропускная способность, требования по работе в режиме реального времени).

- Большинство требований к безопасности в стандарте NISTR 7628 охвачены стандартами ISO 27001, 27002 и IEC 62351. Приложение A к Каталогу рекомендаций по безопасности системы управления на 90 процентов совпадает с NIST, но в нем также содержатся дополнительные перекрестные ссылки на меры безопасности в следующих стандартах: FIPS 140-2, NERC CIP и IEEE 1402 (Руководство по физической и электронной безопасности электрических подстанций).[115]

- Североамериканская корпорация по обеспечению надежности электросистем (NERC) разработала стандарты кибербезопасности «Защита важнейших объектов инфраструктуры (CIP) NERC».[116] Также имеются отдельные стандарты построения комплексной системы кибербезопасности от CIP-002 до CIP-009. Соблюдение стандартов CIP стало обязательным для поставщиков электроэнергии после принятия Закона об энергетической политике 2005 года (EPAct). Проверки начались в 2011 году. В CIP также используется подход, основанный на оценке рисков, в соответствии с которым особое внимание уделяется «важнейшим активам киберпространства» основной сети энергосистемы.

В стандарте NIST SP 800-53 (Рекомендованные системы контроля безопасности для федеральных информационных систем

Краткое резюме	по странам
Эстония (2008 г.)	Эстония подчеркивает необходимость создания безопасного киберпространства в целом и уделяет особое внимание безопасности информационных систем.[126] Все рекомендованные меры носят гражданский характер и сосредоточены на регулировании, обучении и сотрудничестве.
Финляндия (2008 г.)	Основа стратегии страны заключается во взгляде на кибербезопасность как на вопрос безопасности данных и на дело экономической важности, которое тесно связано с развитием финского информационного общества.
Словакия (2008 г.)	В рамках стратегии страны вопросы информационной безопасности играют важнейшую роль в функционировании и развитии общества. В связи с этим цель стратегии заключается в тщательно продуманной разработке системы. Цели стратегии преимущественно сосредоточены на профилактике, а также на готовности и устойчивом развитии.

Продолжение на следующей странице

114 Федеральный закон США Федеральный закон об управлении информационной безопасностью 2002 г. (FISMA)

115 Европейская комиссия: WP 2.2 Inclusion of effective security measures for smart grid security and resilience (2012)

116 Основано на стандартах NERC 1200 (и более позднего 1300)

117 NERC: Mandatory Standards Subject to Enforcement, URL: http://www.nerc.net/standardsreports/standardssummary.aspx (02/13/2013)

Краткое резюме	по странам
Чехия (2011 г.)	Важнейшие цели стратегии кибербезопасности включают защиту от угроз, которым подвергаются информационные и коммуникационные системы и технологии, и снижение потенциальных последствий в случае атаки на ИКТ. Стратегия в основном сосредоточена на беспрепятственном доступе к услугам, целостности данных и конфиденциальности киберпространства Чехии и координируется с другими связанными с ней стратегиями и концепциями.
Франция (2011 г.)	Франция сосредоточена на том, чтобы информационные системы могли противостоять происшествиям в киберпространстве, которые могут нарушить доступность, целостность или конфиденциальность данных. Франция акцентирует внимание как на технических средствах, необходимых для обеспечения безопасности информационных систем и для борьбы с киберпреступностью, так и на киберзащите.
Германия (2011 г.)	Германия сосредоточена на предотвращении и преследовании кибератак, а также на профилактике соответствующих сбоев ИТ, особенно возникающих на важнейших объектах инфраструктуры. Эта стратегия создает основу для защиты важнейших информационных структур. В ней рассматриваются существующие нормативы на предмет, требуются ли дополнительные силы для того, чтобы обезопасить системы ИТ в Германии, и если требуются, то где. Если дополнительные меры необходимы, они реализуются путем обеспечения базовых функций безопасности, утвержденных государством, и путем поддержки малого и среднего бизнеса за счет создания новой оперативной группы.
Литва (2011 г.)	Литва стремится к определению целей и задач для развития электронной информации, чтобы обеспечить конфиденциальность, целостность и доступность электронной информации и услуг, оказываемых в киберпространстве; защитить сети электронной коммуникации, информационные системы и важнейшие объекты информационной инфраструктуры от инцидентов и кибератак; защитить личные данные и право на неприкосновенность частной жизни. В стратегии также определяются задачи, которые, при их реализации, позволят обеспечить полную безопасность киберпространства и компаний, работающих в нем.
Люксембург (2011 г.)	Признавая распространенность ИКТ, стратегия устанавливает, что предотвращение любого неблагоприятного воздействия на здоровье и безопасность населения или на экономику является приоритетной задачей. В ней также указывается значение ИКТ для граждан, общества и экономического роста. Стратегия основана на пяти направлениях деятельности. Они посвящены защите важнейших объектов инфраструктуры и реагированию на инциденты, модернизации нормативно-правовой среды, национальному и международному сотрудничеству, образованию и осведомленности и продвижению стандартов.
Нидерланды (2011 г.)	Нидерланды стремятся к созданию безопасной и надежной среды ИКТ и опасаются злоупотреблений и (крупномасштабных) сбоев, и в то же время признавая необходимость в защите открытости и свободы Интернета. Нидерланды включают в свою стратегию определение кибербезопасности: «Кибербезопасность представляет собой свободу от опасности или ущерба, наносимого сбоем или побочным эффектом работы ИКТ или злоупотреблением ИКТ. Опасность или ущерб, связанный со злоупотреблениями или побочными эффектами, может состоять из ограничения доступности и надежности ИКТ, нарушения конфиденциальности информации, хранящейся в ИКТ, или повреждения целостности такой информации».
Великобритания (2011 г.)	Подход Великобритании основывается на национальных задачах, связанных с развитием кибербезопасности: сделать Великобританию страной с крупной экономикой инноваций, инвестиций и качества в области ИКТ, благодаря чему она будет в состоянии полностью использовать потенциал и преимущества киберпространства. Задача заключается в том, чтобы снижать риски, связанные с киберпространством, такие как кибератаки преступников, террористов и государств, чтобы сделать его безопасным пространством для граждан и компаний.

Таблица 8: Стратегии национальной кибербезопасности (страны ЕС)

и организаций)[118] представлены различные системы контроля безопасности для федеральных информационных систем США на основе структуры управления рисками. В нем также представлен комплект базовых средств контроля безопасности для обеспечения соблюдения минимальных стандартов. В издание 3 включено приложение по системам контроля безопасности ICS. Содержание этого приложения будет перенесено в окончательную версию стандарта NIST SP 800-82.

Стандарт NIST SP 800-82 (Руководство по безопасности промышленных систем управления) сосредоточен на системах SCADA и PLC/DCS. В нем описаны угрозы и уязвимые стороны, а также меры по их устранению. В стандарте SP 800-39 задаются принципы построения общей системы.

Все указанные выше стандарты (за исключением IEC 62351, который отличает слишком узкая сфера применения[119]) базируются на классических подходах на основе риска, совместимых с такими стандартами управления рисками как ISO 27005.

Стандарт ICE 62443, применяемый области промышленных компонентов (SCADA), был усовершенствован и скорректирован для соответствия стандартам серии ISO/IEC 27000. Работа над текущим проектом должна быть завершена в начале 2013 года. Так как в усовершенствовании данного стандарта широко участвовали представители промышленного сектора, ожидается, что он будет широко использоваться.

➥ Рис. 11: Стандарт серии IEC 62443[120]

Вследствие большого количества совпадений между стандартом серии ISO 27000 и стандартом безопасности интеллектуальных сетей NISTR 7628 группа M/490 SGIS рекомендовала разработать отраслевой стандарт для интеллектуальных сетей в рамках серии ISO 27000. Этот стандарт должен будет охватить важные аспекты кибербезопасности интеллектуальной сети. Он также возложит часть ответственности на разработчиков и установщиков ИКТ, а не только на владельцев и операторов. В целом в области стандартизации и регулирования по всему миру происходят большие изменения, заслуживающие пристального внимания.

4.2 Разработка национальной стратегии кибербезопасности

Стратегии определяют цели, пути и способы действий в определенной сфере деятельности. Стратегия национальной кибербезопасности (NCSS) представляет собой один из подходов к повышению уровня безопасности и стабильности при использовании киберпространства. Степень зависимости важнейших объектов национальной инфраструктуры от киберприложений обычно играет в этом контексте основную роль. Таким образом, NCSS обеспечивает «стратегическую структуру для подхода страны к кибербезопасности».[121]

В настоящее время не существует общего определения кибербезопасности на международном уровне. В выпуске 2013 года «Стратегии кибербезопасности для Европейского Союза: открытое, безопасное и надежное киберпространство» дается европейское определение этого термина[122]. Однако концепции кибербезопасности и других ключевых терминов варьируются в зависимости от страны. Отсутствие международной стратегии усовершенствования кибербезопасности несколько затрудняет международное сотрудничество.[123] Большинство национальных стратегий кибербезопасности или эквивалентных заявлений о принципах международных организаций пытается компенсировать этот недостаток путем прямого рассмотрения особой роли международного сотрудничества и определения мер, способных продвигать и поддерживать сотрудничество между странами, например, норм поведения в киберпространстве и мер по укреплению доверия.

4.2.1 Страны ЕС

Помимо стратегии кибербезопасности ЕС и предложенной директивы Европейской комиссии[124], за последние четыре года свои национальные стратегии кибербезопасности опубликовали десять государств–членов ЕС. В ENISA представлен краткий обзор каждой стратегии:[125]

➥ Таблица 8: Стратегии национальной кибербезопасности (страны ЕС)

118 В настоящее время в 3 редакции (2009 г.) с изменениями 2010 г.

119 Стандарт IEC 62351 описывает только вопросы внедрения протокола безопасности, в связи с чем имеет высокую важность для производителей оборудования.

120 Security for industrial automation and control systems (2011), URL: http://ics-cert.us-cert.gov/icsjwg/presentations/fall2011/D2-24-0200pm_Track1_Ahmadi-Holstein_rr_Title-BaseSecStandIndAuto.pdf (02/14/2013)

121 Национальные стратегии кибербезопасности: ENISA (2012), стр. 4

122 Европейская комиссия: Стратегия кибербезопасности Европейского Союза: открытое, безопасное и надежное киберпространство (02/07/2012), стр. 3, URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

123 Европейская комиссия: Стратегия кибербезопасности Европейского Союза: открытое, безопасное и надежное киберпространство (02/07/2012), стр. 3, URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

124 Европейская комиссия: Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM (2013) 48 final, 02/07/2013

125 Национальные стратегии кибербезопасности: ENISA (2012), стр. 5, и http://www.ccdcoe.org/328.html (март 2013 г.)

126 В мае 2007 года Эстония стала первым европейским государством, государственные и банковские сети которого подверглись массовой кибератаке. Причастность конкретного лица смогла быть доказана лишь для части атаки, затронувшей также веб-сайт одной из политической партий страны. См. "Estonia fines man for 'cyber war'". BBC. 2008-01-25. Загружено 2013-03-22. http://news.bbc.co.uk/2/hi/technology/7208511.stm.

4.2.2 Страны, не входящие в ЕС

В данном разделе кратко представлены стратегии кибербезопасности трех стран, находящихся за пределами Европы.[127] Другие страны, такие как Австралия,[128] Индия[129] и Новая Зеландия,[130] также опубликовали государственные стратегии кибербезопасности.

США

США впервые опубликовали свою Государственную стратегию по безопасности киберпространства в 2003 году в рамках Государственной стратегии национальной безопасности. В этом документе описывается комплекс мероприятий в семи взаимосвязанных областях, основанный на модели сотрудничества с участием государства, международных партнеров и частного сектора:

- Экономика: Продвижение международных стандартов и инновационных, открытых рынков
- Защита наших сетей: Повышение безопасности, надежности и устойчивости
- Правопорядок: Расширение сотрудничества и верховенства права
- Оборона: Подготовка к сложным задачам обеспечения безопасности в 21 веке
- Управление Интернетом: Продвижение эффективных и инклюзивных структур
- Международное развитие: Обеспечение мощности, безопасности и процветания
- Свобода в Интернете: Поддержка основных свобод и права на неприкосновенность частной жизни

В международной стратегии США в отношении киберпространства: «Prosperity, Security, and Openness in a Networked World»[131], подготовленной в мае 2011 года, сформулирована международная политика США, направленная на создание открытого, безопасного, надежного и интероперабельного киберпространства, поддержания стабильности с помощью норм поведения в киберпространстве и использование дипломатических, защитных и развивающих средств для решения сложных задач 21 века. Кроме того, на фоне растущей серьезности угроз для важнейших объектов инфраструктуры США и необходимости интеграции физической и кибербезопасности для обеспечения защиты важнейших объектов инфраструктуры, в феврале 2013 года был выпущен Указ президента США о повышении кибербезопасности важнейших объектов инфраструктуры, а также была опубликована новая директива президента о важнейших инфраструктурных системах и устойчивости (PPD-21), которая должна быть реализована одновременно с этим Указом[132]. Оба документа ставят перед органами государственной власти США на всех уровнях задачи, направленные на улучшение выявления и защиты важнейших объектов инфраструктуры США и совершенствование государственно-частного сотрудничества и информационного взаимодействия, в том числе в отношении угроз и их ликвидации, поскольку приблизительно 85% важнейших объектов инфраструктуры США принадлежат компаниям частного сектора и эксплуатируются ими.

Канада

Канада опубликовала свою стратегию кибербезопасности в 2010 году.[133] Эта стратегия строится на трех основных элементах:

- Обеспечение безопасности государственных систем: Первый элемент направлен на четкое определение ролей и обязанностей по укреплению безопасности федеральных киберсистем и повышение осведомленности о кибербезопасности в государственных органах.
- Партнерство в целях обеспечения защиты важнейших киберсистем, находящихся вне юрисдикции федерального правительства: Второй элемент охватывает ряд партнерских инициатив с провинциями и территориями, а также подразумевает участие частного сектора и важнейших инфраструктурных секторов.
- Оказание помощи канадцам для обеспечения их безопасности в Интернете: Третий элемент охватывает борьбу с киберпреступностью и

127 National Cyber Security Strategies: ENISA (2012), стр. 7 f

128 Правительство Австралии: Cyber Security Strategy (2009), URL: http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf (02/15/2013)

129 Department of Electronics and Information Technology, Government of India, URL: http://deity.gov.in/content/cyber-security-strategy (02/15/2013)

130 Правительство Новой Зеландии: Cyber Security Strategy (2011), URL: http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf (02/15/2013)

131 International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, (май 2011 г.), URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

132 Белый дом США: Executive Order on Improving Critical Infrastructure Cybersecurity, (02/12/2013), URL: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Белый дом США: Presidential Policy Directive on Critical Infrastructure Systems and Resilience (PPD-21), (02/12/2013), URL: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

133 Канада: Canada's Cyber Security Strategy – For a stronger and more prosperous Canada (2010), URL: http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/ccss-scc-eng.aspx

защиту канадских граждан в сети. В рамках этого элемента рассматриваются вопросы анонимности и конфиденциальности.

Япония

Япония опубликовала свою стратегию кибербезопасности в 2010 году.[134] Ее можно разделить на несколько основных направлений:

- Дополнение политик с учетом возможных кибератак и создание организации, специализирующейся на ответных мерах.
- Формирование политики, адаптированной к изменениям в среде информационной безопасности.
- Реализация активных, а не пассивных мер информационной безопасности.

Основные мероприятия, охватываемые стратегией, включают:

- Преодоление рисков ИТ для обеспечения безопасности и защиты общества.
- Реализация политики, укрепляющей национальную безопасность и расширяющей знания в области управления критическими ситуациями в киберпространстве, а также интеграция этой политики с политикой в сфере ИКТ как основа социально-экономической деятельности.
- Создание трехчастной политики, комплексно охватывающей перспективы национальной безопасности, управление критическими ситуациями и защиту населения/пользователей. При разработке политики информационной безопасности необходимо учитывать общественное мнение и мнение пользователей.
- Создание политики информационной безопасности, способствующей стратегии экономического роста.
- Создание международных альянсов.

4.2.3 Рекомендации по политике, направленной на обеспечение кибербезопасности

О признании значимости кибербезопасности свидетельствует значительное количество национальных стратегий и заявлений о принципах на эту тему, опубликованных недавно многими государствами — участниками ОБСЕ. Однако в этих документах также проявляются значительные различия в определении кибербезопасности и других ключевых терминов. В ходе работы над обзором стратегий национальной кибербезопасности Европейское агентство по сетевой и информационной безопасности (ENISA) подготовило рекомендации для будущего сотрудничества всех государств–членов ЕС в области кибербезопасности. Эти рекомендации могут распространяться и на международное сотрудничество между всеми странами. Наиболее важные из них перечислены ниже:[135]

Краткосрочные:

- Четко определите сферу применения и цели стратегии, а также точно сформулировать определение кибербезопасности, использованное в ней.
- Изучите и рассмотрите мнения и соображения представителей всех государственных ведомств, национальных регулирующих органов и других государственных учреждений.
- Сотрудничайте с другими государствами — участниками и с Европейской комиссией, учитывая трансграничный и глобальный характер вопросов кибербезопасности.
- Осознайте, что в силу постоянного развития и изменения киберпространства и кибербезопасности стратегия должна быть развивающимся и адаптируемым документом.
- Помните о том, что указанное выше относится не только к новым угрозам, но и к возможностям усовершенствования и повышения эффективности использования информационных и коммуникационных технологий во благо государства, отрасли и граждан.

134 Япония: Information Security Strategy for Protecting the Nation (05/11/2010), URL: http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf

135 National Cyber Security Strategies: ENISA (2012), стр.12

Долгосрочные:

- Согласуйте достаточно точную для формирования общих целей во всех странах ЕС общепринятую концепцию развития кибербезопасности.
- Обеспечьте отсутствие противоречий между стратегией кибербезопасности ЕС и государств — членов и целями международного сообщества. Более того, стратегии должны поддерживать общие усилия по разрешению сложных задач в сфере кибербезопасности.

ENISA готовит руководство по передовой практике в целях оказания поддержки странам в разработке, внедрении и реализации СНК.

Государственный и частный секторы должны более тесно сотрудничать при внедрении СНК. ENISA рекомендует сотрудничать путем обмена информацией и передовыми практиками, а также проведения локальных и международных учений.

4.2.4 Рекомендации по политике, направленной на обеспечение кибербезопасности интеллектуальных сетей

Обеспечение безопасности интеллектуальных сетей является одной из самых актуальных проблем в области кибербезопасности, в особенности в энергетическом секторе. ENISA выпустило на эту тему комплексное исследование,[136] которое завершается десятью фундаментальными рекомендациями. Несмотря на то что идеи, содержащиеся в этих рекомендациях, в первую очередь предназначены для институтов ЕС и государств — членов ЕС, они также могут использоваться и другими государствами — участниками ОБСЕ:

- Рекомендация 1. Европейская комиссия (ЕК) и компетентные органы государств — участников должны реализовывать инициативы по усовершенствованию структуры регулирования и политики в отношении кибербезопасности интеллектуальных сетей на национальном уровне и на уровне ЕС.

- Рекомендация 2. Европейская комиссия в сотрудничестве с ENISA и государствами-участниками должна способствовать созданию государственно-частного партнерства для координации инициатив в области кибербезопасности интеллектуальных сетей.

- Рекомендация 3. ENISA и Европейская комиссия должны поддерживать инициативы по повышению осведомленности и обучению.
- Рекомендация 4. Европейская комиссия и государства — участники в сотрудничестве с ENISA должны поддерживать инициативы по распространению и передаче знаний и опыта.

- Рекомендация 5. Европейская комиссия должна совместно с ENISA, органами кибербезопасности государств — участников, партнерами из частного сектора и, возможно, с некоторыми партнерами за пределами ЕС разработать минимальный комплекс мер безопасности на основании существующих стандартов и нормативов.

- Рекомендация 6. Европейская комиссия и компетентные органы государств — участников должны способствовать развитию механизмов сертификации средств безопасности для компонентов, продуктов и организационной безопасности.

- Рекомендация 7. Европейская комиссия и компетентные органы государств-участников должны поощрять создание испытательных площадок и методов оценки безопасности.

- Рекомендация 8. Европейская комиссия и государства — участники, в сотрудничестве с ENISA, должны продолжать изучение и проработку стратегий для координации мер по противодействию крупномасштабным панъевропейским киберинцидентам, затрагивающим силовые сети.

- Рекомендация 9. Компетентные органы государств-участников в сотрудничестве с группами CERT должны инициировать деятельность по привлечению групп CERT в качестве консультантов к решению вопросов кибербезопасности, затрагивающих силовые сети.

- Рекомендация 10. Европейская комиссия и компетентные органы государств-участников в сотрудничестве с научным и исследовательским сектором должны поощрять исследования в области кибербезопасности интеллектуальных сетей, максимизируя эффект от существующих исследовательских программ.

136 На основании работы ENISA: Smart Grid Security: Recommendations / Survey and Interview analysis (2012)

4.3 Внедрение системы управления безопасностью на основе оценки рисков

Системы управления информационной безопасностью представляют собой основу для реализации любых концепций безопасности ИКТ. Они обеспечивают наличие процессов, политик и организационных структур, необходимых для постоянного контроля над мерами кибербезопасности.
Хотя выбор применимых или сертифицируемых стандартов может зависеть от территориальных соображений (Северная Америка или страны Европы), перечень актуальных стандартов – ISO 27001/2, NISTIR 7638, NERC CIP и IEC 62433 — свидетельствует о едином (и совместимом) общем подходе: система безопасности, основанная на управлении рисками, в которой определяются риски, применимые к базовым активам ИКТ (NERC CIP даже включает предварительный шаг – выявление важнейших киберактивов).

Наиболее широко используемый для сертификации стандарт ISMS, ISO 27001 (более 7940 сертификаций по всему миру[137]) уже совместим или был приведен в состояние совместимости со всеми подходами и будет принят в качестве основы всеобъемлющих ISMS.

Единый подход в специализированных стандартах (IEC 62433, NERC CIP) заключается в том, что все они используются для определения базового уровня безопасности или минимальный комплекс мер, которые будут применяться независимо от оценки риска. Эта концепция очень схожа с подходом, лежащим в основе немецкой системы каталогов IT-Grundschutz[138], и предназначена для получения соизмеримых результатов вместо разрозненных результатов, к которым иногда приводит использование подхода, основанного только на управлении рисками, такого как ISO 27001, Она также может упростить внедрение стандартов путем снижения первоначальных расходов на выявление рисков.

4.4 Включение систем IACS/ SCADA в системы управления информационной безопасностью

Безопасность систем промышленной автоматизации и регулирования (IACS) редко учитывается при создании систем управления информационной безопасностью. Сложности возникают в связи с тем, что информационная безопасность исторически развивалась в различных направлениях, и, несмотря на то, что сами по себе эти процессы совместимы, многие термины и определения различаются или даже являются несовместимыми.

Единый подход указанных выше стандартов состоит во включении IACS в структуру управления безопасностью на основе риска. На Рис. 11 показано, как в стандарте IEC 62433 эти задачи решаются в приложении к различным заинтересованным сторонам (владелец актива, системный интегратор, поставщик компонентов). При этом необходимо решать следующие важные задачи:

- **Урегулирование концептуальных различий целей безопасности**

  Несмотря на то что термин «промышленная безопасность» часто используется как синоним понятия «техника безопасности», в действительности под ним понимается обеспечение конфиденциальности, целостности и доступностью. Для того чтобы действовать на общих основаниях, необходимо совместно определить цели безопасности.

  - Основное значение для IACS имеют (в порядке убывания) целостность, доступность и конфиденциальность.
  - Их необходимо учитывать в совокупности с их воздействием на охрану труда, технику безопасности и окружающую среду.[139]
  - Также необходимо принимать во внимание возникающие в этой связи известные концепции IACS, такие как уровень полноты безопасности (УПБ).
  - Кроме того, требуется рассматривать воздействие мер по обеспечению безопасности на функционирование рабочих процессов и производственную мощность.
  - Изменить подход к управлению рисками
  - В стандарте IEC 62443 используется подход к управлению рисками, который совместим со стандартом ISO 27005, но несколько видоизменен с

137 По состоянию на август 2012 г., URL: http://www.iso27001certificates.com/ (02/13/2013)

138 Каталоги IT-Grundschutz, Федеральное управление по информационной безопасности Германии (BSI)

139 Как в случае с недовольным сотрудником, который выпустил большие объемы сточных вод в Австралии в 2001 году. См. Marshall Abrams, Joe Weiss: „Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia“, http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf. Загружено 2013-03-22.

целью обеспечить многоэтапность процесса оценки риска, который начинается на верхнем уровне организации и постепенно спускается вглубь.

- **Изменение стратегии оценки уязвимых сторон**

  В традиционных подходах к безопасности ИКТ для выявления уязвимых мест часто используется проверка на защиту от несанкционированного доступа в сочетании с аудитом конфигурации. Стандартная проверка на защиту от несанкционированного доступа системы ИКТ может иметь потенциально разрушительные последствия для безопасности IACS и способна серьезно нарушить ее работу. Процесс проверки на защиту от несанкционированного доступа должен быть адаптирован для промышленной среды, а при самом тестировании необходимо применять меры предосторожности для предотвращения возможного физического воздействия сбоев, вызванных тестированием.

- **Введение мер управления внесением исправлений в IACS (отдельно от внесения исправлений в ИКТ)**

  Управление внесением исправлений является самой важной задачей при обеспечении безопасности IACS. Для обеспечения безопасности ИКТ применяется политика частой публикации исправлений для защиты новых уязвимых мест и отражения атак, в которых эксплуатируются эти уязвимые места.

При неожиданной реакции системы установка исправлений в среде IACS способна привести к нарушениям в работе системы или нанесению ей долгосрочного ущерба. Это создает дополнительную нагрузку, связанную с выявлением необходимых исправлений и их последующим тестированием. Тестирование сторонними специалистами не может гарантировать отсутствие влияния изменений на рабочие процессы — это можно сделать только путем проведения проверки в реальной среде.

При управлении внесением исправлений в IACS необходимо учитывать следующее:

- Некоторые устройства могут не входить в сферу внесения исправлений (например, в связи с тем, что поставщик вообще не предлагает исправлений).
- Тестирование определенных ситуаций может оказаться невозможным за пределами производственной среды (а в некоторых случаях — невозможным и в рамках производственной среды в связи с соображениями доступности или безопасности).
- Некоторые уязвимые места невозможно исправить — это приводит к необходимости введения дополнительных мер для снижения воздействия.

В связи с этим рекомендуется разработать отдельный процесс управления внесением изменений — отдельный от существующих процессов внесения изменений в ИКТ.

- **Усиление внешней безопасности**

  Полное физическое и логическое разделение сетей ИКТ во многих случаях недостижимо или нежелательно. Для успешной защиты периметра необходимо учитывать следующее:

- Физическая изоляция не обеспечивает полную безопасность. Некоторые виды вредоносных программ преодолевали физическую изоляцию через USB-подключение (W32.SillyFDC, W32/Agent.BTZ, W32.Downadup, и W32.Stuxnet).[140]

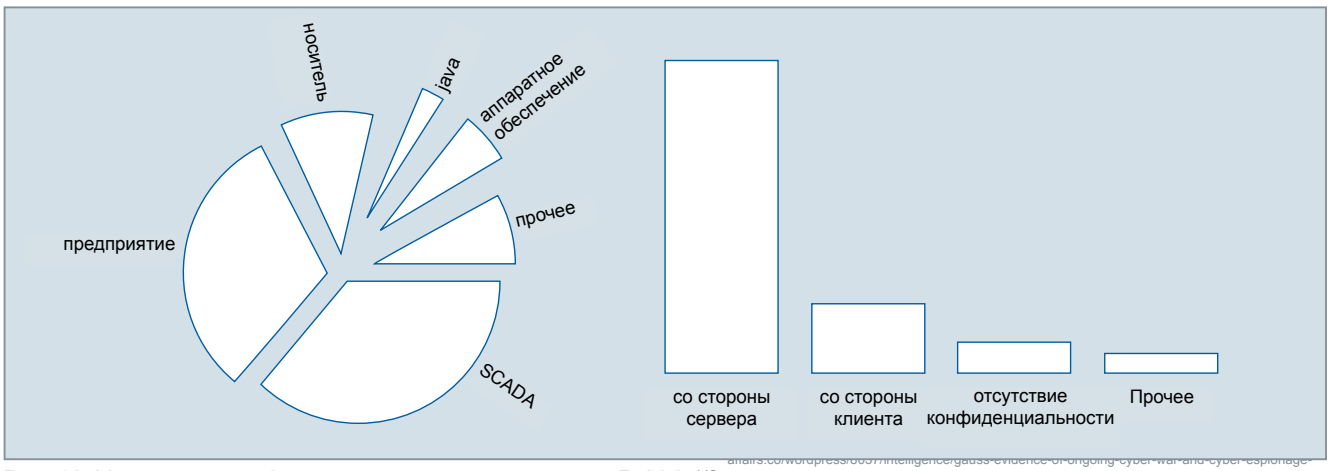


Рис. 12: Уязвимости, информация о которых продается ReVuln[146] affairs.co/wordpress/6057/intelligence/gauss-evidence-of-ongoing-cyber-war-and-cyber-espionage-campaigns.html. Загружено 21.03.2013.

- Многие известные атаки нацелены на IACS через внедрение в корпоративную сеть. Первичным вектором атаки часто бывает электронная почта,[141] затем используются системы ERP и MES или рабочие компьютеры разработчиков, а оттуда осуществляется переход в производственную сеть.

Таким образом, надежный контроль внешней ситуации имеет первостепенное значение. В его основе лежат следующие меры:

- Строгое разделение сети на производственные сети и сеть предприятия.[142]
- Разделение достигается путем применения отдельных ДМЗ и сетей периметра.
- Функциональная интеграция осуществляется через контролируемые шлюзы, которые заменяют информационный поток. За шлюзами необходимо вести тщательный мониторинг.

- **Управление возможностью подключения и реализация сотовой концепции (создание зон и каналов)**

Эта концепция расширена стандартом ISO 62443 до создания тонких ячеек или зон. В соответствии со стандартом IEC 62433, зоны «основаны на функциональности, местоположении, ответственной организации и на результатах оценки риска высокого уровня. Группировка этих активов отражает общие требования к безопасности для каждой зоны и канала». Такая зона может включать группу контроллеров процесса (КП), действующих в рамках единого процесса, в то время как система управления производством (СУП) использует собственную зону. Канал представляет собой связь между двумя (или более) зонами. Он может быть таким простым как межсетевой защитный экран, но может также включать собственную полную ДМЗ вместе со шлюзом приложений или может быть просто USB-носителем для переноса данных.

Кампания	Количество	Страны
strong	668	Все 68 взломанных каналов находились во Вьетнаме
ejun0708	63	5 в России, 3 в Украине и по 2 в Чешской Республике, в Казахстане, Швейцарии, Таджикистане и Беларуси
ejun0614	42	27 в России, 3 в Китае, 3 в Кыргызстане, 2 в Таджикистане и по 1 в Великобритании, США, Южной Корее, Чешской Республике, Германии и Казахстане
strongNewDns	34	Все 34 взломанных канала находились во Вьетнаме
ejun0509	32	31 в России, 1 в Украине
ejun0511	29	21 в России, 4 в Украине, 2 в Казахстане и по 1 в Чешской Республике и Азербайджане
7–28	28	24 во Вьетнаме и по 1 в ОАЭ, Камбодже, Таиланде и Китае
ejun0503	25	23 в России и по 1 в Украине и Чешской Республике
0dayaug12.exe	22	20 в Беларуси и 2 в Казахстане
C:\\WINDOWS\system32\desp.exe	22	12 в США, 5 в России, 3 в Нидерландах и по 1 в Швейцарии и Европейском Союзе

Рис. 13: Отчет о масштабе воздействия Lurid – пример вирусной кампании[150]

141 См., например, серию атак «Ночной дракон», которая началась в 2009 году: "Global Energy Cyberattacks: 'Night Dragon'". McAfee Foundstone Professional Services and McAfee Labs. 10 февраля 2011 г. http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf. Загружено 22.03.2013. Или более позднюю работу: "DHS: Gas pipeline industry under significant ongoing cyberattack. ICS-CERT takes unusual step of issuing public warning to raise awareness". Эллен Мессмер, Network World, 8 мая 2012 г., http://www.networkworld.com/news/2012/050812-pipeline-cyberattack-259069.html. Загружено 22.03.2013.

142 В 2012 году катарская газовая компания RasGas была вынуждена изолировать свою сеть, отключив ее от Интернета, чтобы предотвратить дальнейшее повреждение внутренней инфраструктуры в результате вирусной атаки: „RasGas: new cyber attack against an energy company". By Paganini, Security Affairs, 31 августа 2012 г. http://securityaffairs.co/wordpress/8332/malware/rasgas-new-cyber-attack-against-an-energy-company.html. Загружено 22.03.2013.

Рис. 14: Европейские национальные/государственные группы по реагированию на чрезвычайные и кризисные ситуации (ENISA)

Затем для каждой зоны устанавливаются общие цели безопасности и целевой уровень безопасности. Уровень безопасности представляет собой способ качественного выражения безопасности, необходимой в данной зоне. Уровни безопасности (и фактические последствия) должен определять владелец актива.[143]

4.5 Повышение осведомленности

При рассмотрении вопроса осведомленности о безопасности заметны сохраняющиеся противоречия между фактическим потенциалом угрозы целевых атак и тем, как они воспринимаются. В основном это объясняется тем, что информация о многих атаках, осуществляемых в области поставки и производства энергии, не раскрывается, поскольку операторы установок, на работу которых повлияли атаки, не хотят, чтобы об этих инцидентах стало известно.[144] При таком подходе возникает ситуация (инциденты воспринимаются как изолированные события), которая усиливает эту тенденцию сохранения инцидентов в тайне. В некоторых странах представителей отрасли просят, стимулируют, а иногда и обязывают сообщать о таких инцидентах.

Атаки на промышленные системы управления стали столь важной темой в хакерском сообществе с 2010 года, что на соответствующих конференциях этому вопросу уделяется повышенное внимание (например, направление Blackhat SCADA и ICS). С тех пор интерес к этой теме только вырос, как показывают следующие примеры:

- В сентябре 2012 года компания ReVuln.com продала информацию об уязвимых местах 9 систем ICS, не

143 В проекте стандарта IEC 62443 пока даются только общие уровни безопасности, такие как «высокий», «средний» и «низкий».

144 Причина может заключаться в том, что компании боятся нанести ущерб своей деловой репутации. Другая причина может быть связана с предотвращением распространения конфиденциальной информации, поскольку оно может привести к возникновению новых уязвимых мест.

сообщив о них производителю. ReVuln — это новая компания, которая также продает информацию об уязвимых местах компаний тем, кто планирует на них атаки.

- Уже существуют специальные поисковые системы (ERIPP, SHODAN) для выявления систем SCADA, подключенных к Интернету. Большинство систем, которые можно найти таким образом, очевидно, подключены к Интернету ненамеренно.[145]

На основании результатов анализа инцидентов необходимо предпринимать действия для повышения осведомленности об изменении ситуации с рисками среди тех людей, которые отвечают за данную область, особенно в сфере IACS. Это можно сделать следующим образом:

- Путем обмена информацией о реальных инцидентах в своем сегменте отрасли[147].

- Путем разработки (и внедрения) программ повышения осведомленности о проблемах безопасности в IACS и в области важнейших объектов неядерной энергетической инфраструктуры.

4.6 Обмен информацией

Обмен информацией между государствами, организациями и компаниями не только способствует общей осведомленности о вопросах безопасности, но и является основным способом осознания диапазона существующих угроза.[148]

В большинстве случаев целевые атаки не происходят без предупреждения. Можно предположить, что террористические акты на важнейших объектах инфраструктуры не будут ограничены одним объектом. Аналогичная тенденция просматривается и в области «классического» промышленного шпионажа: кибератаки в этой области проводятся в виде кампаний.

Компания TrendMicro подготовила один из первых подробных отчетов о кампании такого рода в процессе анализа распространения вредоносного программного обеспечения особой формы известной как “Lurid”.[149]

Эта атака была нацелена на известные дипломатические организации, а также на ведомства, связанные с космическими и исследовательскими учреждениями. На Рис. 13 приведены примеры крупнейших кампаний, в которых использовались уникальные вредоносные программы. В целом была выявлена 301 подкампания, затронувшая 2 272 систем.

Исследование кампании «Красный октябрь», направленной против дипломатических организаций, Лабораторией Касперского показало очень похожий результат.[151] Целевые группы были слишком мелкими для того, чтобы их можно было быстро обнаружить или организовать ответную реакцию по всему сектору. Быстрый обмен информацией в рамках сектора может обеспечить решающее преимущество.

Базовые методы также необходимо тестировать на реальных объектах. Это могут быть вторичные объекты, необязательно являющиеся частью важнейшей инфраструктуры. В идеале атаки должны быть выявлены уже на этом этапе. Для того этого требуется быстрый обмен большими объемами информации, а это означает, что предметом такого обмена станет потенциально конфиденциальная информация и информация, связанная с инцидентами, в том числе:

- Информация о кибератаках во время их осуществления

- Информация о выявленных уязвимых местах и об атакованных компонентах

- Информация о путях доступа

- Обмен информацией в настоящее время начинается с национальных групп по реагированию на чрезвычайные и кризисные ситуации. Большинство европейских стран уже создало группы по реагированию на чрезвычайные и кризисные ситуации,[152] и ENISA пытается установить единый стандарт для национальных групп по реагированию на чрезвычайные и кризисные ситуации.[153]

➥ Рис. 14: Европейские национальные/государственные группы по реагированию на чрезвычайные и кризисные ситуации (ENISA)[154]

145 ICS-ALERT-12-046-01—INCREASING THREAT TO INDUSTRIAL CONTROL SYSTEMS http://ics-cert.us-cert.gov/pdf/ICS-ALERT-12-046-01.pdf (02/14/2013)

146 ReVuln, URL: http://revuln.com/ (02/13/2013)

147 Атаки «Ночного дракона», указанные выше, были нацелены на многие международные нефтяные, энергетические и нефтехимические компании. Там же.

148 См. Главу 5.3.

149 TrendMicro, URL: http://www.trendmicro.es/media/misc/lurid-downloader-enfal-report-en.pdf (02/14/2013)

150 TrendMicro, URL: http://www.trendmicro.es/media/misc/lurid-downloader-enfal-report-en.pdf (02/14/2013)

151 Securelist, URL: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation (02/14/2013)

152 Securelist, URL: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation (02/14/2013)

153 Deployment of Baseline Capabilities of National/Governmental CERTs, URL: http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012 (02/14/2013)

154 Использование базовых способностей национальных/государственных групп по реагированию на чрезвычайные и кризисные ситуации, URL: http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012 (02/14/2013)

Обмен информацией такого рода дает очевидные преимущества, если осуществляется в рамках однородных групп (энергетическая промышленность, важнейшие объекты инфраструктуры). Например, коллеги и заинтересованные стороны могут совместно работать над разработкой индикаторов для выявления возможных нарушителей и атак, совместимых образцов передовой практики и целевых контрмер. Тем не менее, для обмена информацией такого рода существуют препятствия. Отдельная проблема — трансграничное общение. В условиях обмена информацией на встречах государственных представителей и экспертов временные задержки представляются слишком длинными. Прямой обмен данными об инцидентах между национальными группами по реагированию на чрезвычайные и кризисные ситуации в этой области пока ведется недостаточно четко, и здесь остаются возможности для прогресса. Эта тема более подробно рассматривается в Главе 5.3.

4.7 Мониторинг безопасности и управление инцидентами

Надлежащий мониторинг ситуации и управление инцидентами, связанными с нарушением безопасности, требуют дополнительных мер, которые выходят за рамки простого выявления таких инцидентов и реагирования на них. Следует рассмотреть дальнейшие шаги, в том числе, помимо прочего, включение кибератак в планы действий по ликвидации последствий чрезвычайной ситуации, пересмотр регулирования и учет тенденций ИКТ.

4.7.1 Выявление случаев нарушения безопасности

Никакие меры безопасности в мире не могут полностью исключить риск атаки со стороны убежденного киберпреступника. В системах, построенных на базе программного обеспечения, всегда есть ошибки, и некоторые из них приводят к появлению уязвимых сторон. Таким образом, вероятность того, что нарушитель найдет пригодную для эксплуатация уязвимость в отдельной системе зависит только от того, на сколько времени ему удалось получить доступ к этой системе. Иными словами, со временем в любой системе будет появляться пригодная для эксплуатация уязвимость. После того как злоумышленник получит доступ к системе, ему также потребуется время, чтобы нанести ущерб.

Если нападающий будет выявлен до того, как он успел нанести ущерб, и вы сумеете своевременно отреагировать, ущерба удастся избежать. Проще говоря, если время реагирования меньше, чем время, необходимое атакующему для нанесения ущерба, то система находятся в безопасности. В безопасности ИКТ эта концепция известна под названием «временная безопасность».[155] Эта взаимосвязь актуальна для всех видов кибератак, особенно в случае нападения на важнейшие объекты инфраструктуры и в секторе энергетики, где ущерб может быть более ощутимым.[156]

Прежде всего она свидетельствует о первостепенном значении мониторинга — без средств выявления никакие меры безопасности, сколько бы они ни стоили, не могут гарантировать достаточный уровень безопасности. В прошлом мониторингом безопасности пренебрегали, особенно в контексте промышленных систем автоматизации и управления, где всегда был более важен мониторинг процесса и доступности.

Несмотря на то что мониторинг процесса и доступности сосредоточен на общем состоянии системы, мониторинг безопасности регистрирует события, которые могут помочь в выявлении нарушений безопасности, например:

- Неудачные и успешные входы в систему
- Попытки подключения к службам
- Аномальные показания датчиков
- Попытки коммуникации за пределами границ безопасности (например, коммуникация между разными ячейками)
- Ситуации ошибки, которые не привели к проблемам доступности или целостности

Многие организации уже применяют системы мониторинга безопасности под разными наименованиями, при этом самый распространенный термин – «информация о безопасности и управление событиями». Централизованные или полуцентрализованные системы используются для:

- Сбора и корреляции данных из разных источников
    - Помощи в выявлении атак или их попыток
    - Способствования определению аномалий путем использования самостоятельных систем датчиков
- Оповещения персонала в случаях, когда автоматизированный анализ совокупности событий

155 Впервые опубликовано в 1999 году как «Временная безопасность».

156 Также см. серьезную атаку вируса Shamoon на энергетическую компанию в Саудовской Аравии: „Saudi Aramco, are we ready for an escalation of cyber attacks?" . Paganini, Security Affairs, 21 августа 2012 г. http://securityaffairs.co/wordpress/8175/hacking/saudi-aramco-are-we-ready-for-an-escalation-of-cyber-attacks.html, Retrieved 2013-03-22.

свидетельствует о наличии аномалии или признаков нарушений безопасности

- Хранения защищенных от несанкционированных манипуляций протоколов пострадавших систем, которые могут быть использованы позднее при проведении судебной экспертизы

4.7.2 Реагирование на инциденты

После выявления инцидента на него требуется надлежащим образом отреагировать. Реагирование на инциденты предусмотрено всеми типичными стандартами информационной безопасности и направлено на:

- Выявление ведущейся атаки (нарушения безопасности)
- Сдерживание происходящего (отражение атаки или ликвидации эффекта от нее)
- Выявление глубинных уязвимостей (например, путем проведения аналитического расследования)
- Искоренение причин инцидента
- Передачу полученной информации (например, национальной группе быстрого реагирования на чрезвычайные и критические ситуации)

Процессы реагирования на инциденты смоделированы в положениях управления непрерывностью деятельности и в нескольких стандартах (особенно в стандарте ISO 22301 – Управление непрерывностью деятельности, ISO 62443, NISTIR 7628, и NERC CIP).

Участие межотраслевых экспертов или групп экспертов, способных анализировать проблемы в точке соприкосновения систем IACS и ИКТ, имеет исключительно важное значение для анализа инцидентов на важнейших объектах неядерной энергетической инфраструктуры. Обучение, проведение учений и наличие квалифицированного персонала являются важнейшими областями, определяющими успех реагирования на инциденты.

Поскольку такие эксперты немногочисленны, а небольшие организации могут оказаться не в состоянии иметь достаточное число квалифицированных специалистов, важно получить внешнюю помощь заранее. Хотя некоторые группы по реагированию на чрезвычайные и кризисные ситуации оказывают такие услуги, предприятиям сферы энергетики специализированная помощь пока не оказывается.[157] Например, этот пробел можно решить с помощью обучения инженеров ИТ/ИКТ и другого значимого персонала.

4.7.3 Учет кибератак при планировании ликвидации последствий

Планирование ликвидации последствий сбоев и повреждений очень развито в энергетическом секторе. Наличие соответствующих планов является обязательным для многих организаций. Планирование ликвидации последствий уже является типичным положением всех стандартов и включает следующие шаги:

- Создание планов действий по ликвидации последствий и подготовка их реализации
- Создание и поддержание резервных и дублирующих систем
- Проведение учений по планам действий по ликвидации последствий и тестирование восстановительных процедур

Эти шаги не меняются для целевых кибератак, однако для этих случаев необходимо добавить еще один важнейший элемент: Когда сбой в работе происходит в результате идущей кибератаки, стандартные сценарии восстановления могут привести к тому, что такая же атака повторится снова, пока не будут устранены лежащие в ее основе причины.

Анализ первопричин был включен в стандарт ISO 22301 (Управление непрерывностью деятельности)[158] только в 2012 году. В стандарте NERC CIP-009-5 он только косвенно упоминается в положении, в котором речь идет о сохранении данных в целях обеспечения возможности анализа причины событий, вызвавших восстановительные работы.

4.7.4 Пересмотр регулирующих мер

Практика контроля индивидуальных систем и процессов и их мониторинга в рамках отдельной территории или компании оказалась слишком ограниченной в свете возрастающей сложности инфраструктуры и увеличения числа участников. Становится все труднее связать происходящие

157 Согласно данным ENISA, группы по реагированию на чрезвычайные и кризисные ситуации в секторе энергетики отсутствуют.

158 Согласно данным ENISA, группы по реагированию на чрезвычайные и кризисные ситуации в секторе энергетики отсутствуют.

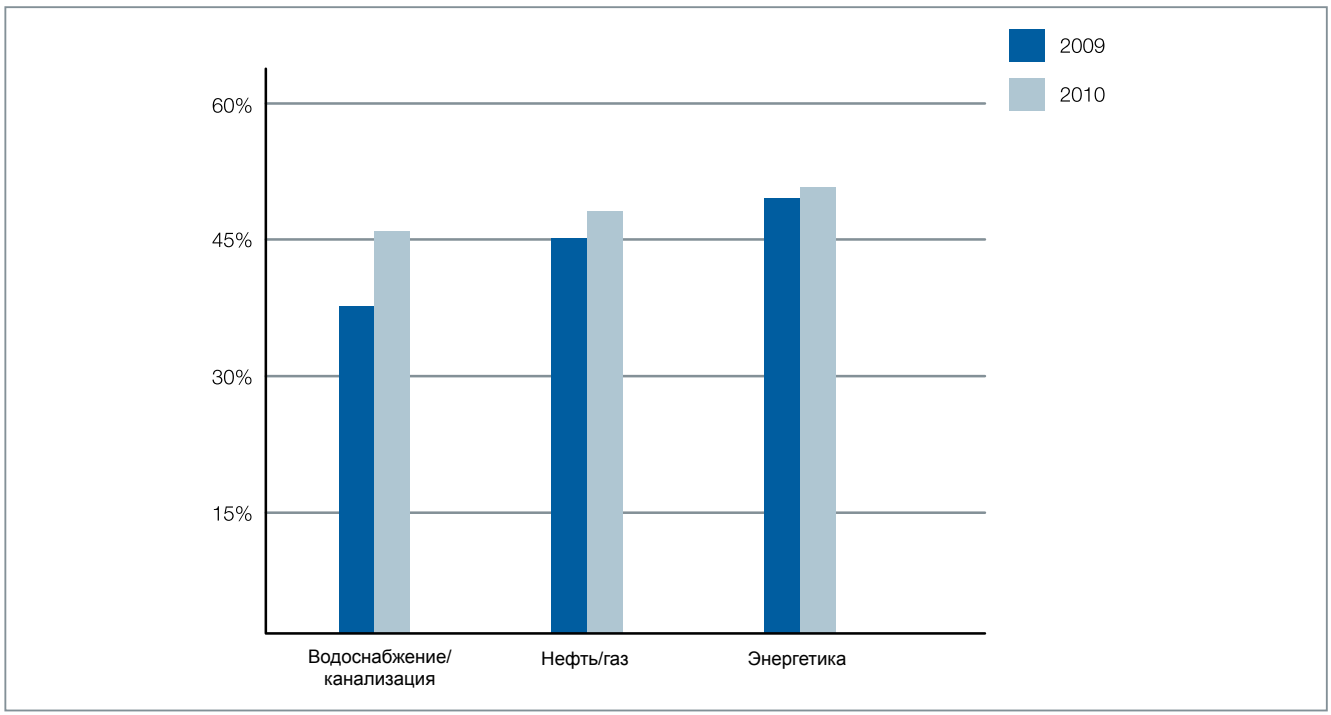


Рис. 15: График усовершенствований: темпы внедрения мер безопасности[163]

сбои с базовыми проблемами, в особенности это касается инфраструктуры интеллектуальной сети.

Сквозной контроль всего пути передачи от производителя до потребителя позволяет выявить и связать ошибки и их причины с учетом разных систем. Это — единственный метод, позволяющий выявить определенные виды атак, при которых использовалось манипулирование (например, саботаж).

Однако обмен этими данными, особенно на международном уровне, сразу приводит к возникновению юридических вопросов, касающихся конфиденциальности и защиты данных. Здесь требуется пересмотреть сложные международные положения, включая однозначные нормы, определяющие требования, актуальные для энергетической отрасли. Это особенно желательно для политически чувствительной темы неприкосновенности частной жизни конечного потребителя.[159]

4.8 Рассмотрение тенденций в сфере ИКТ

В настоящее время для обеспечения большей эффективности управления глобальным потреблением энергии электрические сети трансформируются в цифровую инфраструктуру. На данный момент это считается наилучшим способом решения многих сложных задач будущего. При этом в результате цифровизации сети появляются новые риски, с которыми необходимо бороться с помощью новых надлежащих мер безопасности. Так, меры безопасности, предусмотренные, например, в интеллектуальных счетчиков, совершенствуют их, делая их более эффективными и гарантируя большую бесперебойность работы.[160] Ненадлежащие меры безопасности в энергетическом секторе могут иметь прямые последствия для других секторов и могут даже создать угрозу для безопасности населения.

Интеллектуальный счетчик

Интеллектуальный счетчик представляет собой счетчик энергии (например, для электричества или газа), который отображает показатели реального потребления энергии и фактическое время ее использования конечным потребителем. Европейская система интеллектуального учета утверждает, что счетчики можно отнести к категории интеллектуальных только если они контролируются как минимум одним микропроцессором. В зависимости от модели интеллектуальные счетчики автоматически передают данные поставщику энергии. Эта процедура и сопутствующие процессы, системные решения и услуги в совокупности именуются «системой интеллектуального учета».

159 См. Главу 5.4.

160 IBM: End-to-End security for smart grids (2011)

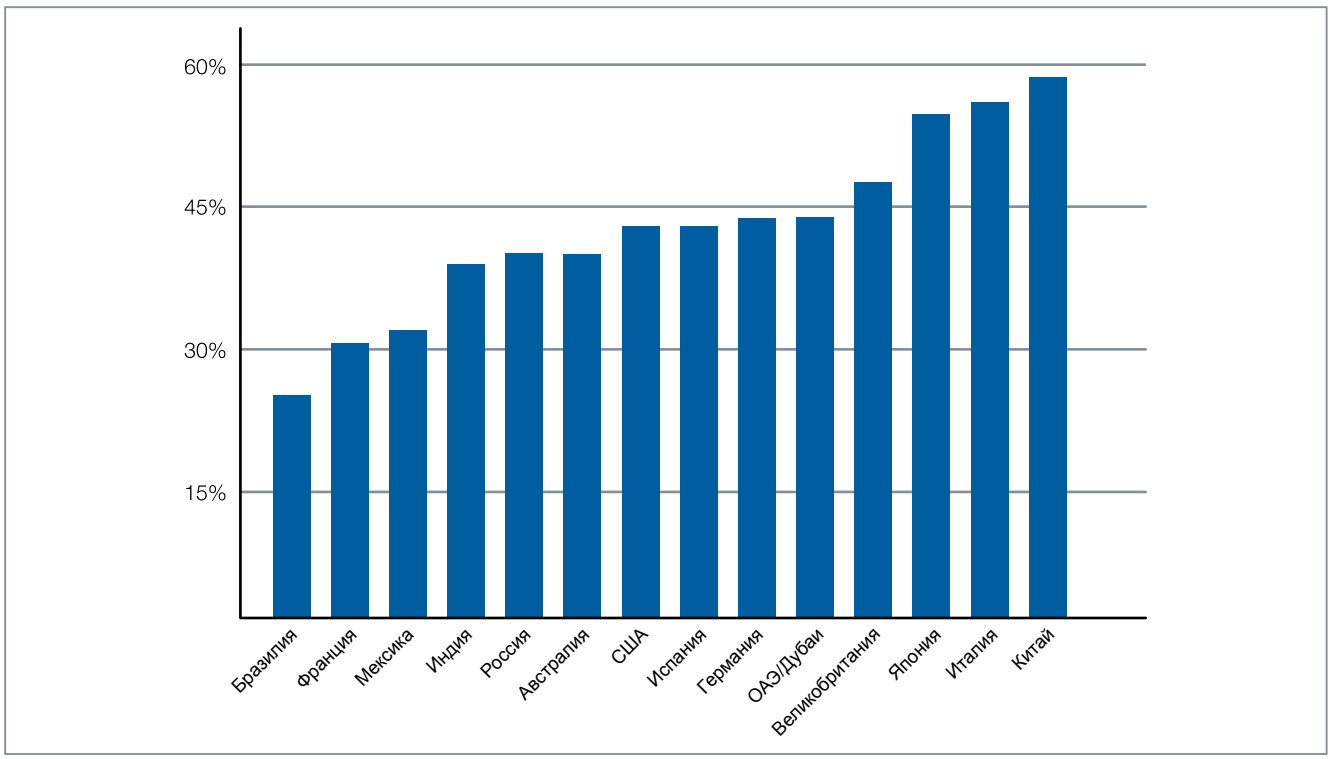


Рис. 16: Учтенные темпы внедрения мер безопасности по странам

Был достигнут прогресс во внедрении мер безопасности во всех важнейших инфраструктурных секторах. Эти меры включают технологии безопасности, политику безопасности, шифрование, аутентификацию и возможности подключения к сети. Однако применение новых мер безопасности к новым угрозам и уязвимым местам пока идет достаточно медленно.[161] В рамках исследования, проведеннаого компанией McAfee в 2011 году, 200 руководителей важнейших объектов инфраструктуры должны были указать, какие меры безопасности используются в их компаниях. Для простоты сравнения ответов участников опроса попросили выбрать меры, использовавшиеся в их компаниях, из перечня возможных мер безопасности:[162]

- Сопровождение программного обеспечения и исправление уязвимостей
- Стандартизованная конфигурация компьютеров
- Передача информации партнерам по отрасли/государству
- Мониторинг угроз
- Запрет на использование USB-устройств или других съемных носителей или ограничение их использования
- Обязательная аутентификация в информационной системе с использованием разделенных секретов маркеров или приборов биометрической идентификации
- Обязательная аутентификация за пределами информационной системы с использованием разделенных секретов маркеров или приборов биометрической идентификации
- Сетевые фильтры при доступе в сети общего пользования
- Меры управления доступом в сеть
- Особые меры контроля безопасности и доступа к базам данных
- Система предотвращения проникновений (IPS)
- Система обнаружения проникновений (IDS)
- Сетевые фильтры между корпоративными системами
- Инструменты управления информационной безопасностью
- Инструменты предотвращения потери данных

161 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), стр 14

162 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), стр. 14

- Выявление аномалий в ролях и деятельности (системы обнаружение отклонений от нормального состояния)
- Вайтлистинг приложений
- Использование инструментов мониторинга сетевой активности
- Использование шифрования (при передаче данных по сети, хранении данных в сети, на жестких дисках ноутбуков, в базах данных, в электронной почте и на переносных устройствах)
- Регулирование использования мобильных устройств (установка антивирусных программ, перепрошивка, отсутствие привязки к сети)
- Мониторинг новых подключений к информационной сети с помощью инструментов аудита или анализа сетевого поведения

Сравнение между секторами водоснабжения/канализации, нефти/газа и энергетики показало, что компании энергетического сектора не так много сделали для развития мер безопасности в период с 2009 по 2010 год, но в целом сектор энергетики по-прежнему опережает два других сектора по уровню безопасности.

Лишь немногие компании внедрили передовые меры безопасности, такие как инструменты для мониторинга сетевой активности или выявления ролевых аномалий. [164] Тем временем, именно эти меры необходимы во всех секторах важнейшей инфраструктуры в свете нынешних угроз и уязвимых мест.

Сравнение стран показывает, что темпы внедрения мер безопасности в Китае составляют почти 60 процентов. За лидером следуют Италия и Япония.

➥ Рис. 16: Темпы внедрения мер безопасности по странам (в соответствии с показателями отчетности)[165]

4.9 Резюме и рекомендации

Несмотря на то что организационные меры безопасности уже достаточно подробно освещены в международных стандартах, необходимо продолжать их развитие в параллели с эволюцией угроз и уязвимых мест. При этом необходимо осознавать, что существующие стандарты информационной безопасности разрабатывались без учета потребностей важнейших объектов неядерной энергетической инфраструктуры, которая сталкивается с разнообразными угрозами, включая террористические атаки на киберсистемы важнейших объектов неядерной энергетической инфраструктуры. В результате каждая организация и оператор также должны найти собственный способ снижения рисков безопасности и адаптации общих стандартов к собственным особым требованиям. Стандарты внедрения мер технологической безопасности в области промышленной автоматизации и регулирования находятся на высокой стадии развития, однако сфера энергетики и другие важнейшие секторы инфраструктуры охвачены еще не в полной мере. В этой области требуется дополнительное развитие, а также более комплексный взгляд на физическую и кибербезопасность важнейших объектов инфраструктуры.
Необходимо анализировать риски с учетом особенностей практики обеспечения безопасности, которые можно найти в сферах ИКТ и промышленных систем контроля (ПСК). Специалисты в области безопасности ИКТ и ПСК должны сформулировать политики, направленные на снижение рисков и угроз, после чего эти политики должны быть одобрены менеджментом. В конечном итоге необходимо посвятить время и усилия развитию комплексного обучения кибербезопасности ИКТ/ПСК разработчиков и специалистов в сферах ИКТ, кибербезопасности и проектирования.

Технические меры безопасности, относящиеся к системам ИКТ, должны быть значительно усовершенствованы для противодействия текущим и будущим рискам безопасности интеллектуальных сетей.[166]

Ниже перечислены основные рекомендации для представителей отрасли, основанные на существующей передовой практике:

- Повышайте осведомленность и стройте культуру безопасности.
- Разрабатывайте программы обучения для инженеров и

163 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), стр 14

164 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), стр. 15

165 McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), стр 15

166 WP 2.2 Inclusion of effective security measures for smart grid security and resilience, European Commission (2012)

разработчиков, включая в них понимание аспектов кибербезопасности ИКТ и ПСК.

- Постройте систему управления безопасностью, основанную на оценке рисков.
  - Оценивайте и отслеживайте риски по мере их появления, учитывайте изменения в угрозах, уязвимостях и инфраструктуре.
  - Применяйте меры безопасности в целях снижения этих рисков.
  - Постоянно внедряйте усовершенствования.
- Делитесь информацией об уязвимых местах и инцидентах.
- Ведите мониторинг безопасности и управляйте последствиями экстренных ситуаций.
  Следует отметить, что постоянно и быстрыми темпами меняющейся системе кибербезопасности, а также стандартам в области энергетики/IACS, требуется столь же гибкая и способная к быстрой адаптации структура.
- Государственные органы и власти должны:
- Повышать осведомленность и строить культуру безопасности.
- Поддерживать обмен информацией об атаках, злоумышленниках и уязвимых местах важнейших объектов инфраструктуры в рамках государственно-частных партнерств для обмена информацией.
- Усовершенствовать нормативно-правовую базу в отношении:
  - Обязательного обмена информацией и соблюдения конфиденциальности
  - Обязательных стандартов кибербезопасности для важнейших объектов неядерной энергетической инфраструктуры и критической инфраструктуры
  - Способствовать принятию стандартов безопасности IACS
- Предоставить руководство в отношении применимых стандартов и нормативов.

Подробные рекомендации для государственных органов рассматриваются в следующей главе.

5. Передовая практика защиты важнейших объектов инфраструктуры в рамках ОБСЕ

ОБСЕ Организация по безопасности и сотрудничеству в Европе

5. Передовая практика защиты важнейших объектов инфраструктуры в рамках ОБСЕ

Энергетическая безопасность, определяемая как надежная, доступная и устойчивая поставка энергии[167], стала стратегической задачей для всех стран. Энергетическая безопасность невозможна без надежной и безопасной энергетической инфраструктуры. Однако, как ясно показано в предыдущих главах, сегодняшняя энергетическая инфраструктура по большому счету уязвима. Большинство рисков, связанных с энергетической инфраструктурой, носят универсальный характер, но их воздействие на разные важнейшие секторы инфраструктуры имеет свои особенности. Так, существует потребность в единой комплексной системе защиты важнейших объектов инфраструктуры, обеспечивающий основу для общих и конкретных действий по обеспечению безопасности компонентов инфраструктуры и критических процессов в различных важнейших инфраструктурных секторах. Ниже перечислены основные цели общей системы защиты важнейших объектов инфраструктуры:

- Объединение усилий соответствующих заинтересованных сторон из государственного и частного сектора.
- Достижение сотрудничества по вопросам координации, гармонизации и, возможно, интеграции совместных и индивидуальных целей, стратегий, процессов, структур, способностей и возможностей в разных сферах деятельности.
- Обеспечение безопасности и надежности важнейших объектов инфраструктуры и важнейших процессов.[168]

Большинство государств — участников ОБСЕ приняли общие системы обеспечения безопасности важнейших объектов инфраструктуры путем разработки государственных стратегий в отношении них. Многие страны также опубликовали государственные стратегии кибербезопасности, направленные на противодействие опасностям, исходящим из киберпространства (см. Главу 4.2). Эти стратегии создают общую структуру для сотрудничества между множеством различных заинтересованных сторон. Несмотря на то что конкретные нюансы структур и стратегий являются делом внутренней политики каждой страны, все же можно выделить несколько общих составных элементов. Создавая национальные системы защиты важнейших объектов инфраструктуры вокруг этих составных элементов, политики, а также владельцы и операторы объектов инфраструктуры в этих странах могут обеспечить достаточную унификацию для ведения совместных действий, в то же время обеспечивая достаточную свободу для реализации индивидуальных мероприятий в рамках каждого сектора важнейшей инфраструктуры. В остальной части настоящего Руководства, таким образом, будут рассмотрены шесть составных элементов:

- Партнерства;
- Анализ угроз и уязвимостей;
- Обмен информацией;
- Регулятивные стимулы и диалог между регулирующими органами;
- Управление непрерывностью деятельности; и
- Учения.

5.1 Партнерства

Сегодня существует широкий консенсус о важности сотрудничества при обеспечении безопасности важнейших объектов инфраструктуры . Как следствие, все чаще звучат призывы к созданию государственно-частных партнерств (ГЧП). ГЧП строятся на базовой предпосылке о том, что активное участие государственных и частных заинтересованных сторон

167 В 2006 году Европейская комиссия определила три основные задачи европейской энергетической политики: устойчивость, конкурентоспособность и безопасность поставок. См.: A European Strategy for Sustainable, Competitive and Secure Energy, COM(2006) 105 final, Brussels, March 8, 2006, стр. 17-18.

168 На основании: Heiko Borchert and Karina Forster, "Protecting Critical Energy Infrastructures: How to Advance Public-Private Security Cooperation", in Protecting Critical Energy Infrastructure from Terrorist Attack, OSCE CTN Newsletter Special Bulletin, January 2010, стр. 14-17, здесь стр. 14.

поможет разработать принципы защиты и безопасности, соответствующие выявленным рискам и необходимому уровню готовности. Кроме того, ГЧП обладают потенциалом, который позволяет им избегать регулирования в форме принятия законодательных актов, создавая таким образом стимулы для взаимодействия корпоративного сектора с государственным.

Однако потребность в защите важнейших объектов инфраструктуры с помощью таких партнерств выходит за пределы взаимодействия между государственным и частным сектором. Здесь также необходимо реализовать два дополнительных направления сотрудничества:

- Государственно-частные партнерства свидетельствуют о потребности в сотрудничестве между государственными органами. Широкое межведомственное взаимодействие необходимо для обеспечения безопасности важнейших объектов инфраструктуры, поскольку различные органы устанавливают нормы, правила и стандарты обеспечения безопасности в различных важнейших инфраструктурных секторах. В некоторых случаях государственные органы по-разному подходят к решению вопросов защиты важнейших объектов инфраструктуры. Некоторые из них являются сторонниками рыночного подхода, в то время как другие твердо верят в законодательную роль государства. Эти различия, могут стать серьезным препятствием на пути сотрудничества с привлечением частного сектора, и привести к нескольким последствиям, которые будут рассмотрены позже.

- Партнерства между частными организациями являются ответом корпоративного сектора на межорганизационное сотрудничество. Зависимости между важнейшими инфраструктурными секторами являются типичной и широко признанной характеристикой обеспечения безопасности важнейших секторов инфраструктуры. Это требует разработки совместных подходов по всей корпоративной цепи поставок внутри важнейших инфраструктурных секторов и между ними. Достичь этого совсем непросто, поскольку реализация таких совместных подходов означает, что конкурирующие компании должны сотрудничать, обмениваясь конфиденциальной информацией. Некоторые представители важнейших инфраструктурных секторов, ставшие первыми жертвами киберпреступников, уже признали преимущества сотрудничества внутри конкурентной среды. Другие еще только начинают понимать важность сотрудничества, так как были защищены от атак. В результате очень большое внимание должно быть направлено на определение соответствующих ролей и ожиданий в отношении государственно-частных партнерств.

Государственно-частное партнерство

Государственно-частные партнерства (ГЧП) представляют собой форму контрактного сотрудничества между государственными органами и частными организациями. ГЧП создаются для разделения обязанностей и сотрудничества между частными партнерами и государственными органами таким образом, что частная организация обеспечивает максимально эффективную деятельность, а государственные органы следят за тем, чтобы достигаемые цели соответствовали общественным интересам. Государственные органы надеются, что партнерство с частным сектором экономики снизит давление на государственный бюджет, поскольку частная компания должна предоставлять часть средств или все средства самостоятельно, а это означает, что она будет стремиться к обеспечению экономической эффективности проектов.

Например, Министерство национальной безопасности США признает значение построения эффективных государственно-частных партнерств в своем Государственном плане защиты инфраструктуры (ГПЗИ). Система партнерства ГПЗИ способствует координации и сотрудничеству между владельцами и операторами частного сектора и государственными органами на всех уровнях. Это достигается путем создания Советов по координации сектора (СКС), состоящих из представителей частной отрасли, и Государственных советов по координации (ГСК), состоящих из представителей государственных органов разных уровней. Функции СКС и ГСК включают комплексное планирование, разработку методологии, оценку рисков, внедрение программ защиты и стратегий поддержания устойчивости, управление инцидентами, профессиональную подготовку, проведение учений и выявление требований к научно-исследовательской работе.

Несмотря на то что данный подход к построению партнерств привел к положительным результатам для Министерства национальной безопасности США, универсальной модели для создания партнерств в сфере защиты важнейших объектов инфраструктуры на данный момент не существует. Опыт показывает, что каждая заинтересованная сторона преследует собственные конкретные интересы. При выявлении и сочетании их общих интересов можно создать взаимовыгодные условия для сотрудничества (Рис. 17). При этом имеет смысл рассмотреть следующие шаги:

- Шаг 1: Проанализировать и установить мотивацию каждого партнера, включение которого планируется в партнерство по защите важнейших объектов инфраструктуры. Это необходимо для выяснения взаимных ожиданий и вклада каждой стороны.

- Шаг 2: Установить амбиции и цели партнерства на основе общих национальных целей в сфере защиты важнейших объектов инфраструктуры; прояснить цель партнерства и задач, которые оно должно выполнить (также см. Шаг 5).

- Шаг 3: Проанализировать существующую нормативно-правовую базу, применимую к каждому важнейшему инфраструктурному сектору; выявить обязательные и самостоятельно установленные нормы, правила и принципы; оценить адекватность существующей нормативно-правовой базы в свете ожидаемых рисков и существующего уровня готовности; обсудить, как можно ликвидировать возможные пробелы.

- Шаг 4: Предоставить механизмы, защиту и правовую определенность для обмена информацией, относящейся к защите важнейших объектов инфраструктуры, между всеми задействованными заинтересованными сторонами (см. Раздел 5.3).[169] Предоставить механизмы для добровольных инициатив, включая развитие образцов передовой практики и обмен ими, а также для консультаций и диалога в целях обеспечения постоянных и эффективных партнерских отношений.

- Шаг 5: Создать институциональную структуру, поощряющую межорганизационное сотрудничество и обмен информацией; разъяснить роли и вклад каждого партнера (например, государственных органов, владельцев и операторов важнейших объектов инфраструктуры, поставщиков продукции, ассоциаций); выявить единые контактные точки для каждого партнера; установить рекомендации для сотрудничества.

- Шаг 6: Начать с малого, сосредоточившись на одном или двух важнейших инфраструктурных секторах; постепенно развиваться на фоне обеспечения готовности всех заинтересованных сторон к сотрудничеству, рассматривая уровней угрозы.[170]

- Шаг 7: Определить важнейшие этапы для анализа достижений и определения потенциальных следующих действий.

- Шаг 8: Предусмотреть постоянный процесс проверки для пересмотра и обновления отношений партнерства, чтобы обеспечить продолжающийся прогресс, соотносимый с общей средой риска и с мерами безопасности и защиты, которые требуются для обеспечения оптимального уровня защиты.

➥ Рис. 17: Характеристики государственно-частных партнерств в сфере кибербезопасности[171]

5.2 Анализ угроз и уязвимых сторон

Анализ угроз и уязвимых сторон является важнейшим инструментом для связи государственных и частных мер, направленных на обеспечение безопасности. Общая осведомленность о ситуации и общее понимание ситуации в отношении основных рисков и вероятных последствий разных важнейших инфраструктурных секторов имеют первостепенное значение. Если государственный и частный сектор не смогут прийти к согласию в этой точке, то их сотрудничество будет поставлено под угрозу. Поскольку большое значение имеет восприятие, совместный анализ угроз и уязвимых сторон по всем важнейшим инфраструктурным секторам является идеальным способом достижения взаимопонимания того, какие потребности необходимо удовлетворить, и почему и как это нужно сделать. В частности, совместный анализ угроз и уязвимых сторон повышает осведомленность о важнейших областях взаимозависимости между разными секторами, благодаря чему проливает свет на важнейший аспект национальной и корпоративной устойчивости к атакам.

Невозможно создать единую структуру для анализа рисков и уязвимых мест, которая соответствовала бы среде каждого государства—участника ОБСЕ. Между участниками существует слишком много различий, в частности, в отношении разделения полномочий и ответственности (например, централизованная или децентрализованная политическая система, федеральное разделение власти). Несмотря на эти различия, в сообществе ОБСЕ можно выделить несколько образцов передовой практики:

- Единый комплекс категорий риска: в Нидерландах и в Великобритании процесс разработки государственной

169 Лучший способ обеспечения правовой определенности в высокой степени зависит от существующей национальной нормативно-правовой базы. Помимо принятия законодательства, заинтересованные стороны также могут принять решение о рассмотрении самостоятельно установленных правил.

170 Как показывает опыт, работа с реальными угрозами является основным фактором, на котором строится сотрудничество.

171 Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models (Washington, DC: Intelligence and National Security Alliance, 2009), стр. 6

		Интересы	Возможности	Ограничения
Телекоммуникационные компании, поставщики программного и аппаратного обеспечения и поставщики интернет-услуг (ПИК)		Хотят поставлять услуги и защищать конфиденциальность клиентов Хотят быть надежными поставщиками: оптимальные результаты работы не менее, а может, и более важны, чем постоянный доступ Необходимо гарантировать, что регулирование не задушит развитие и не поставит их в менее выгодное положение с точки зрение экономической конкуренции	Имеют специалистов-техников, способных быстро находить аномальные операции Имеют возможности для блокирования атак «в нисходящем направлении» Имеют возможности для продажи программного обеспечения системы безопасности клиентам и для применения стандартов с помощью соглашений о подключении с абонентами	Не спешат слишком сильно погружаться в обмен информацией в отношении безопасности по соображениям конфиденциальности и ответственности Вероятно, не будут склонны повышать затраты на безопасность
Государство в роли регулирующего органа		Нуждаются в надежности и защите для обеспечения защиты важнейших объектов инфраструктуры Зависит от целостности и защиты интернет-операций для защиты конфиденциальности граждан и экономического благополучия страны	Могут сыграть необходимую роль в правоприменении в отношении кибербезопасности Также могут предоставить платформу для международных действий и обращений Могут предоставить стимулы, поощряющие более активное участие ГЧП в кибербезопасности	Сталкиваются с трудностями при координации реагирования нескольких крупных органов Имеют фрагментарные и распыленные полномочия Процессы классификации вызывают помехи в способности делиться информацией Обеспечение безопасности в некоторых случаях может противоречить соображениям конфиденциальности
Пользователи: Крупные корпорации, малый бизнес, физические лица, центры информационного обмена и анализа (ISAC), государственные и частные организации и научные центры	Физические лица	Нуждаются в доступности по требованию Им требуется более высокая степень защиты информации личного порядка и персональных компьютеров Подозрительно относятся к роли правительства в регулировании Интернет-сферы и требуют твердых правил и жесткого надзора за регулирующими органами	У них имеется большое количество аппаратных устройств, которые могут использоваться для добровольного сбора и распространения информации в отношении потенциальных или реальных атак	Часто подвергаются риску инцидентов, связанных с нарушением кибербезопасности Не подготовлены или не привыкли к тому, чтобы защищаться от атак
	Государство	Зависит от наличия Интернета, необходимого для предоставления государственных услуг, передачи информации, хранения больших объемов информации и получения доступа к ней и поддержки операций национальной безопасности	Обладает большими сетями, которые уже отслеживаются на предмет информации об угрозах и содержат полезный набор данных для анализа угроз	Медленно переходят к более новым и безопасным технологиям Не умеют хорошо координировать реагирование
	Компании (малый бизнес находится ближе к категории индивидуальных пользователей)	Нуждаются в доступности по требованию Всерьез интересуются надежностью сетей для ведения электронного бизнеса и защиты коммуникаций, а также для защиты фирменной и конфиденциальной информации Должны получить гарантии, что регулирование не окажет неблагоприятного воздействия на их бизнес и инновации	Часто создают изощренную структуру обеспечения безопасности или обращаются к поставщикам услуг по безопасности Делятся информацией через отраслевые объединения, организации по стандартам и системы связи с государством Участвуют в разработке стандартов	Применяют новые технологии и практики более медленно по мере увеличения размера организации Их участие в обмене информацией ограничено в связи с соображениями конфиденциальности и обязательств

Рис. 17: Характеристики государственно-частных партнерств в сфере кибербезопасности

стратегии безопасности является основой выявления рисков национальной безопасности. Эти риски также включают сценарии, применимые к конкретным объектам инфраструктуры. Единая система создается путем включения важнейших объектов инфраструктуры в общую национальную политику обеспечения безопасности. Обе эти страны определяют комплекс иллюстративных категорий риска на национальном уровне. Эти же категории используются как единая основа для анализа рисков на субнациональном уровне. Это гарантирует последовательность комплекса категорий риска, который может использоваться при определении характеристик риска на каждом уровне национальной политической системы.[172]

- Методическое руководство: Федеральное управление гражданской защиты Швейцарии, которое координирует деятельность правительства Швейцарии в области защиты важнейших объектов инфраструктуры, приложило серьезные усилия к определению надежных методов анализа рисков, связанных с важнейшими объектами инфраструктуры. Особенно стоит отметить следующие аспекты: Во-первых, благодаря программе Risiken Schweiz («Риски для Швейцарии») была создана единая платформа, которая используется для определения рисков национальной безопасности с помощью различных заинтересованных сторон. Во-вторых, Национальный каталог рисков включает общий обзор основных рисков, в котором делается различие между природными, техногенными и общественными категориями рисков. На основании этого каталога были разработаны идеальные сценарии рисков, которые дают дополнительную справочную информацию. Все соответствующие заинтересованные стороны могут использовать эти сценарии. В-третьих, национальные эксперты разработали инструментарий для оценки рисков национальной безопасности. Этот инструментарий состоит из четырех категорий последствий (например, воздействие на людей, окружающую среду, экономику и общество) и универсального определения разных шкал для оценки вероятности и возможности реализации сценария. Наконец, было также опубликовано руководство по определению важнейших элементов и объектов национальной инфраструктуры.[173] В рамках этой общей системы федеральные органы теперь взаимодействуют с властями кантонов для анализа рисков на субнациональном уровне.[174] Необходимо заметить, что все эти инициативы были разработаны с участием экспертов из частного сектора.

- Вопросы трансграничного взаимодействия: В глобальном мире цепи поставок проходят через разные страны, что ведет к необходимости межнационального сотрудничества по вопросам обеспечения безопасности важнейших объектов инфраструктуры. Канада и США, например, в 2010 году приняли двусторонний план действий для решения общих задач. В частности, в этом плане будут «определены конкретные действия по поддержке совместных инфраструктурных целей и повышению вовлеченности». При этом в Плане действий установлены три задачи: Построение партнерских отношений, направленных на повышение устойчивости инфраструктуры, усовершенствование обмена информацией и достижение управления рисками. С точки зрения анализа рисков План действий предусматривает создание «виртуальной канадско-американской группы по анализу рисков важнейших объектов инфраструктуры (…), которая будет вести совместный анализ инфраструктуры на основании информации о рисках, проводить оценку уязвимых мест и определять приоритетные методики, процессы и образцы передовой практики. Он также предусматривает разработку и подготовку совместных аналитических продуктов, которые могут применяться на трансграничном уровне».[175] План действий также подразумевает создание трансграничной региональной программы оценки устойчивости для оценки важнейших объектов инфраструктуры, поддерживающей анализ угроз и уязвимых сторон. Она предполагает рассмотрение всех угроз, уязвимых мест и последствий, связанных с важнейшими объектами инфраструктуры, представляющими взаимный интерес для США и Канады. Проведение оценок этих объектов инфраструктуры позволяет всем заинтересованным сторонам определить устойчивость, зависимость и взаимозависимость, а также каскадный эффект от потенциального сбоя или перерыва в работе важнейших объектов инфраструктуры. Сочетание группы по анализу виртуальных рисков и этой программы позволяет США и Канаде оценить угрозы и уязвимые места и в то же время представляет собой

172 Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models (Washington, DC: Intelligence and National Security Alliance, 2009), стр. 6.

173 Schweizerische Eidgenossenschaft, URL: http://www.infraprotection.ch (02/13/2013)

174 Schweizerische Eidgenossenschaft, URL: http://www.kataplan.ch (02/13/2013)

175 Canada-United States Action Plan for Critical Infrastructure (Washington, DC/Ottawa: Department of Homeland Security/Public Safety Canada, 2010), URL: http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf (02/13/2013)

инструмент для обмена информацией и образцами передовой практики.

5.3 Обмен информацией

Обмен информацией имеет ключевое значение в обеспечении безопасности важнейших объектов инфраструктуры. Бесперебойный, надежный и регулярный обмен информацией между всеми задействованными сторонами гарантирует общую осведомленность и общее понимание ситуации в любой момент времени. Обмен информацией делится на три категории которые должны быть включены в комплексный подход:

- Межгосударственный обмен информацией осуществляется путем передачи потоков информации между различными государственными органами на разных уровнях правительства и является обязательным условием для обеспечения единого государственного подхода к взаимодействию с частным сектором.

- Государственно-частный обмен информацией — это обмен информацией между государственными и частными заинтересованными сторонами. Он имеет огромное значение, поскольку в большинстве государств — участников ОБСЕ большей частью важнейших объектов инфраструктуры владеют и управляют частные компании.

- Обмен информацией внутри частного сектора необходим, поскольку цепи поставок затрагивают разные компании, работающие в разных инфраструктурных секторах и сегментах отрасли. Это иллюстрирует потребность в обмене информацией между частными компаниями одного или нескольких важнейших инфраструктурных секторов.

Для управления этими информационными потоками требуется разработка соответствующих принципов и структур с учетом особенностей различных важнейших секторов инфраструктуры и существующих нормативно-правовых систем. При этом необходимо ответить на четыре основных вопроса:[176]

- **Почему?** Обмен информацией — ежедневная задача, поэтому он должен быть интегрирован во все элементы стратегии защиты важнейших объектов инфраструктуры страны. В лучшем случае обмен информацией будет неотъемлемой частью следующих основных задач обеспечения безопасности важнейших объектов инфраструктуры.

  - Определение стратегии: создание национальной стратегии обеспечения безопасности важнейших объектов инфраструктуры требует широкого взаимодействия между государственным и частным сектором. Оно позволить наладить поток информации между обоими секторами, способствуя достижению взаимопонимания в отношении амбиций, целей, вкладов и ограничений всех заинтересованных сторон. При определении стратегии обмен информацией поможет составить общую картину происходящего при решении вопросов, имеющих решающее значение для национальной и корпоративной готовности и устойчивости.

  - Анализ угроз и уязвимых сторон: обмен информацией о рисках и уязвимых сторонах необходим, поскольку государственный и частный секторы зачастую по-разному смотрят на риски, угрозы и уязвимые места, а также стратегии, направленные на их снижение. При обмене информацией о риске огромную роль играет доверие, однако создание среды, в которой оно будет культивироваться — весьма сложная задача. Опыт различных государств — участников ОБСЕ показывает, что обмен информацией, касающейся риска, лучше всего осуществляется, когда этот процесс инициируют небольшие группы, к которым затем присоединяются другие участники, способные вывести дискуссию на новый уровень и предложить новые темы для обсуждения.

  - Выявление важнейших активов и определение целей защиты: Помимо важнейших национальных активов существуют активы, которые отличает высокая важность для корпоративных цепей поставок и отдельных компаний. Обмен информацией может помочь в повышении осведомленности сторон о важности этих компонентов. Уровень защиты, который считается необходимым для важнейших объектов национальной инфраструктуры, определяет то, какие меры защиты и безопасности необходимо предпринять. Несмотря на то что государства могут устанавливать необходимые цели по защите, они обычно не осуществляют оперативное управление самой инфраструктурой. Следовательно, обмен информацией необходим для

176 Canada-United States Action Plan for Critical Infrastructure (Washington, DC/Ottawa: Department of Homeland Security/Public Safety Canada, 2010), URL: http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf (02/13/2013) Final Report and Recommendations (Washington, DC: National Infrastructure Advisory Council, 2012); Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive (Washington, DC: Department of Homeland Security, 2012)

обеспечения соответствия целей по защите общей оценке рисков и уровню корпоративной готовности.

- Предотвращение кризисов, управление кризисами, восстановление после кризисов: обмен информацией является непременным условием работы по предотвращению инцидентов, связанных с важнейшими объектами инфраструктуры, или ликвидации их последствий. Без взаимного информирования об уровне готовности каждого партнера, точках соприкосновения, процедурах на случай чрезвычайной ситуации и возможностях по реагированию на чрезвычайную ситуацию планирование на случай реализации наихудших сценариев было бы невозможно. В экстренной ситуации, и в особенности при инцидентах в киберпространстве, возможность обмениваться информацией в режиме реального времени играет решающую роль. Этим обусловлены специализированные требования в сфере информационной безопасности, которые необходимо учитывать при разработке принципов и протоколов обмена информацией.

- Вспомогательная деятельность: существует много видов деятельности, которые могут поддерживать национальные инициативы в области защиты важнейших объектов инфраструктуры. Среди них основную роль играют научные исследования и разработки, а также стандартизация. И то, и другое напрямую влияет на способность корпоративного сектора принимать соответствующие меры безопасности для снижения рисков и ликвидации уязвимостей, связанных с важнейшими объектами инфраструктуры. Учет вспомогательной деятельности расширит программу защиты важнейших объектов инфраструктуры, позволяя рассматривать национальную готовность должным образом — в свете других политических целей, таких как национальное процветание и национальные инновации. Создание институциональной системы, позволяющей экспертам государственного и частного сектора постоянно находиться в диалоге по этим вопросам, приведет к тому, что деятельность в разных сферах будет связанной и последовательной, а в случаях, когда это необходимо — гармонизированной. Это позволит создать научную, технологическую и отраслевую основу национальной безопасности, которая будет готова поддерживать защиту важнейших объектов инфраструктуры.

- **Что?** То, какой информацией необходимо обмениваться, в высокой степени зависит от поставленной задачи и от задействованных в ее решении лиц. В целом информацию можно разделить на связанную с инцидентами и не связанную с инцидентами. Это разделение полезно, поскольку оно помогает установить следующее: (1) ожидается ли, что получатель такой информации предпримет немедленные действия; и есть ли необходимость в (2) обмене информацией в режиме реального времени; и (3) особых условиях информационной безопасности. Все три этих аспекта актуальны для

Информация государственного сектора	Информация частного сектора
• Знания о кибервозможностях ключевых террористических организаций • Информация о связях между разными террористическими и нетеррористическими группами • Знания о векторах прошлых атак • Знания о возможных векторах будущих атак, полученные из анализа киберпреступных подпольных веб-сайтов	• Информация о крупных категориях активов в энергетическом секторе (например, данные по газу, нефти, электроэнергии, возобновляемым источникам энергии; показатели надежности; информация о торговых операциях с энергией) • Информация о технических уязвимостях по определенным продуктам программного и аппаратного обеспечения, используемым операторами энергетической инфраструктуры • Анонимизированная информация о воздействии прошлых атак • Данные о потребностях по восстановлению, возникающих в результате разных форм атаки • Данные о схемах атаки в других важнейших секторах инфраструктуры, которые могут служить признаками раннего предупреждения для энергетического сектора

Таблица 9: Обмен информацией между государственным и частным сектором для снижения рисков террористических атак в киберпространстве на объекты энергетического сектора

информации, связанной с инцидентами, и, таким образом, способствуют разработке особых механизмов обмена информацией, основной целью которых является быстрое и бесперебойное взаимодействие между множеством разных заинтересованных лиц.

С другой стороны, информация, не связанная с инцидентами, может включать общие знания об угрозах, уязвимых сторонах, рисках, долгосрочных тенденциях развития в рамках важнейших инфраструктурных секторов и между ними, общую прогнозную информацию о безопасности, долгосрочные цели политики регулирования и образцы передовой практики. Такую информацию можно передавать более или менее свободно, не уделяя большого внимания срокам, что облегчает бремя, налагаемое особыми требованиями к обмену информацией.

Подготовка к защите от терроризма в киберпространстве, направленного на энергетический сектор, потребует крайне качественной и конкретной информации. Такие подробности выходят за пределы задач данного Руководства, однако общие соображения по этому поводу кратко представлены в Таблице 9.

- **Как?** Чтобы обеспечить беспрепятственную передачу информации между заинтересованными сторонами, занимающимися вопросами защиты важнейших объектов инфраструктуры в стране, необходимо установить основные правила и организационные принципы такой передачи. Некоторые государства — участники ОБСЕ уже создали специальные организации и/или инициативы для развития обмена информацией между государственным и частным сектором.

Кампания	Организация	Веб-сайт
Европейский Союз	Сеть предупредительной информации о важнейших объектах инфраструктуры	https://ciwin.europa.eu
Германия	Allianz für Cybersicherheit (Альянс по кибербезопасности)	https://www.allianz-fuer-cybersicherheit.de/
Швейцария:	MELANI (Центр отчетности и анализа по целостности и безопасности информации)	http://www.melani.admin.ch/
Испания	Национальный центр защиты важнейших объектов инфраструктуры	http://www.cnpic-es.es/en/index.html
Нидерланды	CPNI.NL	http://www.cpni.nl
Великобритания	Центр защиты национальной инфраструктуры	http://www.cpni.gov.uk
США	Среда распространения информации	http://www.ise.gov
	Национальный центр координации инфраструктуры	http://www.dhs.gov/national-infrastructure-coordinating-center
Прочее	Центр информационного обмена и анализа нескольких штатов	http://msisac.cisecurity.org
	Центр информационного обмена и анализа ИТ (IT-ISAC)	https://www.it-isac.org
	Центр информационного обмена и анализа сектора электроэнергетики (IT-ISAC)	http://www.esisac.com/

Таблица 10: Некоторые платформы обмена информацией, относящейся к CIP, в государствах-участниках ОБСЕ

- Институциональное оформление этих решений может быть разным и во многом зависит от национальных особенностей. Почти во всех случаях участники согласовали комплекс основных правил и принципов, которыми необходимо руководствоваться при обмене информацией. Основой этих правил и принципов является цветовое кодирование информации теми, кто желает ее опубликовать, т.е. поставщик информации определяет ее использование другими лицами. В большинстве случаев доступ к информации ограничивается государственными органами, участниками программ информационного обмена в определенном секторе, участниками программ информационного обмена в других важнейших инфраструктурных секторах и сочетанием всех трех категорий. Информация, имеющая отношение к обеспечению безопасности важнейших объектов инфраструктуры, является чувствительной. Так, существуют страны, в которых были приняты конкретные нормативные акты в отношении распространения информации, относящейся к защите важнейших объектов инфраструктуры, и не допускают несанкционированного доступа к такой информации. В частности, в Канаде были принят нормативно-правовой акт, дополняющий Закон о доступе к информации, в котором оговаривается, какая информация должна считаться конфиденциальной.[177]

  Нормативно-правовые акты, регулирующие информационный обмен также включают правила поведения, которые должны соблюдать отдельные эксперты, участвующие в передаче информации (например, при участии во встречах). Кроме того, существуют критерии отбора новых экспертов (например, согласие действующих экспертов на принятие нового члена, обязательная проверка биографических данных или личные встречи с представителями государственных органов, регулирующих процесс информационного обмена). В большинстве стран обмен информацией начинается с инициатив определенного сектора. По мере того как обмен информацией становится более полным и содержательным, он начинает использоваться для рассмотрения вопросов, затрагивающих несколько секторов. Например, вопросы информационной безопасности и безопасности SCADA важны для нескольких важнейших инфраструктурных секторов, в связи с чем обмен информацией, посвященный им, необходимо организовать на межсекторном уровне. Помимо личных встреч, обмен информацией возможен в электронной форме через онлайн-платформы.

- **С кем?** Выбор экспертов, участвующих в обмене информацией, возможно, является самой сложной задачей. Это вопрос не только количества, но и качества:
  - неоднократно обмен информацией начинался с малого, чтобы сохранить гибкость и выработать базовый уровень доверия. Общих правил в отношении максимального числа участников не существует, однако для создания атмосферы доверия важно сохранять стабильность состава группы, поддерживая очень низкую текучесть кадров.

  - При рассмотрении вопроса качественного состава группы следует опираться на международный опыт, который показывает, что уровень должностного положения участника в рамках представляемой организации важен для реализации действий, которые могут оказаться необходимыми в результате обмена информацией. Среди дополнительных факторов, имеющих значение для участников процесса обмена информацией, следует выделить опыт и знания. В некоторых странах участники процесса обмена информацией преднамеренно не допустили к участию в нем экспертов из определенных областей. Например, члены правоохранительного сообщества некоторых стран не участвуют в обмене информацией, поскольку разглашение определенных сведений потребовало бы от них совершения действий, которые могли бы отрицательно сказаться на готовности участников делиться какой-либо информацией в принципе. В то же время другие страны по крайней мере поддерживают связь с правоохранительным сообществом.

5.4 Регулятивные стимулы и диалог с регулирующими органами

Стимулы могут использоваться для оказания влияния на поведение объекта с целью добиться желаемого результата. Позитивные и негативные стимулы (например, санкции) являются частью нормативно-правовой базы во многих областях политики. За последние несколько лет во многих государствах-участниках ОБСЕ применялись регулятивные стимулы, направленные на поощрение использования возобновляемых источников энергии. До настоящего времени стимулы редко использовались для поощрения поведения, связанного с безопасностью и защитой.

177 "Identifying and Marking Critical Infrastructure Information Shared in Confidence with the Government of Canada", URL: https://www.publicsafety.gc.ca/prg/ns/ci/lbl-snstv-info-eng.aspx (02/12/2013)

Учитывая то, насколько неохотно положительные стимулы применяются в области безопасности, количество случаев, которые можно было бы считать образцами передовой практики, крайне ограничено. Одним из этих немногих примеров является доклад сэра Майкла Питта 2007 года, в котором анализировались уроки, извлеченные из наводнения, произошедшего в Великобритании летом того же года. В своем докладе Питт предположил, что за стремление к экономической эффективности, возможно, пришлось заплатить устойчивостью к воздействию таких маловероятных, но имеющих серьезные последствия событий, как наводнения. По мнению Питта, «регулирующим органам следует дать однозначное указание всегда принимать в учет устойчивость». Рассматривая и одобряя планы операторов важнейших объектов инфраструктуры, связанные с поддержанием устойчивости, и затем утверждая капитальные и операционные расходы, необходимые для реализации этих планов, экономические регулирующие органы могли бы создавать компаниям положительные стимулы для инвестирования средств в поддержание устойчивости.[178]

Предложение Питта относилось к тем отраслям, в которых цены утверждаются экономическими регулирующими органами. В других отраслях положительные рыночные стимулы включают налоговые льготы, изменения в оценке компаний и изменения в законодательстве об ответственности. Например, американский сенатор Либерман предложил, освобождать владельцев и операторов инфраструктуры ИКТ от гражданской ответственности, связанной с киберинцидентами, если они соблюдали определенные условия, например, обеспечивали полное соответствие мерам безопасности для получения сертификацию третьей стороны.[179]

Отрицательные стимулы (например, санкции), имеют большее распространение, и в том числе чаще используются в целях, связанных с безопасностью и защитой. Например, в Германии, Федеральное агентство по рынкам электроэнергии, газа, телекоммуникаций, почты и железных дорог (Bundesnetzagentur) может налагать на операторов телекоммуникационных сетей, которые нарушают закон Германии о телекоммуникациях, санкции (напр., обложение штрафов или введение надзора) [180]

Необходимо помнить, что стимулы действуют только в том случае, если поставленные цели достижимы. Таким образом, возникает необходимость в мониторинге соответствия со стороны заинтересованного лица. Германия и Франция требуют от операторов энергетической инфраструктуры представления концепций защиты и безопасности, в которых должны учитываться вопросы информационной безопасности. Внедрение этих требований проверяется соответствующими государственными надзорными органами.[181] Это обеспечивает механизм мониторинга. Государствам, заинтересованным в предоставлении регулятивных стимулов для защиты важнейших объектов инфраструктуры, имеет смысл наладить между заинтересованными лицами государственного и частного сектора диалог, ориентированный на выполнение законодательных требований.

- Со своей стороны, государству необходимо обеспечить участие в диалоге всех органов, ответственных за регулирование безопасности важнейших объектов инфраструктуры. В большинстве случаев эти органы сотрудничают с министерствами энергетики, транспорта, инфраструктуры, здравоохранения и экономики. Как правило, создание общей системы для соответствующих важнейших секторов инфраструктуры поручается именно этим министерствам. Министерства внутренних дел (или те министерства, которым поручена защита важнейших объектов инфраструктуры), с другой стороны, не всегда своевременно адаптируются к изменениям в сфере регулирования безопасности важнейших объектов инфраструктуры. Таким образом, существует первичная потребность в налаживании диалога с государственными регулирующими органами, направленного на достижение баланса в сложном взаимодействии между вертикальным, касающимся определенных секторов, регулированием, установленным в прошлом, и горизонтальным регулированием, в котором учитываются широкие принципы защиты важнейших объектов инфраструктуры. Это особенно справедливо для регулирования в области информационной безопасности, которое затрагивает все важнейшие инфраструктурные секторы.

- Также необходим диалог на тему регулирования между государственным и частным сектором. Во многих государствах — участниках ОБСЕ технические стандарты и национальное законодательство для важнейших секторов инфраструктуры идут рука об

178 Learning lessons from the 2007 floods. The Pitt Review (London: Cabinet Office, 2008), para 16.1-16.46, URL: http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/flooding_review/flood_report_web.pdf (03/12/2013), http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/flooding_review/flood_report_web.pdf (03/12/2013))

179 SEC. 105(e), стр. 2105, Cyber Security Act of 2012, (03/12/2013). Закон Либермана о кибербезопасности не был принят Конгрессом США

180 Telekommunikationsgesetz (TKG) §115, June 22, 2004, URL: http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf (03/12/2013)

181 Telekommunikationsgesetz (TKG) §109; Instruction générale interministérielle relative à la sécurité des activités d'importance vitale, no. 6600/SGCN/PSE/PPS of September 26, 2008, p. 26–31, URL: http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_1338.pdf (03/12/2013)

руку. Большинство законов не оговаривают напрямую цели безопасности и защиты, а, скорее, ссылаются на стандарты и руководящие принципы, обеспечивая необходимую гибкость и свободу политических решений в условиях, когда новые изменения могут требоваться по мере изменения стандартов. Несмотря на то что общие положения соответствующих законов остаются неизменными, допускается принятие и внедрение базовых стандартов и руководящих принципов. Однако по мере роста технологических сложностей и дальнейшего повышения взаимосвязи между важнейшими объектами инфраструктуры возникает потребность в диалоге о нормах, стандартах и руководящих принципах среди представителей различных секторов. Такой диалог должен помочь определить, приведут или изменения в одном секторе к необходимости предпринимать действия в других важнейших инфраструктурных секторах, и должен в этом отношении служить информационной базой для диалога между государственным и частным сектором по вопросам регулирования.

5.5 Управление непрерывностью деятельности

Обеспечение безопасности важнейших объектов инфраструктуры (CIP) и управление непрерывностью деятельности (BCM) — две стороны одной и той же медали. CIP рассматривает готовность и устойчивость с национальной точки зрения, в то же время концентрируясь на общей готовности страны справиться с инцидентами, способными иметь дестабилизирующие последствия. BCM используется для оценки тех же показателей с корпоративной точки зрения, уделяя особое внимание созданию процессов и ресурсов, необходимых для достижения коммерческих целей. Учитывая взаимодополняемость CIP и BCM, некоторые государства — участники ОБСЕ рассматривают возможность объединения двух этих направлений. Прекрасным образцом в этом отношении является Швейцария.

Под руководством Федерального управления сырьевого обеспечения национальной экономики (FONES) было проведено несколько исследований по анализу рисков для разных инфраструктурных секторов. В 2011 году была обновлена основная часть анализа недавнего риска по ИКТ в энергетическом секторе. Этот анализ содержит общее описание структуры сектора и его основных процессов, определение и оценку шести основных рисков, а также предложения по снижению этих рисков. В составе шести основных рисков рассматривается сбой в работе системы управления первичной сети, важнейших элементов и полное отключение центра обработки и передачи данных Swissgrid[182]. К исследованию сектора были привлечены швейцарские электроэнергетические компании энергосистемы общего назначения и VSE, ведущее объединение компаний энергетического сектора.

На основании этого анализа и при поддержке FONES, VSE и швейцарская энергосистема начали работать над руководством по непрерывности деятельности в сфере ИКТ всего энергетического сектора,[183] которое было опубликовано в 2011 году. Это руководство использует предыдущий анализ рисков и содержит общие рекомендации по минимальным стандартам управления непрерывностью деятельности в энергетическом секторе наряду с особыми рекомендациями по внедрению. Эти рекомендации сосредоточены на пяти важнейших компонентах инфраструктуры: система управления сетью, важнейшие элементы системы управления сетью, центр хранения и обработки данных, телекоммуникации и системы контроля и связи.[184] В настоящее время новые руководящие принципы по управлению непрерывностью деятельности ИКТ в энергетическом секторе являются добровольными, а не обязательными. Ассоциация VSE уже начала проводить учебные курсы по реализации этих руководящих принципов на практике, поэтому можно ожидать, что в будущем они повлияют на деятельность операторов.

Тесное взаимодействие между FONES, VSE и швейцарской энергосистемой было ключом к согласованию новых руководящих принципов по управлению непрерывностью деятельности ИКТ. Сотрудничество между этими заинтересованными сторонами и Управлением по гражданской защите Швейцарии также сыграло важную роль в гармонизации различных методов, использовавшихся этими двумя ведущими органами. В результате новая государственная стратегия Швейцарии по обеспечению безопасности важнейших объектов инфраструктуры обеспечивает основу системы, в которую можно встроить BCM.[185]

5.6 Учения

Проведение регулярных учений и проверок позволяет персоналу персонал сохранять уверенность и точность действий в сложных ситуациях, повышая их и общую уверенность в своих силах. Учения и

182 Swissgrid является владельцем и оператором швейцарской сети электропередачи.

183 Руководящие принципы охватывают национальную сеть электропередачи и межрегиональные распределительные сети, а также соответствующие уровни трансформации. Региональные и местные распределительные сети в нее не включаются.

184 Непрерывность деятельности ИКТ. Handlungsempfehlungen zur Sicherstellung der Versorgung (Aarau: Verband Schweizerischer Elektrizitätsunternehmen, 2011), URL: http://www.strom.ch/uploads/media/VSE_ICT-Continuity_12-2011_D_01.pdf (03/12/2013)

185 Nationale Strategie zum Schutz kritischer Infrastrukturen, (2012), URL: http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski.parsysrelated1.82246.downloadList.57269.DownloadFile.tmp/strategieski2012d.pdf (02/12/2013)

проверки также помогают выявить новые уязвимости, поскольку в кризисных ситуациях люди обычно находятся под воздействием стресса и реагируют поспешно и не задумываясь, а, главное, действуют неправильно и иррационально.[186]

ENISA,[187] НАТО[188] и отдельные государства — участники ОБСЕ[189] регулярно проводят учения по кибербезопасности. В зависимости от цели учений, отдельные операторы важнейших объектов инфраструктуры могут принимать в них участие, чтобы усовершенствовать свои системы управления чрезвычайными и кризисными ситуациями. Такие учения, в свою очередь, дают возможность не только провести совместную тренировку, но и обсудить образцы передовой практики и получить информацию для принятия решений.

Учения такого масштаба[190] требуют нескольких месяцев или даже лет подготовки, в связи с чем их требуется планировать на долгосрочную перспективу. Это является проблемой для операторов важнейших объектов инфраструктуры, поскольку они обычно не готовят столь подробные долгосрочные планы. Решение может заключаться в подготовке плана учений, охватывающего несколько лет, учитывающего результаты собственных проверок и результаты учений операторов, а также национальных и международных учений. Для государственных органов это означало бы, что их планирование должно быть обязательным с точки зрения сроков и содержания. Изменения в графике, содержании или целях учений, происходящие в последнюю минуту, могут привести к тому, что некоторые или все операторы важнейших объектов инфраструктуры не смогут принять в них участие. Чтобы охватить как можно более широкий спектр учений без предъявления слишком большого числа требований к участникам, рекомендуется применять ступенчатую программу учений. Это может означать, что в первый год проведения учений один важнейший инфраструктурный сектор проводит учения с государством. В последующие годы происходит ротация секторов, а каждые 5 или 10 лет все секторы проводят учения с государством в виде группы. Если участники используют систему ключевых показателей деятельности (КПД) для учений, то можно отследить улучшение или ухудшение в системе управления кризисами. В силу разнообразия участников и сценариев эти КПД должны быть как можно более общими, например, измерение сроков реагирования.

После учений всегда необходимо проводить подробную оценку, подробно рассматривая все успехи и недостатки. Не следует обходить вниманием неудачи, поскольку в противном случае участников может успокоить ложное ощущение безопасности, и они будут считать, например, что полностью готовы к отражению атаки. Такое впечатление, вводящее в заблуждение, может иметь отрицательные последствия для всей важнейшей инфраструктуры и страны, если атака на важнейшие объекты инфраструктуры или на другие сферы действительно произойдет, а согласованные методы и процессы не сработают.

5.7 Резюме и рекомендации

При защите важнейших объектов инфраструктуры необходимо решать массу различных сложных задач. Несмотря на то, что положения о безопасности и защите важнейших объектов инфраструктуры и процессов не являются всеобъемлющими, они были установлены задолго до того, как обеспечение безопасности важнейших объектов инфраструктуры было выделено в отдельную область государственной политики. Во-вторых, ландшафт риска постоянно меняется. Чтобы стандарты, концепции и меры безопасности и защиты успевали реагировать на эти изменения, они должны быть динамичными. В-третьих, риски, которым подвергаются важнейшие объекты инфраструктуры страны, могут выйти далеко за пределы государственных границ, в связи с чем при защите важнейших объектов инфраструктуры делается особый акцент на международное сотрудничество. Наконец, бремя защиты важнейших объектов инфраструктуры практически в полной мере ложится на плечи частного сектора, который владеет и управляет большинством важнейших объектов инфраструктуры во всем мире. Таким образом, возникает серьезная потребность в тесном взаимодействии между государственным и частным сектором, а также в доверии, основанном на четко определенных ролях и обязанностях.

Чтобы справиться со всеми этими сложными задачами, необходимы комплексные системы защиты важнейших объектов инфраструктуры. Такие системы необходимо адаптировать в соответствии с конкретными особенностями каждой страны и каждого важнейшего сектора инфраструктуры. Гибкость структуры имеет ключевое значение, но при этом она не должна приводить к фрагментации подходов к защите важнейших объектов инфраструктуры, поскольку всеми признается ценность совместимых мер, основанных на оценке риска, особенно в таком важном и глобальном секторе, как энергетика. Вместо этого существует потребность в концептуальных составных элементах, позволяющих одновременно осуществлять совместные действия в

186 BSI-Standard 100-4, p. 83ff

187 Учения под названием «Кибер Европа». Cf. URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe (02/13/2013)

188 Учения под названием «Кибер коалиция» и «Кибер Атлантик»

189 Например, LÜKEX в Федеральной Республике Германии, cf. URL: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Sonstiges/Infos_ueber_Luekex.html (02/13/2013)

190 С точки зрения количества участников и сложности материала

рамках сотрудничества и в то же время приобретать дополнительную гибкость действий. В настоящей главе рассматриваются шесть составных элементов:

- Для установки и развития защиты важнейших объектов инфраструктуры необходимы полноценные партнерства. Такие партнерства следует создавать по трем направлениям: Межгосударственные (государственные-государственные) партнерства для достижения межведомственного взаимодействия в государственном секторе; государственно-частные партнерства, способствующие сотрудничеству между министерствами, государственными органами и частными владельцами и операторами важнейших объектов энергетической инфраструктуры; и частно-частные партнерства для стимулирования корпоративного взаимодействия по всем цепям поставок внутри важнейших инфраструктурных секторов и между ними. Универсального метода для создания таких партнерств не существует, однако можно рассмотреть некоторые предложения: (1) выяснить взаимные ожидания и вклад каждой стороны путем анализа и определения мотивации партнеров; (2) установить амбиции и цели партнерства в области CIP; (3) проанализировать существующую нормативно-правовую базу; (4) обеспечить правовую определенность для обмена информацией, относящейся к CIP; (5) обеспечить институциональную структуру сотрудничества; (6) начать с малого; (7) определить важнейшие этапы для анализа; и (8) регулярно пересматривать и обновлять отношения партнерства, чтобы обеспечить постоянный прогресс.

- Анализ рисков и уязвимостей важен для достижения общей осведомленности и общего понимания рисков и уязвимых сторон, относящихся к защите важнейших объектов инфраструктуры. Передовая практика построения соответствующих процессов включает:

    - определение единого комплекса категорий и сценариев риска, которые могут использоваться на всех уровнях системы выработки политических решений и в каждом секторе;

    - методическое руководство, в особенности точное в отношении важнейших показателей, с тем чтобы избежать получения результатов оценки, которые невозможно сравнивать, поскольку они не были гармонизированы с самого начала;

    - специальные подходы к межнациональному анализу рисков, такие как общие процессы для обмена информацией и совместная оценка рисков.

- Общая ситуационная осведомленность и общее понимание ситуации невозможны без бесперебойного информационного потока между задействованными сторонами внутри государственных органов, между государственным и частным сектором и внутри частных секторов. Планирование обмена информацией для поддержания защиты важнейших объектов инфраструктуры требует, чтобы заинтересованные лица в государственном и частном секторе определили, какой информацией и почему они будут обмениваться, какого рода информация требуется для решения соответствующих задач, как будет осуществляться передача и защита информации, и кто будет участвовать в обмене информацией. Помимо прочего, образцы передовой практики обмена информацией показывают, что:

    - обмен информацией следует начинать с малого и развивать постепенно, чтобы сохранить гибкость и добиться доверия;

    - для обмена информацией и распределения индивидуальной ответственности при обращении с переданной информацией необходимо установить четкие правила;

    - личные встречи могут быть дополнены электронными платформами обмена информацией;

    - то, какая задача должна быть выполнена, во многом определяется требованиями к информационной безопасности, при этом информация, относящаяся к инцидентам, принципиально отличается от информации, не относящейся к инцидентам.

- Ответственность за защиту важнейших объектов инфраструктуры преимущественно лежит на частном секторе. Государственный сектор может поощрять инвестиции в безопасность и защиту важнейших объектов инфраструктуры с помощью целевых стимулов. Рыночные стимулы включают, помимо прочего, налоговые льготы, изменения в оценке компаний, учитывающие индивидуальную степень готовности, и освобождение от гражданской ответственности. Другие важные стимулы включают то, что государство будет делиться информацией об угрозах. Образцы передовой практики также показывают, что широкое вовлечение сторон особенно необходимо при рассмотрении вопросов регулирования для выявления и анализа воздействия норм защиты и безопасности, стандартов и принципов на важнейшие инфраструктурные секторы;

- Основываясь на идее стимулирования корпоративной деятельности по обеспечению защиты и безопасности, государства частично должны обеспечивать защиты важнейших объектов инфраструктуры путем применения модели Управления непрерывностью деятельности (BCM). Модель BCM стала стандартной практикой для многих компаний. Приводя государственные системы CIP в соответствие с основными принципами BCM, государства признают деятельность корпораций по обеспечению готовности. Образцы передовой практики также показывают, что модель BCM можно использовать для управления непрерывностью деятельности в сфере ИКТ важнейших объектов инфраструктуры, что в то же время позволяет добиться общенациональной и корпоративной устойчивости. Иногда государства пользуются этим приемом в своих национальных программах обеспечения готовности.

- Учения являются прекрасным способом оценить сильные и слабые стороны на определенный момент. Благодаря совместным тренировкам заинтересованные стороны из государственного и частного сектора получают ценную информацию о возможностях и ограничениях другой стороны. Проводить учения, которые приносят реальную пользу, достаточно сложно. В связи с этим необходимо тщательно планировать то, какие цели должны быть достигнуты, какие важнейшие инфраструктурные секторы будут задействованы, и какие риски / векторы атаки будут проанализированы. Заключительным этапом каждых учений должна быть точная оценка и подробный анализ всех действий.

6. Предложения по будущей роли ОБСЕ в повышении кибербезопасности важнейших объектов неядерной энергетической инфраструктуры

ОБСЕ Организация по безопасности и сотрудничеству в Европе

6. Предложения по будущей роли ОБСЕ в повышении кибербезопасности важнейших объектов неядерной энергетической инфраструктуры

На основании решения Совета министров 6/07 от 30 ноября 2007 года, государства — участники ОБСЕ обсудили роль этой организации в обеспечении защиты важнейших объектов неядерной энергетической инфраструктуры. В результате нескольких конференций и семинаров стало понятно, что ОБСЕ может сыграть важную и дополняющую роль по поддержке и укреплению национальной деятельности в области защиты важнейших объектов инфраструктуры и программ, применимых к их защите, в других международных организациях. На основании этих результатов[191] вклад ОБСЕ в решение вопросов кибербезопасности важнейших объектов неядерной энергетической инфраструктуры (и, возможно, вопросов, выходящих за эти пределы) можно разделить на три широкие категории:

Мобилизация политической поддержки

- ОБСЕ могла бы повысить осведомленность об угрозе террористических актов в киберпространстве, направленных на важнейшие объекты энергетической инфраструктуры и других важнейших инфраструктурных секторов, и о вероятных последствиях таких злонамеренных действий.

- Государства-участники могли бы изучить вопрос о применении положений, относящихся к защите важнейших объектов энергетической инфраструктуры от террористических актов, при реализации других мер, связанных с кибербезопасностью или безопасностью ИКТ, и осуществляемых ОБСЕ, в случаях, когда это возможно и целесообразно.

Развитие сотрудничества

- ОБСЕ должна поощрять многосторонний обмен информацией о методах оценки затрат на киберриски и о преимуществах обеспечения кибербезопасности на примере энергетического сектора.

- ОБСЕ могла бы стать центром для распространения спектра инициатив по распространению информации (например, расширение спектра деятельности ENISA в Центральную Азию через ОБСЕ).

- ОБСЕ могла бы продвигать и облегчать формирование межгосударственных, государственно-частных и частно-частных партнерств в области защиты важнейших объектов инфраструктуры путем организации семинаров по представлению образцов передовой практики, распространения информации и составления руководств и инструкций по передовой практике.

191 Например, см. Report of the Secretary General on Opportunities for Co-operation between the OSCE and Relevant International Organizations in the Field of Protection of Critical Energy Infrastructure from Terrorist Attacks, SEC.GAL/202/08, 30 October 2008; Executive Report on the OCEEA-ATU Expert Meeting on Protection Critical Energy Infrastructure from Terrorist Attack, SEC.GAL/153/08, August 29, 2008; Executive Report on the Public-Private Expert Workshop on Non-Nuclear Critical Energy Infrastructure from Terrorist Attacks, Vienna, February 11-12, 2010

Расширение национальных возможностей

- С помощью организации семинаров по представлению образцов передовой практики и распространения информации ОБСЕ могла бы продвигать развитие способностей для выполнения важнейших задач кибербезопасности, например:
    - Выявление – обнаружение: Выявление злонамеренных действий в киберпространстве, определение зависимостей в отношении будущих векторов атак и анализ атак в других важнейших инфраструктурных секторах в свете возможных уроков, которые могут быть извлечены владельцами и операторами объектов энергетической инфраструктуры.
    - Защита и реагирование – разработка: Разработка методов и концепций для обеспечения безопасности ИКТ по всем важнейшим инфраструктурным секторам и обмена опытом организации управления кризисами, связанными с инцидентами, в рамках важнейших инфраструктурных секторов и между ними.
    - Снижение рисков – подготовка: Подготовка планов непрерывной деятельности в сфере ИКТ для энергетического сектора и прочих важнейших инфраструктурных секторов, связанных с энергетикой.
- ОБСЕ могла бы способствовать наращиванию институционального потенциала для обеспечения кибербезопасности в энергетическом секторе на основе поддержки национального межведомственного сотрудничества и координации и поддержки создания структур, механизмов и протоколов для обмена информацией, относящейся к кибербезопасности.
- Несмотря на то что многие страны ведут обмен информацией самостоятельно, ОБСЕ могла бы стимулировать трансграничный обмен информацией о планировании действий и имеющихся возможностях на случай чрезвычайной ситуации в связи с киберинцидентами в энергетическом секторе и в других важнейших инфраструктурных секторах, связанных с энергетикой.
- ОБСЕ могла бы способствовать повышению компьютерной грамотности основного персонала, работающего на важнейших объектах инфраструктуры и в государственных органах надзора над важнейшей инфраструктурой.
- ОБСЕ могла бы стать организатором проведения учений по кибербезопасности в сотрудничестве с другими международными организациями, имеющими более ограниченное членство или другое географическое распределение (например, ENISA).

7. Дополнительная литература

8. Глоссарий

9. Сокращения

ОБСЕ Организация по безопасности и сотрудничеству в Европе

7. Дополнительная литература

1. Speake, Graham: Applying ISA/IEC 62443 to Control Systems, Manufacturing Enterprise Solutions Association, MESA (2012 г.), URL: http://www.yca-yokogawa-usersgroup.com/uploads/3/1/8/5/3185440/mesatutorial_-_isa99_security.pdf

2. Booz & Company по поручению Европейской комиссии Исследование: Stock-Taking of existing Critical Infrastructure Protection Activities (2009 г.), URL: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/2009_CIP%20stock_taking.pdf

3. Borchert, Heiko and Karina Forster: Protecting Critical Energy Infrastructures: How to Advance Public-Private Security Cooperation, in Protecting Critical Energy Infrastructure from Terrorist Attack, OSCE CTN Newsletter Special Bulletin (2010), pp. 14-17. URL: http://www.osce.org/atu/41367.

4. Bundesamt für Sicherheit in der Informationstechnik, Dr. Harald Niggemann: Cyber-Sicherheit – Bedrohungslage und Maßnahmen, URL: http://prisma-zentrum.com/download/120904%20Innovation%20B_Vortrag_Folien%20Referent.pdf

5. Bundesministerium des Inneren: Schutz kritischer Infrastrukturen – Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden (2008), URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf;jsessionid=D97DF90DA95A17955BF369CFED0FF9EE.2_cid287?__blob=publicationFile

6. Bundesrepublik Deutschland: Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz), 24.02.2012, URL: http://www.gesetze-im-internet.de/atg/

7. Bundesrepublik Deutschland: Telekommunikationsgesetz (TKG), 22.06.2004, URL: http://www.gesetze-im-internet.de/tkg_2004/

8. Cabinet Office: Learning lessons from the 2007 floods. The Pitt Review (2008), URL: http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/flooding_review/flood_report_web.pdf

9. Canada-United States Action Plan for Critical Infrastructure (Washington, DC/Ottawa: Department of Homeland Security/Public Safety Canada, 2010), URL: http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf

10. Commission of the European Communities: On a European Programme for Critical Infrastructure Protection (2005), URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF

11. Computerworld: Shamoon malware attacks, URL: http://www.computerworld.com/s/article/9230547/Kill_timer_found_in_Shamoon_malware_suggests_possible_connection_to_Saudi_Aramco_attack

12. CSO-Online: Cyberattacks on natural gas pipeline companies, URL: http://blogs.csoonline.com/critical-infrastructure/2165/ics-cert-alert-natural-gas-pipelines-under-attack

13. European Commission: A European Strategy for Sustainable, Competitive and Secure Energy (2006), URL: http://europa.eu/documents/comm/green_papers/pdf/com2006_105_en.pdf

14. European Commission: Critical Energy Infrastructure Protection (2008), URL: http://ec.europa.eu/energy/infrastructure/critical_en.htm

15. European Commission: Cyber security in the Digital Agenda (2012), URL: http://ec.europa.eu/digital-agenda/en/cybersecurity

16. European Commission: European Programme for Critical Infrastructure Protection (2006), URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

17. European Commission: Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM (2013) 48 final (02/07/2013), URL: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

18. European Commission: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (2009), URL: http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_risk_governance_report.pdf

19. European Commission: Study: Stock-Taking of Existing Critical Infrastructure Protection Activities (2009), URL: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/2009_CIP%20stock_taking.pdf

20. European Commission: Work Package 2.2 – Inclusion of effective security measures for smart grid security and resilience (2012), URL: http://ec.europa.eu/information_society/policy/nis/docs/smartgrid/wp2_2security_measures.pdf

21. European Commission/Harnser Group: A Reference Security Management Plan for Energy Infrastructure (2010), URL: http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf

22. European Network and Information Security Agency (ENISA): Good Practice Guide Network Security Information Exchanges (2009), URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide

23. European Network and Information Security Agency (ENISA): Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime (2012), URL: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime

24. European Network and Information Security Agency (ENISA): Incentives and Challenges for Information Sharing in the Context of Network and Information Security (2010), URL: http://www.enisa.europa.eu/media/news-items/enisa-analyses-the-incentives-and-challenges-to-public-2013-private-information-sharing

25. European Network and Information Security Agency (ENISA): National Cyber Security Strategies (2012), URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

26. Европейское агентство по сетевой и информационной безопасности (ENISA): Smart Grid Security (2013), URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/

27. European Network and Information Security Agency (ENISA): Smart Grid Security – Recommendations for Europe and Member States (2012), URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations

28. European Network and Information Security Agency (ENISA): Smart Grids Security (2013), URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations

29. Fred Schreier: On Cyberwarfare, in: DCAF Horizon 2015 Working Paper No. 7 (2012), URL: http://www.dcaf.ch/Publications/On-Cyberwarfar

30. Премьер-министр Франции: Instruction générale interministérielle relative à la sécurité des activités d'importance vitale, (2008), no. 6600/SGCN/PSE/PPS of September 26, 2008, URL: http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_1338.pdf

31. Gabriel Weimann: Cyberterrorism: The Sum of All Fears?, Studies in Conflict & Terrorism (2005), URL: http://dx.doi.org/10.1080/10576100590905110

32. Government of Canada: National Strategy for Critical Infrastructure (2009), URL: http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-eng.pdf

33. G8 presidency of the Russian Federation: Official Website of the G8 presidency of the Russian Federation in 2006: Global Energy Security (2006), URL: http://en.g8russia.ru/docs/11.html

34. Homeland Security Project: Cyber Security Task Force: Public-Private Information Sharing (2012), URL: http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf

35. ICS-ALERT-10-301-01A – CONTROL SYSTEM INTERNET ACCESSIBILITY, URL: http://ics-cert.us-cert.gov/pdf/ICS-ALERT-11-343-01A.pdf

36. IEC 62443-2-4: Baseline Security Standard for Industrial Automation Control Systems, URL: http://ics-cert.us-cert.gov/icsjwg/presentations/fall2011/D2-24-0200pm_Track1_Ahmadi-Holstein_rr_Title-BaseSecStandIndAuto.pdf

37. ifo Institut für Wirtschaftsforschung e.V.: ifo Schnelldienst 07/2011 (8.4.2011), URL: http://www.cesifo-group.de/de/ifoHome/publications/docbase/details.html?docId=15521107

38. Intelligence and National Security Alliance (INSA): Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models (2009), URL: http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx

39. Kaspersky: The „Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies, URL: http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies

40. Kuratorium Sicheres Österreich (KSÖ): Cybersicherheit in Österreich (2012), URL: http://www.kuratorium-sicheres-oesterreich.at/themen/detail-ansicht/thema/cybersicherheit-in-oesterreich/

41. McAfee: In the Crossfire – Critical Infrastructure in the Age of Cyber War (2010), URL: http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf

42. McAfee: In the Dark – Crucial Industries Confront Cyberattacks (2011), URL: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf

43. Mehmet Nesip Ogun: Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes, Journal of Applied Security Research (2012), URL: http://dx.doi.org/10.1080/19361610.2012.656252

44. Ness, Larry: Terrorism and Public Utility Infrastructure Protection (2008), URL: http://www.ensec.org/index.php?option=com_content&view=article&id=154:terrorismandpublicutility-infrastructureprotection&catid=84:energyinfrastructureprotection&Itemid=324

45. Netherlands: Ministry of the Interior and Kingdom Relations, National Risk Assessment method Guide 2008 (2008).

46. National Infrastructure Advisory Council (NIAC): Intelligence Information Sharing. Final Report and Recommendations (2012), URL: http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf

47. Public Safety Canada: Identifying and Marking Critical Infrastructure Information Shared in Confidence with the Government of Canada, URL: https://www.publicsafety.gc.ca/prg/ns/ci/lbl-snstv-info-eng.aspx

48. Securing America's Future Energy: How Vulnerable Are Energy Facilities to Cyber Attacks? (2010), URL: http://www.secureenergy.org/sites/default/files/1111_SAFEIntelligenceReport3120100120.pdf

49. Sicherheitsforum Baden-Württemberg: SiFo-Studie 2009/2010 – Know-how-Schutz in Baden-Württemberg (2010), URL: http://www.sicherheitsforum-bw.de/index.php?option=com_content&view=article&id=54&Itemid=82

50. Siemens AG: IT-Security in der Prozessautomatisierung mit Siemens SIMATIC PCS: 7 ARC Whitepaper Simatic PCS7, URL: http://www.automation.siemens.com/mcms/process-control-systems/SiteCollectionDocuments/efiles/pcs7/support/marktstudien/ARC_WhitePaper_Siemens_SIMATIC_PCS7_Security_de.pdf

51. Siemens AG: Operational Guidelines für Industrial Security (2011), URL: http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_de.pdf

52. Statistisches Bundesamt: Fachserie 4 Reihe 6.1 Produzierendes Gewerbe (2010), URL: https://www.destatis.de/DE/Publikationen/Thematisch/Energie/Struktur/BeschaeftigungUmsatzKostenstruktur.html

53. T-Systems: Best Practice – Das Kundenmagazin von T-Systems Ausgabe 04/2011 (2011), URL: http://www.t-systems.de/news-media/ausgabe-04-2011/754902

54. Techworld: ReVuln showcases vulnerabilities in SCADA software, but won't report them to vendors - Meldung auf techworld.com, URL: http://news.techworld.com/applications/3412614/revuln-showcases-vulnerabilities-in-scada-software-but-wont-report-them-to-vendors/

55. The National Academies Press (NAP): Terrorism and the Electric Power Delivery System (2012), URL: http://www.nap.edu/openbook.php?record_id=12050&page=1

56. The Smart Grid Interoperability Panel (SGIP): Introduction to NISTIR 7628 – Guidelines for Smart Grid Cyber Security (2010), URL: http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf

57. TNO: Good practices manual for CIP policies for policymakers in Europe (2011), URL: http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=2&item_id=2011-09-21%2010:30:22.0&Taal=2

58. TrendMicro: The „Lurid" Downloader – Report of a targeted malware campaign by TrendMicro, URL: http://www.trendmicro.es/media/misc/lurid-downloader-enfal-report-en.pdf

59. U.S. Congress: Cyber Security Act of 2012 (2012), URL: http://www.gpo.gov/fdsys/pkg/BILLS-112s2105pcs/pdf/BILLS-112s2105pcs.pdf

60. U.S. Department of Energy: A Comparison of Cross-Sector Cyber Security Standards (2005), URL: http://www.inl.gov/scada/publications/d/a_comparison_of_cross-sector_cyber_security_standards.pdf

61. U.S. Department of Homeland Security: A Comparison of Oil and Gas Segment Cyber Security Standards (2004), URL: http://scadahacker.com/library/Documents/Standards/Comparison%20of%20Oil%20and%20Gas%20Segment%20Cyber%20Security%20Standards.pdf

62. U.S. Department of Homeland Security: Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive (2012) , URL: http://www.dhs.gov/xlibrary/assets/mgmt/mgmt-classified-national-security-program-implementation-directive.pdf

63. U.S. Department of Homeland Security: Information Sharing Strategy (2008), URL: http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf

64. U.S. Department of Homeland Security: National Infrastructure Protection Plan, NIPP (2012), URL: https://www.dhs.gov/national-infrastructure-protection-plan

65. U.S. Department of Homeland Security: Energy Sector-Specific Plan (2010), URL: http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf;

66. U.S. Department of Homeland Security: Communications Sector-Specific Plan (2010), URL: http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf

67. U.S. Government Accountability Office (GAO-11-117): Electricity Grid Modernization (01/12/2011), URL: http://www.gao.gov/new.items/d11117.pdf

68. Verband Schweizerischer Elektrizitätsunternehmen: ICT Continuity. Handlungsempfehlungen zur Sicherstellung der Versorgung (2011), URL: http://www.strom.ch/uploads/media/VSE_ICT-Continuity_12-2011_D_01.pdf

8. Глоссарий

Бот-сеть
Бот-сеть представляет собой группу компьютеров, контролируемых из одного источника , на которых запущены связанные программы и командные файлы. Хотя бот-сети могут использоваться для распределенная обработки данных, например, при обработке научных данных, этот термин обычно означает группу из нескольких компьютеров, которые были заражены вредоносной программой.

Компьютерный вирус-червь
Компьютерный вирус-червь – это компьютерная программа, самовоспроизводящаяся после запуска. В отличие от компьютерного вируса, червь распространяется, не заражая другие файлы данных или сектора загрузки своим кодом. Черви распространяются через сети или съемные носители, такие как USB-накопители.

Важнейшие объекты инфраструктуры (CI)
Физические ресурсы, услуги и оборудование информационных технологий, сети и активы, значение которых таково, что ограничение их дееспособности или их разрушение может привести к ослаблению безопасности, экономики, социального благополучия или социальной безопасности, к ущербу окружающей среды или какому-либо сочетанию этих элементов в любом государстве или штате.

Защита важнейших объектов инфраструктуры (CIP)
Программы, мероприятия и взаимные действия, применяемые владельцами и операторами для защиты их важнейших объектов инфраструктуры.

Защита важнейших объектов энергетической инфраструктуры (CEIP)
Программы, мероприятия и взаимные действия, применяемые владельцами и операторами для защиты их важнейших объектов энергетической инфраструктуры.

(Распределенная) атака типа «отказ в обслуживании» (DoS-атака)
Попытка ограничения доступа к компьютеру или сетевому ресурсу. Несмотря на то что средства осуществления, мотивы и цели таких атак могут быть разными, обычно они состоят из усилий одного или нескольких людей, направленных на временное или постоянное прерывание или приостановку услуг основного компьютера, подключенного к Интернету. Один распространенный метод атаки предполагает отправку компьютеру-цели огромного количества запросов о связи извне, с тем чтобы перегрузить сервер, который в результате оказывается не в состоянии передавать обычные сообщения или отвечает так медленно, что фактически недоступен. В целом, DoS-атаки вынуждают либо перегрузить целевой компьютер (компьютеры), либо использовать все его ресурсы, и тогда он больше не сможет оказывать ожидаемые услуги.

Промышленные системы автоматизации и управления
Новое назначение систем ICS, включающее аспект автоматизации. В новых стандартах обычно говорится об IACS, а не ICS.

Инфраструктура
Структура взаимозависимых сетей и систем, составляющих различимые отрасли, учреждения (включая людей и процедуры), и возможности распределения, которые обеспечивают надежный поток продуктов и услуг, бесперебойное функционирование государственных органов на всех уровнях, а также общества в целом.

Атака с применением технологии «незаконный посредник» (MITM)
Такой тип атаки представляет собой форму активной прослушки, в которой третья сторона вводит в заблуждение двух партнеров по коммуникации, заставляя их верить, что они разговаривают напрямую друг с другом. Обычно применяется для уничтожения защитного кодирования (например, соединения SSL в онлайн-банкинге). На самом деле оба партнера по коммуникации шифруют свои данные, но делают это таким образом, что «незаконный посредник» может прочитать их и направить другому лицу.

Риск
Вероятность потери, ущерба или травмы. Степень риска определяется двумя факторами: (1) стоимостью актива, назначенной его владельцем/оператором, и воздействием потери или изменения этого актива, и (2) вероятностью того, что определенная уязвимость будет использована для конкретной угрозы.

Оценка рисков
Процесс оценки угроз уязвимым местам актива для выработки экспертного мнения о вероятности потери или повреждения и его воздействии, в качестве руководства к действию..

Управление рисками
Обдуманный процесс понимания рисков и принятия решений, а также реализации действий для снижения риска до определенного уровня, который является приемлемым уровнем, достигаемым с приемлемым уровнем затрат. Такой подход характеризуется определением, оценкой рисков и контролем над ними до уровня, соизмеримого с надлежащим.

Анализ трафика
Этот термин используется для обозначения мониторинга и чтения данных (с помощью программ или оборудования), передаваемых по компьютерным сетям. Хотя коммерческий анализ трафика используется для анализа и поддержания сетей, также существуют анализ, нацеленный на перехват данных.

Диспетчерское управление и сбор данных (SCADA)
Системы SCADA представляют собой один из видов промышленных систем контроля (ICS) – они контролируют и оценивают физические процессы с помощью датчиков и программируемых устройств управления. SCADA часто используется как синоним ICS или IACS для всего спектра технологий, связанных с кибер-физическим взаимодействием.

Угроза
Любое событие, которое потенциально может нарушить работу или разрушить важнейший объект инфраструктуры или какой-либо его элемент. Комплексный подход к угрозам включает несчастные случаи, стихийные бедствия и подготовленные атаки.

Оценка угрозы
Стандартизированный и надежный метод оценки угроз для инфраструктуры.

Уязвимость (уязвимая сторона, место)
Характеристика элемента проекта, внедрения или функционирования важнейшего объекта инфраструктуры, которая делает его восприимчивым к разрушению или выходу из строя в результате угрозы.

9. Сокращения

АТП ДПТНУ - Антитеррористическое подразделение / Департамент по противодействию транснациональным угрозам / ОБСЕ

BCM – Управление непрерывностью деятельности

BSI – Федеральное управление по информационной безопасности Германии

CERT – Группа быстрого реагирования на нарушения компьютерной безопасности

CIP – Защита важнейших объектов инфраструктуры

COTS - Готовый коммерческий продукт

DB AG – Deutsche Bahn AG (Железные дороги Германии)

DDoS – Распределенная атака типа «отказ в обслуживании»

DoS – Отказ в обслуживании

ENISA – Европейское агентство по сетевой и информационной безопасности

ES-ISAC – Центр информационного обмена и анализа сектора электроэнергии

ESMA - Европейская система интеллектуального учета

ЕС – Европейский Союз

FONES - Федеральное управление сырьевого обеспечения национальной экономики Швейцарии

ICT – Информационные и коммуникационные технологии (ИКТ)

МЭА – Международное энергетическое агентство

IEC – Международная электротехническая комиссия (МЭК)

IRGC - Международный совет по управлению рисками

ISMS – Система управления информационной безопасностью

ISO – Международная организация по стандартизации (ИСО)

IT-ISAC – Центр информационного обмена и анализа

KPI – Ключевые показатели деятельности (КПД)

MELANI – Melde- und Analysestelle Informationssicherung

НАТО – Организация североатлантического договора

NCSS – Государственная стратегия кибербезопасности

NERC – Североамериканская корпорация по обеспечению надежности электросистем

NIPP – Национальный план защиты инфраструктуры

NIST – Национальный институт стандартов и технологии США

PDCA – «Планирование, реализация, контроль, корректировка»

ГЧП – Государственно-частное партнерство

ROE – Рентабельность капитала

SCADA – Система дистанционного управления и сбора данных

10. Список рисунков и таблиц

Организация по безопасности и сотрудничеству в Европе работает во имя стабильности, процветания и демократии в 57 государствах путем политического диалога на темы общих ценностей и путем практических действий, обеспечивающих долговременные перемены к лучшему.

ОБСЕ Организация по безопасности и сотрудничеству в Европе

Организация по безопасности и сотрудничеству в Европе
Wallnerstrasse 6
A-1010 Vienna,
Austria
Телефон: +43 1 514 360
info@osce.org