USAID
FROM THE AMERICAN PEOPLE

РУКОВОДСТВО ПО РАЗРАБОТКЕ СТРАТЕГИИ КИБЕР БЕЗОПАСНОСТИ ЧЕРНОМОРСКОГО РЕГИОНА

December 2017
This publication was produced for review by the United States Agency for International Development (USAID). It was prepared by the National Association of Regulatory Utility Commissioners (NARUC).

РУКОВОДСТВО ПО РАЗРАБОТКЕ СТРАТЕГИИ КИБЕР БЕЗОПАСНОСТИ ЧЕРНОМОРСКОГО РЕГИОНА

Project Title: Energy Sector Cybersecurity

Sponsoring USAID Office: USAID/ Europe and Eurasia Bureau

Cooperative Agreement #: USAID CA # AID-OAA-A-16-00049

Date of Publication: December 2017

Authors: Miles Keogh, Paul Stack, Ben Morano (NARUC)

National Association of Regulatory Utility Commissioners

This publication is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of the National Association of Regulatory Utility Commissioners (NARUC) and do not necessarily reflect the views of USAID or the United States Government.

Содержание

Вводная информация и признательность

Национальная ассоциация членов комиссий по регулированию коммунальных предприятий (NARUC) при поддержке Агентства Международного развития США (USAID), разработала этот документ - Руководство по разработке стратегии кибер безопасности Черноморского региона, чтобы обеспечить информацию и поделиться опытом, который поддержит органы регулирования Черноморского региона в разработке стратегий по кибер безопасности своих комиссий. На основании опыта и наилучшей практики комиссий штатов и других стран документ был разработан, чтобы осветить важные проблемы и вопросы, которые будут решать органы регулирования, начиная процесс разработки своих уникальных стратегий по кибер безопасности.

Содержание данного документа было представлено работой Научно-исследовательской лаборатории NARUC с органами регулирования штатов по кибер безопасности, а также на двух семинарах с органами регулирования Черноморского региона при поддержке USAID, которые проводились в Киеве, Украине, 30 ноября - 1 декабря, 2016г. и Таллинне, Эстонии, 30-31 марта, 2017г.

Введение

Кибер безопасность во многом похожа на путешествие с неизвестными, вызовами и множеством разных путей, которыми можно пойти. Так же как карта является основой для путешествия, разработка стратегии является основополагающей для любой комиссии, которая хочет серьезно воспринимать кибер безопасность. И в США и в ЕС большинство комиссий по регулированию начали свою работу по кибер безопасности с создания стратегии.

В свете выше сказанного, Руководство по разработке стратегии кибер безопасности Черноморского региона определяет четкие этапы, которые должны пройти органы регулирования в процессе разработки своих собственных стратегий кибер безопасности. Руководство включает ключевые вопросы, которые должны решать органы регулирования при структурировании своих стратегий и перечисляет примеры, детализируя тот факт, как комиссии США подходили к каждому из заданных вопросов. Так же, как можно потеряться путешествуя без карты, комиссии, начинающие работу по кибер безопасности не имея стратегии, не будут эффективными.

Необходимо подчеркнуть, что данное Руководство не предназначается для того, чтобы навязывать регуляторам что делать, или как должны выглядеть их стратегии. Перед каждой комиссией стоят разные реалии и каждая имеет свои приоритеты и ресурсы в своем распоряжении. У каждой комиссии будут разные ответы, и они будут разрабатывать разные стратегии в соответствии со своими нуждами и приоритетами. В то время, как конечные результаты будут варьироваться, уделить время и подумать о проблемах и вопросах представленных в данном руководстве – это самый важный этап. В конце данного процесса, каждая комиссия будет иметь базовую структуру и ответы, для того, чтобы разработать свою уникальную стратегию по кибер безопасности.

Этот процесс может показаться пугающим, но не должен быть таким. Следуя по этапам и отвечая на вопросы, представленные в Руководстве, комиссия должна иметь базовую структуру и направление, чтобы создать простую и эффективную стратегию, которая может расти и развиваться, в то время как комиссия и энергокомпании движутся в направлении все большего сотрудничества и эффективности в улучшении кибер безопасности в секторе энергетики.

1. Первый этап – определение миссии и целей

По сути, любая стратегия кибер безопасности содержит определение того, почему комиссия ценит кибер безопасность, каковы цели комиссии, и как будут добиваться этих целей. До разработки стратегии кибер безопасности, каждая комиссия должна прежде всего определить свои ценности и цели – то есть почему кибер безопасность важна для них и чего они хотят достичь, решая этот вопрос.

Этот первый шаг задает тон всему процессу создания стратегии и посылает послание энергокомпаниям, что кибер безопасность важна. Определив ожидания регулятора, комиссия может сказать энергокомпаниям, что осторожные расходы компаний приемлемы, и, давая такое послание, мотивировать их серьезно воспринимать кибер безопасность. Этот процесс не должен быть сложным. Многие комиссии США начали с нескольких предложений или параграфов в виде политического заявления.

Однако в конце первого этапа комиссия должна четко сказать о своих целях, как они будут направлены на кибер безопасность, какая будет роль комиссии, и какой будет уровень взаимодействия с энергокомпаниями и другими заинтересованными лицами. Это политическое заявление, независимо от размера, обеспечит чувство цели, идентичности, и долгосрочного направления комиссии, и послужит тому, чтобы сообщить внутренне и внешне, что именно ценит комиссия в отношении кибер безопасности.

1.1 Заявление миссии

Заявление миссии позволяет комиссии определить “кем она является” в мире кибер безопасности. Заявление миссии должно подчеркнуть приоритеты комиссии и вопросы, которые она считает важными, а также определить, каким будет порог прогресса по кибер безопасности. В то время как заявления миссии могут во многом различаться, каждое должно четко объяснять, что важно для комиссии, на таком языке, который будет понятен и служащим комиссии и внешним заинтересованным лицам. Это очень важно, так как это определит ожидания как внутренне в комиссии, так и внешне для заинтересованных лиц. Если энергокомпании и другие заинтересованные лица не смогут определить приоритеты комиссии, им будет трудно действовать соответственно.

Заявление миссии должно также определить цели стратегии. Эти цели или задачи обеспечивают картину того, куда хочет идти комиссия. Цели любой комиссии должны быть реалистичными и достижимыми, сочетая то, что ценит комиссия с реальностями, которые

стоят перед ней. Цель стать “на 100% полностью кибер безопасной,” например, будет нереальной для комиссии. Можно подумать, что такая цель покажет, насколько серьезно комиссия относится к вопросу кибер безопасности, но на самом деле эта цель будет контр продуктивна, так как и комиссия, и энергокомпании не смогут ее достичь.

Вместо этого комиссия может решить определить свои цели как наличие возможности улучшить кибер инвестиции со стороны энергокомпаний, имея хорошую коммуникацию с компаниями и развивая прозрачную и полезную отчетность. Эти цели четко определяют, что пытается сделать комиссия, и кроме того, они достижимы.

Практический пример комиссии по регулированию коммунальных предприятий и транспорту штата Вашингтон

Например, регуляторы комиссии штата Вашингтон разработали следующее утверждение миссии:

Наша миссия – защищать народ нашего штата, обеспечивая, чтобы услуги энергокомпаний, принадлежащих инвесторам, и транспортные услуги, были надежными, безопасными и со справедливо установленными ценами. Чтобы обеспечить нашу миссию в отношении кибер безопасности, задачи данной стратегии - это облегчить принятие решений на основе рисков, взвешивая компромиссы и действия поддержки, такие как:

- *Предотвращение кибер атак, направленных на объекты жизнеобеспечения;*
- *Снижение уязвимости к кибер атакам; и*
- *Минимизация урона и времени восстановления после того, как кибер атаки имели место.*

Внешнему наблюдателю заявление миссии может показаться общим, но для энергокомпании, правительственного агентства или комиссии в целом язык и послание абсолютно понятны. Слова “безопасный, доступный, надежный и со справедливой ценой” подчеркивают то, что задачи комиссии в отношении кибер безопасности совпадают с общей миссией регулятора коммунальных и транспортных услуг по обеспечению безопасных, надежных, доступных коммунальных услуг для потребителей. Другими словами, кибер безопасность не повлияет на ключевую миссию комиссии. Более того, язык подчеркивает, что комиссия будет использовать подобный подход в уравновешивании интересов, используя процесс принятия решений на основе рисков.

Как обсуждалось на втором семинаре USAID-NARUC в Таллинне, Эстонии, органы регулирования коммунальных услуг не являются экспертами по кибер или безопасности. Вместо этого, они – люди “до” и “после”, будь то строительство новой станции или готовность к аварийной ситуации. Утверждение миссии Комиссии по регулированию коммунальных услуг штата Вашингтон подчеркивает этот момент, фокусируя внимание на компонентах кибер безопасности до и после, отмечая, что комиссия будет работать с энергокомпаниями по снижению уязвимости и “предотвращению кибер атак против объектов жизнеобеспечения” (часть, которая до) и минимизировать повреждения и время восстановления после того, как кибер атаки произошли (часть после).

Язык “фасилитации” и “поддержки” также подчеркивает еще один ключевой момент по поводу подхода комиссии к вопросу кибер безопасности. Язык подразумевает, что основная группа, которая имеет задачу кибер безопасности, будет не у регулятора, а у энергокомпаний. Комиссия не будет заниматься микро менеджментом и работать над мелкими деталями создания защиты кибер безопасности, а скорее играть роль фасилитатора и надзора. Полезная аналогия была сделана выступавшими на семинаре в Таллинне – регуляторы не строители замков, но они должны быть в состоянии анализировать и знать, что составляет прочный хорошо построенный замок. Фактически комиссия не обязана иметь технические и строительные навыки, чтобы строить тот самый замок, но они должны быть в состоянии направлять процесс и осуществлять надзор.

Последние пункты также важны тем, что это цели, которые достижимы. Определяя такие цели, как снижение уязвимости и минимизация ущерба, комиссия по регулированию коммунальных услуг и транспорту штата Вашингтон признает, что полностью устранить кибер атаки невозможно. Действительно, не может быть на 100% кибер безопасной системы, и комиссия не будет ожидать этого от энергокомпаний. Вместо этого комиссия сконцентрирует внимание на принятии того факта, что нет совершенной кибер безопасности, и будет работать, чтобы смягчать сопутствующие риски и управлять ими.

2. Разработка стратегии кибер безопасности – вопросы, которые надо задавать

Как только комиссия узнала, кто они (заявление миссии) и куда они хотят идти (цели), тогда они смогут разработать стратегию кибер безопасности, чтобы определить, как они планируют достичь этих целей, уровень взаимодействия, который у них будет с энергокомпаниями, и какова будет их роль. Это может начинаться, и во многих случаях начинается, с небольшого масштаба, до того как развиться со временем. Комиссии штатов Коннектикут и Вашингтон имеют две из самых сложных стратегий всех органов регулирования штатов, но обе начали с намного более простой точки отсчета. Когда комиссия по регулированию коммунальных предприятий и транспорта начала фокусировать внимание на кибер безопасности, они начали с двух страниц изложения, с указанием, что кибер безопасность представляет из себя проблему, и они обеспечат приоритеты. На основе этого меморандума, комиссия сформировала рабочую группу, которая в свою очередь работала с другими заинтересованными лицами, чтобы разработать более сложную стратегию кибер безопасности обозначившую приоритеты комиссии, масштаб и вид вовлечения. Начав с простого, комиссия указала, что кибер безопасность будет приоритетом для них и это помогло определить ожидания, как внутри комиссии, так и внешне, и задать темп, чтобы привести их к тому, где они находятся сейчас.

Следующая часть была разработана, чтобы обеспечить точку отсчета для регуляторов. Эти вопросы не имеют одного правильного ответа, но должны использоваться, для того, чтобы посмотреть, что каждая комиссия хочет получить от этого процесса, когда она разрабатывает свою стратегию.

Как Артур Хаус, бывший председатель органа регулирования штата Коннектикут, отметил в своей презентации для органов регулирования в Киеве, Украине, в декабре 2016г., очень важно для органов регулирования сделать по крайней мере первый шаг. Первый шаг установит цели и путь вперед для каждой комиссии и будет служить основой для начала разговора с энергокомпаниями, что приведет к улучшению кибер безопасности в секторе энергетики.

2.1 Сфера стратегии

Какую сферу вы хотите, чтобы ваша стратегия покрывала? Какие секторы она должна включать и какой уровень фокусирования должна иметь?

Вопрос сферы относится к **широте** и **глубине** фокуса и внимания комиссии к кибербезопасности. Этот вопрос является фундаментальным для разработки стратегии кибер безопасности. Каждая комиссия должна сопоставить свою сферу с реальностью, которая стоит перед ней – например, ресурсы, приоритеты, взаимоотношения с энергокомпаниями – чтобы определить, какая сфера имеет больше всего смысла для них. Отсюда сфера может расширяться при изменении реальности или обстоятельств. Как упоминалось во введении, успешные стратегии были разработаны с разными ответами на вышеупомянутый вопрос, поэтому нет универсального шаблона.

Что касается широты, сфера должна включать такие секторы, которые хотел бы выбрать регулятор. Например, штат Коннектикут первоначально решил включить энергораспределительные компании, компании природного газа, воды и телекоммуникации.

В свою очередь, глубина относится к степени и регулярности взаимодействия, которое комиссия ожидает иметь со своими энергокомпаниями и коммунальными предприятиями. Для стран Черноморского региона, где довольно мало распределительных и передающих компаний, вопрос сферы может быть довольно прямолинейным, в то время как для Украины, в которой 40 распределительных компаний или “облэнерго,” НКРЭКП может захотеть рассмотреть некоторые подходы более крупных штатов США.

В то время как есть несметное количество примеров штатов США, комиссия штата Вашингтон и комиссия общественных услуг штата Кентукки будут служить полезным контрастом в подходах, которые могут использовать регуляторы Черноморского региона:

- Комиссия по регулированию коммунальных предприятий и транспорта штата Вашингтон определила, что для них лучше начать с малого, чтобы процесс начался, вместо того, чтобы ждать. Другими словами, они хотели упростить процесс и работать успешно с ограниченными ресурсами. Комиссия начала с 12 вопросов, и они решили, что они будут только задавать эти вопросы энергокомпаниям инвесторов. Со временем стратегия строилась, чтобы стать более всесторонней и вовлечь дополнительные заинтересованные лица. Комиссия штата Вашингтон

сказала, что они узнали, что если начинать с минимального масштаба, это потребует меньшего времени и ресурсов, и это поможет добиться успеха и даст толчок, чтобы дальше наращивать потенциал комиссии в области кибер безопасности.

- Комиссия по регулированию коммунальных услуг штата Кентукки начала с более широкого и глубокого диапазона, включая все свои компании в процесс. И хотя этот подход более детальный, он требует больше времени и ресурсов, а также скоординированных компаний, чтобы использовать этот подход и быть эффективным.

Полезной точкой отсчета для определения диапазона комиссии является Руководство по кибер безопасности 2017г. научно-исследовательской лаборатории NARUC, которое обеспечивает вводное объяснение ключевых вопросов и включает более 100 вопросов, которые надо задавать энергокомпаниям. В то время как не каждый вопрос может относиться к комиссии, выбор ряда вопросов, которые комиссия хотела бы задать энергокомпаниям, может быть легким и эффективным местом для начала.

2.2 Подготовка комиссии

Как должна подготовиться комиссия?

По сути, эффективное управление кибер безопасностью связано с **процессом** и **посредничеством** для комиссий. В то время как технические знания важны, подход и упор должны делаться на поперечном разрезе и вовлечении многих департаментов внутри комиссии. Одна из самых больших ошибок комиссии - это выделить кибер безопасность как строго техническую проблему.

Вместо этого комиссии должны создать рабочую группу из тех, которые могут соединять с заинтересованными группами и которые знают, как управлять процессами и конкурирующими интересами. Эффективным для многих комиссий США оказалось выявление лидера внутри руководства, который мог бы помочь привести процесс в действие, а также сотрудников в разных областях работы комиссии. В то время как этот подход является эффективным, конкретная организация и структура рабочих групп во многом различаются, и комиссии должны выбирать ту структуру, которая лучше всего подходит под их приоритеты и организационную схему. Комиссии США определили, что группы с техническими и политическими специалистами, а также с членом комиссии , возглавляющим процесс, оказались очень успешными.

В свете вышесказанного, стратегия должна четко формулировать: 1) какие сотрудники в комиссии будут работать по кибер безопасности – это также означает определение того, должна ли быть конкретная должность по кибер безопасности или сотрудники должны работать по кибер безопасности дополнительно к другим обязанностям; и 2) как первоначально комиссия планирует подойти к вопросу кибер безопасности.

2.3 Сотрудники по кибер безопасности и политики

Кто будет нести ответственность внутри? Какие внутренние политики необходимы?

Для ответственного подхода к кибер безопасности, необходимо чтобы был **персонал** и **финансирование** в комиссии. В то время как уровни финансирования и обеспечения персоналом могут сильно отличаться по комиссиям, эти два элемента являются ключевыми для успешной кибер безопасности. В США, например, в штатах Техас, Нью-Йорк и Огайо комиссии назначили персонал для работы над кибер безопасностью, в то время, как комиссия штата Вашингтон назначила дополнительно двух человек, один с опытом в сфере разработки политики, второй с опытом в сфере услуг регулирования. В 2017 году, Комиссия по торговле штата Иллинойс (ICC) решила ввести должность Директора по кибер безопасности, более высокого уровня. Вместо того, чтобы нанимать новый персонал, регулирующие органы могут также наращивать потенциал существующего персонала, чтобы они работали по кибер безопасности вдобавок к текущим обязанностям. Не обязательно, чтобы они были назначены на полный рабочий день - это может занимать только часть рабочего времени, но это время должно быть определено и задание поставлено.

Комиссии также должны проводить реалистичную оценку своих отношений с энергокомпаниями, и того, насколько они могу получать информацию от них. Обмен информацией и управление ей является ключом к успеху. Наиболее успешные комиссии США убедились, что регулирующие органы и энергокомпании должны сотрудничать по-другому, когда речь идет о кибер безопасности, в отличие от других вопросов.

Это касается не только того, как регулирующие органы сотрудничают с энергокомпаниями, но и того, кто руководит этим сотрудничеством. Те, кто взаимодействует с энергокомпаниями в отношении других вопросов, правильные ли это люди, чтобы работать по вопросам кибер безопасности? Общение и обмен информацией является ключевым, и комиссии должны убедиться, что выбрали правильных людей для построения взаимоотношений и эффективной работы со соими коллегами в энергокомпаниях.

В кибер безопасности есть технические аспекты, которые могут легко восприниматься компьютерными специалистами. Однако, в сфере регулирования энергокомпаний и коммунальных предприятий, специалисты по экономике и по вопросам регулирования должны понимать язык кибер безопасности и соответствующих вопросов для того, чтобы оценивать работу энергокомпаний и коммунальных предприятий. Комиссии должны приложить все усилия, чтобы такие специалисты в энергокомпаниях и в регулирующих органах, которые занимаются техническими и экономическими вопросами, общались между собой и понимали друг друга. В то время, как у каждой стороны есть конкурирующие интересы, цели и заботы, создание определенного уровня общения и понимания обеих сторон приведет к более исчерпывающему и эффективному планированию.

Для назначения правильного персонала и механизмов, которые они используют для общения, стратегия по кибер безопасности может выделить следующее:

- Сколько человек, и какой именно персонал комиссии будет заниматься кибер безопасностью от лица комиссии.

Как описано выше, США определили, что лучшими рабочими группами по кибер безопасности являются те, в которых есть представители разных департаментов. Учитывая, что доверие и сотрудничество являются первостепенными в сфере кибер безопасности, важно назначить правильный персонал или членов комиссий для работы с коллегами из энергокомпаний и коммунальных предприятий по чувствительным вопросам, людей, которые будут отличаться от тех, которые работают с энергокомпаниями и коммунальными предприятиями по более негативным и провокационным вопросам.

- Уровень финансирования, который комиссия отложит специально на решение вопросов кибер безопасности
- Политики внутренней и внешней коммуникации, которые понадобится изменить или принять комиссиям, чтобы обеспечить внедрение стратегии кибер безопасности и взаимодействовать с энергокомпаниями и коммунальными предприятиями. Например, комиссия должна определить, нужна ли новая политика для работы с чувствительной информацией, которую она получает в сфере кибер безопасности. В свою очередь, стратегия должна определить, необходимо ли комиссии пересмотреть и/или разработать дополнительные процедуры или процессы, и как она это сделает.

2.4 Требования работы и отчетность

Какие у вас функциональные требования к компаниям, которые вы регулируете?

Комиссии должны определить, чего они ожидают от своих энергокомпаний в контексте инвестиций в кибер безопасность, чтобы такие ожидания могли быть включены в дальнейшее планирование и функционирование. Чтобы это обеспечить, комиссии должны определить, от каких событий защита является обязательной, таких как утечка данных и функциональные перебои. При определении, что приемлемо, а что нет, все заинтересованные лица смогут проводить планирование соответствующим образом.

Также важно для комиссий определить способы взаимодействия со своими энергокомпаниями. Как энергокомпании будут осведомлять комиссии, и какой способ общения будет лучшим? Кто будет принимать участие в проверке, и каким образом будет производиться сообщение об инцидентах? Эти процессы необходимо разработать в течение процесса планирования при участии энергокомпаний. Это обеспечит вовлеченность и приведет к более эффективному процессу.

Примеры штатов США

План работы – регулирующие органы штата Коннектикут работали совместно с энергокомпаниями и решили двигаться дальше в сторону создания плана работы, который энергокомпании будут предоставлять регулирующим органам на ежегодной основе.

Брифинги – штат Мичиган, Айова и Индиана – эти штаты проводят неформальные брифинги в компании. Такие брифинги запланированы на постоянной основе (как минимум раз в год).

Аудиты – штат Пенсильвания.

Примечание: Необходимо помнить, что проводить аудит кибер безопасности регулирующие органы должны осторожно, так как аудит является, в некотором роде, негативным по своей природе и может не соответствовать укреплению мер доверия, которых требует совместная работа по кибер безопасности.

Требования к отчетности по нарушениям – штат Нью-Джерси устанавливает требования к отчетности по нарушениям для своих энергокомпаний, чтобы установить ожидания того, как они будут взаимодействовать, и какую информацию необходимо передавать.

Программа управления рисками – Комиссия общественных услуг штата Кентукки выбрала вариант внедрения программы управления рисками, которая стала полностью совместным процессом для разных заинтересованных лиц, и привела к созданию структуры плана действий по безопасности на основании рисков, включая механизм постоянного общения о проблемах, угрозах и лучших практиках.

Отчетность - Какую отчетность вы предпочитаете, до, во время или после событий?

Комиссии США постоянно убеждаются, что неформальное общение и практика отчетности являются наиболее эффективным подходом, так как они позволяют проводить более открытое и честное обсуждение, а также обмениваться более полезной информацией. Процесс отчетности также должен соответствовать рискам. Например, формальный отчет об аудите не затрагивает должным образом все вовлеченные элементы. Вместо этого, запланированные полурегулярные личные проверки позволяют проводить более спокойные обсуждения и обмениваться информацией.

Во время события, связанного с кибер безопасностью, все общение должно быть сосредоточено на расчетном времени до восстановления после атак. Определение даты локализации каждого несанкционированного доступа к данным не только помогает управлять ожиданиями заинтересованных лиц, но также устанавливает базовые параметры, из которых можно извлечь уроки и в дальнейшем оценить работу.

После события необходимо разработать процесс для энергокомпаний, по которому они будут предоставлять "итоговый отчет" включая корректирующие шаги и усвоенные уроки. Такой отчет должен предоставить комиссии, и ее энергокомпаниям полезную информацию в отношении того, как произошло событие, какие шаги или действия можно было сделать для его предотвращения, и какие шаги энергокомпания и комиссия сделают следующими.

Практический пример штата Коннектикут:

Регулирующие органы штата Коннектикут согласились, что конфиденциальность для них имеет большое значение, поэтому, совместно с энергокомпаниями, они решили проводить ежегодные заседания для проверки защиты кибер безопасности с запретом на ведение записей и заметок. Фактически, комиссия по регулированию коммунальных предприятий PURA потребовала от всех участников ежегодных заседаний подписать соглашение о неразглашении. В своей презентации на семинаре в Таллинне Арт Хаус заметил, что стратегия PURA штата Коннектикут уточняет, как должны проходить общение и отчетность, что он в полной мере резюмировал в следующем списке:

- Предоставление полного отчета проходит на ежегодном заседании;

- План презентации каждой энергокомпании, ключевые моменты и таблицы предоставляются регулирующему органу до заседания;
- Учитывая, что запрещено вести записи и делать заметки (в дополнение к соглашениям о неразглашении), регулирующие органы и энергокомпании договорились о максимальном раскрытии информации во время заседания;
- Затем регулирующие органы и энергокомпании придут к соглашению об итоговом отчете ежегодного заседания. Итоговый отчет не будет включать в себя результаты или чувствительную информацию какой-либо отдельной энергокомпании;
- Итоговый отчет затем будет подан в качестве заключительного отчета губернатору, законодательной власти и общественности, при этом предоставляя общие результаты ежегодного заседания.

Для более детальной информации, стратегия PURA предоставляет обзор обсуждений отчетности, которые прошли после самого первого заседания регулирующего органа совместно с энергокомпаниями по природному газу и электроэнергии по вопросам кибер безопасности в 2015 году:

> В отношении стандартов отчетности по кибер безопасности, [некоторые энергокомпании] предпочитают использовать ES-C2M2. Они говорят, что уже используют ES-C2M2 для соответствующих программ кибер безопасности и считают, что их легче и более важно использовать, чем подстраиваться под требования штата к отчетности. Они также предположили, что концепция ES-C2M2 для MIL [показателей уровня готовности] могла бы быть полезной для отчетности, чтобы соответствовать требованиям отчетности PURA. Однако, они предупредили, что числовые показатели могут быть неправильно понятыми неосведомленной аудиторией. Они также предложили использовать "тепловые карты" положения дел в своей кибер безопасности в качестве механизма ежегодной отчетности, чтобы передать общее состояние в сферах, требующих больше всего внимания.
>
> Компании по электроэнергии и газу считают, что ES-C2M2 предоставляет хорошую структуру для определения рамок обсуждения кибер безопасности, в то время как модель рейтинга MIL была бы слишком субъективной. Также они были обеспокоены, что каждая компания может внедрить модель рейтинга по-своему. Они не хотят, чтобы процесс был сравнительным по своей природе. Более того, им было неудобно использовать детализированную оценку по системе количественного рейтинга для ES-C2M2, но они бы приняли отчетность по уровням готовности. Они указали, что возможно и ожидаемо, что не все области безопасности на высшем уровне готовности. Каждая компания балансировала бы между риском и пользой от перехода на более высокий уровень, в то же время, обосновывая определенный уровень готовности по каждой категории.
>
> PURA признало, что множество факторов влияет на уровень готовности компании по каждому набору элементов управления и заверило компании, что им позволят обосновать свою отчетность. [Определенные энергокомпании] указали, что они примут и будут следовать ES-C2M2 в поддержку процесса PURA. Они заявляют, что разрабатывали свои собственные программы в противовес ES-C2M2 во время разработки модели и не заметили пробелов ни в одном направлении между их текущими программами и новой моделью готовности. Однако, степень охвата каждой темы может различаться. Компании отметили, что модель ESC2M2 обеспечивает стандарты, по которым энергокомпании общаются с Министерством национальной безопасности и Министерством экономики на федеральном уровне.

[Консультант PURA] предположил, что отчеты компаний должны описывать состояние их эксплуатационной кибер безопасности за предыдущий год. Дальнейшие детали должны включать в себя обсуждения изменяющихся реалий угроз, уровень атак и количество зарегистрированных и предотвращенных атак. Компании считают, что такое требование уже предусмотрено отчетностью ES-C2M2.

2.5 Стимулирующая деятельность

Предполагает ли ваша комиссия стимулировать деятельность и инвестиции?

Комиссии должны определить, достаточно ли волнуют их недостатки, чтобы сказать, что в кибер безопасности ожидаются инвестиции. В то время как такая поддержка может рассматриваться энергокомпаниями как возможность тратить по своему усмотрению, такой подход использовался по другим вопросам в США, таким как поддержка возобновляемой энергии и бытовых потребителей с низким доходом. Какой-то вид указания часто необходим, так как энергокомпании обычно думают, что любые вопросы, которые регуляторы открыто не поддерживают, не будут разрешены. Однако важно найти правильный баланс, так чтобы энергокомпании не рассматривали это как приглашение к безрассудным тратам. Так же как почти во всех решениях, которые должны принимать регулирующие органы, наилучшим подходом будет стимулирование осторожных инвестиций и осторожных мер по кибер безопасности.

Практический пример штата Коннектикут:

В стратегии штата Коннектикут, комиссия определила стратегию, которая в целом предполагала стимулировать:

- Основное изменение: от кибер безопасности в качестве конфиденциального дела компании, к обмену информацией с регулирующими органами
- Отношение энергокомпаний: признают серьезность кибер угроз и необходимость новых политик и действий
- Корпоративная культура: понимание и обязательство изменить привычки безопасности по всей компании
- Принятие необходимости образования, постоянной коммуникации
- Признание того факта, что кибер безопасность - это государственный вопрос

2.6 Взаимоотношения с другими заинтересованными лицами

С кем еще вы будете работать (правоохранительными органами, информационными технологиями и т. д.)? Как вы будете работать с ними?

Стратегия кибер безопасности должна наверно иметь главу, которая определяет другие заинтересованные лица, работающие над кибер безопасностью, и описывает какими будут взаимоотношения и сотрудничество между комиссией и всеми другими заинтересованными лицами и вовлеченными правительственными агентствами. Это поможет решать и минимизировать любую неопределенность, зоны, которые пересекаются, и недостатки в регуляторной юрисдикции, а также укрепить ту роль, которую, которую будет играть регулятор в отношении кибер безопасности.

Эта глава важна. Так как многие разные заинтересованные лица играют свою роль в кибер безопасности. Эффективное сотрудничество со всеми заинтересованными лицами позволяет принимать более информированные решения. Правоохранительные органы, руководство в области информационных технологий, продавцы, разведывательное сообщество, и соседние энергокомпании, все вовлечены в кибер безопасность. В то время как уровень взаимодействия с разными заинтересованными лицами может различаться, комиссии должны определить, какие организации больше всего связаны с их работой и как они могут наилучшим образом сотрудничать и общаться с ними.

В Среднеатлантическом регионе США комиссии собирают группы заинтересованных лиц на ежеквартальной основе. Хотя встречи открыты и заметны, официальный протокол не ведется, и есть намерение проводить неформальные беседы, дающие стратегический контекст, а не формальное совместное расследование (что в административном отношении было бы более обременительным.)

Необходимо подчеркнуть, что эта глава будет очень конкретной для каждой комиссии по регулированию на основе обстоятельств характерных для каждой страны. В США вопросы федеральной юрисдикции и юрисдикции штата означают, что сотрудничество и координация между заинтересованными лицами и правительственными агентствами могут быть запутанными и сложными. Регуляторы Черноморского региона могут столкнуться с различными уникальными вызовами, характерными для их соответствующих стран.

Составляя эту главу, органы регулирования должны рассмотреть пример органа регулирования коммунальных предприятий штата Коннектикут. Комиссия по регулированию коммунальных предприятий тесно сотрудничала с офисом губернатора и поделилась проектом с заинтересованными лицами, чтобы проанализировать в частности эту главу. Это помогло обеспечить то, что все были на одной волне по поводу роли органа регулирования и взаимоотношений, которые они будут иметь со всеми другими сторонами.

2.7 Стандарты

На семинаре в Таллинне в марте 2017г. органы регулирования Черноморского региона выразили заинтересованность потенциально включить предмет стандартов в свои стратегии. Необходимо время, чтобы разработать стандарты и скорее всего со временем они будут совершенствоваться. Поэтому при разработке стратегии кибер безопасности, органы регулирования могут объяснить, собираются ли они разрабатывать и утверждать стандарты вместо того, чтобы фактически перечислить или разработать сами стандарты.

Органы регулирования заинтересованные в кибер безопасности определенно должны ознакомиться с тем, чего требуют стандарты защиты объектов жизнеобеспечения NERC (CIP) от Объединенной энергосистемы. Эти обязательные стандарты, и структуры, основанные на соответствии, обязывают операторов энергетической системы соответствовать конкретной практике кибер безопасности. Кроме рассмотрения стандартов NERC CIP, органы регулирования Черноморского региона должны также анализировать основные принципы кибер безопасности технологий (CSF) Национального института стандартов. Все вместе, NERC CIP и NIST CSF выступают в качестве существующей лучшей практики того, как стандартный подход и подход на основе управления рисками дополняют друг друга, чтобы обеспечить прочную кибер безопасность.

Комиссиям важно понимать, что есть различие между стандартами и наилучшей практикой. Это во многом относится к подходам к кибер безопасности на основе соответствия или на основе рисков, которые Руководство по кибер безопасности для органов регулирования NARUC 2017г. освещает детально. Ниже представлен отрывок из Руководства по данной теме:

Стандарты NERC со временем совершенствовались, но в целом используется подход, основанный на требованиях. Хотя эти стандарты и прочные и во многом улучшились по сравнению с тем, что было раньше, органы регулирования штатов должны помнить, что Стандарты NERC CIP все еще развиваются в отношении к объединенной энергосистеме. Те, кто заинтересован в улучшении этих стандартов доказывают, что системы распределения и другие ключевые сферы, где кибер безопасность остается проблемой для органов регулирования штатов, могут быть не полностью охвачены существующими стандартами. Кроме того, те, кто оспаривают, что стандарты CIP являются не полными, указывают, что соответствие только доказывает *соответствие*; кибер безопасность энергокомпаний должна быть основана на *оценке рисков*. Управление рисками включает оценку, снижение рисков и постоянное улучшение, в то время как соответствие предлагает рассматривать кибер безопасность в фиксированной точке времени, а не иметь динамическое представление о ней. Энергокомпании могут соответствовать стандартам CIP и все же не быть защищенными. Энергокомпании; энергокомпании могут также быть защищенными, но не соответствовать стандартам CIP. Одно не гарантирует другое. Сами по себе эти стандарты обеспечивают существенную основу, в то время как использование других инструментов в дополнение к стандартам может дать еще более сильный результат на основе рисков.[1]

[1]Руководство по кибер безопасности для органов регулирования научно-исследовательской лаборатории NARUC, 2017г. Стр. 12

Данная глава Руководства подчеркивает, что соответствие и стандарты сами по себе могут быть хорошей основой и могут способствовать хорошим результатам кибер безопасности. Однако органы регулирования не должны думать, что будет достаточно иметь контрольный перечень или подход с требованиями конкретных стандартов.

В свете выше сказанного, стратегия органа регулирования может захотеть подчеркнуть, что комиссия понимает разницу между стандартами и наилучшей практикой и будет работать с энергокомпаниями и правительственными агентствами, чтобы создать правильные стандарты для конкретной страны и использовать подход на основе рисков, чтобы мотивировать хорошую, эффективную работу по кибер безопасности. Стратегия могла бы просто включить подход комиссии к разработке правил. Стандарты NERC CIP являются хорошим ресурсом, для того, чтобы по крайней мере определить тематические области, где применялись стандарты. Ниже представлена Версия 5 Стандартов CIP [2]:

Номер	Название/Выводы	Дата внедрения
CIP-002-5.1	Кибер безопасность — категоризация кибер системы BES	07/01/2016
CIP-003-6	Кибер безопасность – Контроль управления безопасностью	07/01/2016
CIP-004-6	Кибер безопасность – Персонал и Обучение	07/01/2016
CIP-005-5	Кибер безопасность – Периметр электронной безопасности	07/01/2016
CIP-006-6	Кибер безопасность – Физическая безопасность кибер систем BES	07/01/2016
CIP-007-6	Кибер безопасность – Управление безопасностью системы	07/01/2016
CIP-008-5	Кибер безопасность – Отчеты об инцидентах и планирование деятельности по оказанию помощи	07/01/2016
CIP-009-6	Кибер безопасность – Планы действий по ликвидации последствий для кибер систем BES	07/01/2016
CIP-010-2	Кибер безопасность – Управление изменением конфигурации и оценка уязвимости	07/01/2016
CIP-011-2	Кибер безопасность – Защита информации	07/01/2016
CIP-014-2	Физическая безопасность	10/02/2015

В отличие от Объединенной системы, необходимо отметить, что в настоящее время нет обязательных всесторонних стандартов на уровне распределительных систем в США.

[2]http://www.nerc.net/standardsreports/standardssummary.aspx

2.8 Другое

Чему еще должна научиться комиссия, чтобы быть готовой?

Каждая комиссия должна определить, какой уровень готовности приемлем для них, и сколько времени, усилий и внимания они хотят вложить в кибер безопасность. Какой уровень времени персонала и ресурсов они хотят посвятить изучению кибер безопасности? Хотят ли они, чтобы их сотрудники стали экспертами по данному предмету или по крайней мере хорошо понимали профессиональный язык? Необходимо ли им, чтобы сотрудники были сертифицированы или получили разрешения? Ответы на эти вопросы будут различаться, в зависимости от приоритетов и целей комиссии.

Как комиссия будет оценивать себя, и улучшать свою работу?

Органы регулирования также рассмотрят, как они будут измерять свой успех, и заниматься циклом постоянных улучшений.

3. Разработка стратегий внутренней и внешней коммуникации

Как отмечалось везде в данном документе, коммуникация - как внутри комиссии, так и между органами регулирования и энергокомпаниями — абсолютно важна для эффективной кибер безопасности. В то время как комиссии разрабатывают свои стратегии кибер безопасности, они также должны определить стратегии внутренней и внешней коммуникации по кибер безопасности, которые могут включать отличия от стандартного протокола коммуникации.

Внутри, комиссии должны разработать стратегию коммуникации, которая позволит разным департаментам, представляющим разные интересы, разговаривать и обсуждать свои приоритеты и озабоченность в отношении разных вопросов, связанных с кибер безопасностью и включить этот процесс в разработку и исполнение стратегии кибер безопасности. Как и с другими вопросами, разные департаменты внутри комиссии будут иметь разные приоритеты по кибер безопасности. Для примера, сотрудники информационных технологий могут быть более положительно настроены по отношению к инвестициям в кибер безопасность энергокомпаниями, в то время как финансисты могут смотреть на те же инвестиции более отрицательно из-за того, что затраты будут передаваться на потребителей. Для групп с конкурирующими интересами в комиссии важно разговаривать и понимать друг друга, чтобы создавать более полное понимание рисков, налагаемых кибер безопасностью и имеющимися вариантами при разработке стратегии комиссии.

Внешне комиссии должны определить средства и методы для коммуникации, которые будут наиболее эффективными для них во взаимоотношениях с энергокомпаниями. Как упоминалось раньше, самые успешные комиссии США обнаружили, что необходим другой подход при взаимодействии и разговорах с энергокомпаниями по вопросу кибер безопасности. В то время как взаимоотношения между комиссиями и энергокомпаниями

могут иногда быть спорными по другим вопросам, эти разногласия не должны переходить в область кибер безопасности. Сотрудничество и взаимодействие являются ключевыми в обеспечении эффективной безопасности, и они важны для взаимоотношений между органами регулирования и энергокомпаниями при решении вопросов кибер безопасности. Самые успешные комиссии обнаружили, что может оказаться необходимым, чтобы развивать эффективно работающие взаимоотношения с энергокомпаниями, разработать стратегию коммуникации для сотрудников, которые не взаимодействуют с энергокомпаниями по другим вопросам. Вместо этого назначать сотрудников, которые вовлечены в рабочую группу по кибер безопасности, таких как сотрудники по техническим и политическим вопросам, чтобы они общались со своими коллегами в энергокомпаниях, чтобы помочь начать совместное обсуждение. Открытие разных каналов коммуникации посылает сигнал энергокомпаниям, что органы регулирования хотят создать продуктивные взаимоотношения, что отделено от других вопросов, которые могут вызывать разногласия.

4. Проект структуры стратегии кибер безопасности

Эта глава должна обеспечить шаблон, который комиссии могут подогнать и адаптировать на основе своих конкретных нужд, приоритетов и обстоятельств конкретных стран. Этот проект структуры обеспечивает важные темы и области, которые могли бы быть полезными для комиссий, чтобы включить их или подумать о них, в тот момент, когда они разрабатывают свои стратегии. Однако каждая комиссия должна в конце концов определить структуру, которая будет самой полезной для них.

Заявление о важности кибер безопасности, как приоритета и обязательства действовать

- Каковы ценности и цели комиссии?

Сфера взаимодействия – Секторы где регуляторы будут взаимодействовать

- Определение сферы и фокуса стратегии комиссии

Внутренняя подготовка комиссии

- Создание рабочей группы с представителями по всей комиссии

Функциональные требования к комиссиям и энергокомпаниям

- Определение ожиданий энергокомпаний и взаимодействие с энергокомпаниями

Отчетность

- Практика отчетности до, во время и после событий

Роль и взаимодействие с другими органами (Государственный сектор, правоохранительные органы, энергокомпании)

- С какими еще заинтересованными лицами будет работать комиссия, и как они будут взаимодействовать?

Стратегии внутренней и внешней коммуникации

- Разработка эффективных стратегий коммуникации, которые могут выходить за рамки нормы

Стандарты

- Описание подхода, который будет использовать комиссия в отношении установления добровольных и обязательных правил

Часть I – Заинтересована ли комиссия в разработке стандартов?
Часть II – Если да, то каким будет процесс, какие темы будут включены, и какие документы и существующие стандарты или механизмы могли бы послужить руководством для комиссии в планировании процесса (NERC CIP, NIST, и т.д.)?

Цикл постоянного улучшения

- Как комиссия будет оценивать себя и улучшать

Направление роста

- Начинать с малого и двигаться в направлении все большего потенциала

For questions regarding this publication, please contact Erin Hammel (ehammel@naruc.org).

National Association of Regulatory Utility Commissioners (NARUC)
1101 Vermont Ave, NW, Suite 200
Washington, DC 20005 USA
Tel: +1-202-898-2210
www.naruc.org