USAID
FROM THE AMERICAN PEOPLE

БАЙЕСОВСКАЯ МЕТОДИКА ОЦЕНКИ КИБЕРБЕЗОПАСНОСТИ ДЛЯ РЕГУЛЯТОРОВ

September 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).

БАЙЕСОВСКАЯ МЕТОДИКА ОЦЕНКИ КИБЕРБЕЗОПАСНОСТИ ДЛЯ РЕГУЛЯТОРОВ

Соглашение о сотрудничество №: AID-OAA-A-16-00049

Получатель: Национальная ассоциация регуляторов коммунальных предприятий (NARUC)

Дата публикации: сентябрь 2017 г.

Подготовлено: NARUC

National Association of Regulatory Utility Commissioners

Издание стало возможным благодаря поддержке Отдела энергетики и инфраструктуры Управления по Европе и Азии в рамках соглашения о сотрудничестве с Национальной ассоциацией регуляторов коммунальных предприятий №AID-OAA-A-16-00049. Изложенные в документе мнения принадлежат автору и могут не совпадать со взглядами Агентства США по международному развитию и Национальной ассоциации регуляторов коммунальных предприятий.

Содержание

1. ВВЕДЕНИЕ

Рамочная система оценки кибербезопасности USAID-NARUC для регуляторов из черноморского региона представляет собой легкий в обиходе инструмент, при помощи которого регулятор может оценивать степень кибербезопасности энергетических компаний. Архитектоника рамочной системы позволяет регуляторам проводить упорядоченный анализ достигнутого компаниями уровня кибербезопасности, а также определять те аспекты, где требуется дальнейшее совершенствование.

Рамочная система во многих смыслах является побратимом модели, известной под названием "Первичный задел NARUC для государственных регуляторов в сфере кибербезопасности", в которой изложен комплексный подход к основам кибербезопасности для экономических регуляторов и приведена последовательность мероприятий, которые позволяют регулирующим комиссиям стать эффективным партнером для энергетических компаний в профилактике и нивелировке кибератак, а также повышении общей защищенности энергетического сектора в целом.

“Первичный задел” предусматривает пять первоначальных мер со стороны регулятора. Одной из первых и наиболее важных в ряду этих мер является опрос лицензиатов со стороны регулирующей их инстанции-регулятора. “Первичный задел” содержит 107 примерных вопросов, напрямую позаимствованных из опросов, осуществленных регуляторами в США. Вопросы относятся к 12 ключевым сферам в области кибербезопасности, и их формулировка имеет своей целью получение регулятором достаточной информации от лицензиатов в целях оценки общего уровня киберзащищенности последних.

Сами по себе вопросы, однако, эффективны лишь в той степени, в какой регуляторы способны правильно истолковать ответы на таковые. С учетом этого соображения, регуляторам придется приложить усилия к тому, чтобы поработать над наращиванием собственной компетенции по проблематике основных концепций и стратегий киберзащищенности. Потребуются время и усилия со стороны персонала регулятора в целях ознакомления с ландшафтом угроз кибербезопасти, а также отвечающим данным угрозам оптимальным наработкам добротной кибергигиены и оборонительной стойки. Если регуляторы хотят понять и оценить ответы компаний по проблематике кибербезопасности, им надлежит быть подкованными в вопросах глубоко эшелонированной защиты и системной устойчивости; каким образом выстраивать приоритеты систем и сетей в сопоставлении с их компонентами; а также как задействовать эффективные структуры соподчиненного управления - и это лишь некоторые из перечисленных направлений деятельности.

В довершение к этим мероприятиям, USAID и NARUC разработали данную рамочную систему для использования в качестве систематического и структурированного механизма для регуляторов из черноморского региона, при посредстве которого последние смогут анализировать ответы энергетических компаний, а также приходить к целостным общим выводам в отношении как уровня готовности энергетических компаний, так и аспектов, где требуется дальнейшее совершенствование. Рамочная система была сверстана как исходя из учета конкретных вызовов в вопросах кибербезопасности, так и из соображений уникальной роли экономического регулятора. Кибербезопасность может быть весьма технологична по своей сути, и на данный момент нет

параметров либо исчерпывающих критериев количественных замеров работы системы кибербезопасности одной отдельно взятой компании. Такое отсутствие критериев ограничивает возможность сопоставления друг с другом поступательного развития компаний, как и сравнение оборонительной стойки каждой из них.

В свете вышеизложенного, рамочная система имеет своей целью содействовать регулятору в проведении базового количественного анализа энергетических компаний по ключевым категориям кибербезопасности (как то - планирование, закупки у поставщиков, кадровая политика и т.д.) путем привлечения в значительной степени качественных аспектов ответов на вопросы из “Первичного задела”. После чего рамочная система дает возможность регулятору синтезировать каждый раздел в общую панораму оценки с отсылкой к сильным сторонам; аспектам, подлежащим дальнейшему совершенствованию; аспектам резистентности, а также аспектам, заслуживающим дальнейшего исследовательского внимания.

Хотя данная рамка и не выведет на конечный точный цифровой показатель (мол, уровень кибербезопасности компании составляет 66%) и не позволит легко сопоставить показатели по ряду компаний, ее функция близка к той, которую выполняет Модель зрелости потенциала кибербезопасности подсектора электроэнергетики Министерства энергетики США (ES-C2M2) - инструмента самооценки, которым пользуются энергетические компании для замера и совершенствования своих кибервозможностей. Как и модель ES-C2M2, рамочная система дает регулятору возможность целостного анализа того, в какой степени подходы компании к проблематике кибербезопасности являются усовершенствованными и нетривиальными.

Вдобавок к рамочной системе как таковой (Раздел 5) мы присовокупили разделы с описанием того, в какой степени на данный инструментарий оказала информационное воздействие роль экономического регулятора (Раздел 2); поэтапная инструкция по его применению (Раздел 3); а также контекст и руководство в отношении того, где и каким образом его надлежит применять (Раздел 4).

2. РОЛЬ РЕГУЛЯТОРА

Итак - чем именно занимаются экономические регуляторы и каким образом эта деятельность будет претерпевать изменения либо оставаться неизменной, когда речь заходит о реагировании на вызовы кибербезопасности? Данный раздел посвящен основам того, что представляет собой роль экономического регулятора применительно к проблематике кибербезопасности и каким образом Рамочная оценочная система кибербезопасности была разработана для содействия регуляторам в эффективном осуществлении этой роли.

Регуляторы - люди из "До" и "После"

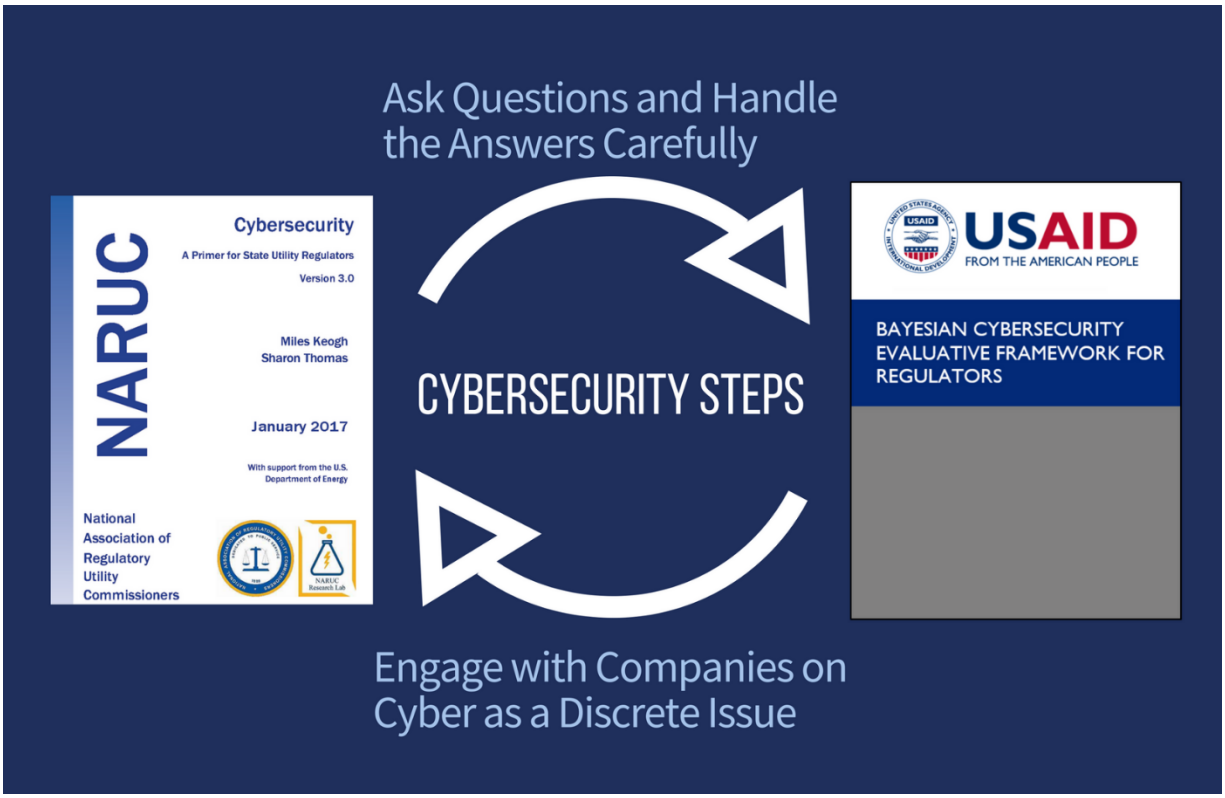
Ключевая обязанность экономических регуляторов заключается в том, чтобы гармонизировать возмещение издержек с интересами общества, гарантировать, что капиталовложения компаний-традиционных монополий гармонизированы с различными - и подчас конфликтующими друг с другом - целями общей инвестиционной политики - как то: доступность, надежность, безопасность, а также защищенность - среди многих прочих.

Вот почему во многих смыслах регуляторы снискали репутацию людей из "До" и людей из "После" - они задают перспективу и ключевые цели наперед, а также пост фактум дают оценку деятельности и производственным показателям компаний в контексте реализации данных целей.

Например - как явствует из приведенной ниже картинки, регуляторы выдвигают цели и оценивают результаты в таких сферах деятельности, как обеспечение надежности и готовности к нештатным ситуациям, но не они восстанавливают энергоснабжение по месту аварии в результате отключений после погодных катаклизмов.

.

В вопросах кибербезопасности регуляторы будут и впредь выступать в роли людей из "До" и "После". Они не будут присваивать себе функции строителей системы киберзащищенности, но им придется помогать в формулировке задач в соответствии с целями политики и периодически анализировать результаты деятельности энергетических компаний. Вот почему как “Первичный задел”, так и Руководство регулятора USAID-NARUC по стратегическому развитию кибербезопасности делают упор на том, что регуляторам надлежит прежде всего разработать стратегию, в рамках которой будут изложены цели и требования комиссии, и сформулировано, каким образом комиссия рассчитывает сотрудничать с энергетическими компаниями при постановке целей и оценке прогресса в достижении таковых.



Формулировка вопросов, которые адресуются к самым важным вопросам кибербезопасности помогает задать планку ожиданий и подает сигнал компаниям - суть которого - что им надлежит иметь план либо готовые наработки по каждому из ожидаемых параметров. Если это компонент "До" во взаимодействии регулятора с компанией по тематике кибербезопасности, то компонент "После" подразумевает рассмотрение ответов - т.е., в какой степени результаты деятельности компании совпадали с ожидаемыми.

В целях эффективной оценки работы компаний регуляторы должны владеть базовым пониманием того, что считается удовлетворительным ответом - то есть, что представляет собой добротная кибербезопасность. В дополнение к “Первичному заделу”, регуляторам следует рассмотреть Стандарты защиты критической инфраструктуры (CIP) Североамериканской корпорации по надежности электроснабжения (NERC), а также Рамочной системы кибербезопасности Национального института стандартов и технологий (NIST), которые представляют собой комплексную рамочную схему для организаций при формулировании ими подходов к кибербезопасности.

При том, что совершенствование понимания ключевых концепций кибербезопасности будет последовательным процессом без ограничения по времени в деятельности комиссий, эта Рамочная система оценки кибербезопасности призвана предоставить регуляторам организованный подход, в основе которого - привлечение ответов компаний по широкому ряду и диапазону вопросов с последующей консолидацией таковых в единый целостный аналитический документ.

3. КАК ПОЛЬЗОВАТЬСЯ РАМОЧНОЙ СИСТЕМОЙ ОЦЕНКИ

Рамочная система оценки, представленная в Разделе 6, по своей структуре и принципам применения во многих аспектах схожа с системой ES-C2M2 - инструментом, наиболее широко применяемым компаниями для оценки собственными силами своих нормативов киберзащищенности, а также процессуально-должностных ведомственных инструкций. Задавая себе вопросы по тематике ключевых вопросов кибербезопасности, компании в состоянии оценить степень зрелости своего наличного потенциала кибербезопасности и выдать визуальный анализ своей защищенности в целом (рис. 1) Затем компании могут использовать эти результаты для выявления зазоров и формулировки плана мероприятий по устранению и нивелировке наиболее серьезных уязвимостей (рис. 2)

Иллюстрация 1: Визуальный анализ компании на основе самооценки ES-C2M2.

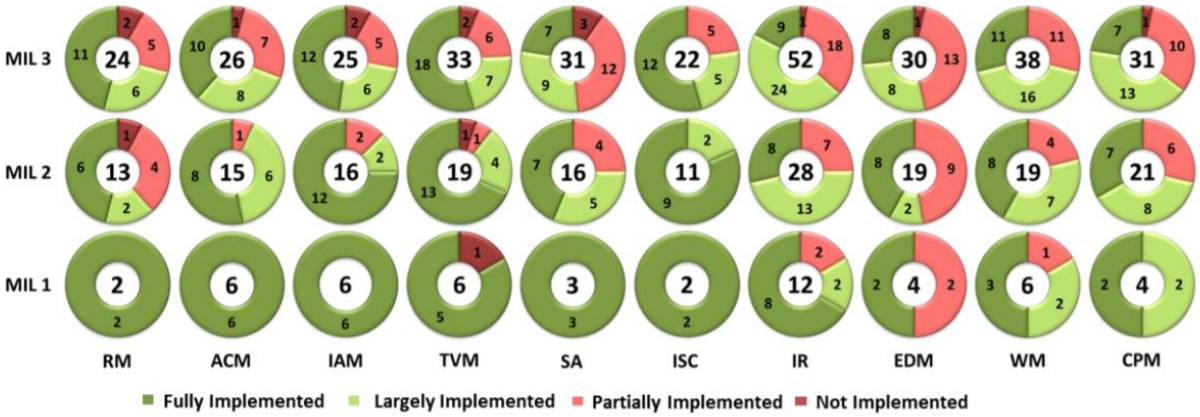


Иллюстрация 2: Компании используют результаты самооценки на основе ES-C2M2 для выявления упущений и верстки планов мероприятий.

	Inputs	Activities	Outputs
Perform Evaluation	1. ES-C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct ES-C2M2 Self-Evaluation Workshop with appropriate attendees	ES-C2M2 Self-Evaluation Report
Analyze Identified Gaps	1. ES-C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Cost-benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	Project tracking data

[1]

[1] Source of Images: Christopher, Jason. United States Department of Energy. "Cybersecurity Capability Model Update" *Helping Utilities with Cybersecurity Preparedness: The C2M2* April 23, 2015.

Рамочная система оценки весьма схожа по структуре с ES-C2M2. Обе они в значительной степени зиждятся на вопросах и анализе качественных параметров при оценке киберготовности. Однако, в противовес инструменту самооценки, рамочная система была создана для использования *регуляторами* с целью проведения опроса компаний для оценки их готовности. Во многих аспектах она действует аналогично аудиту по проблематике управления, формулируя вопросы к компаниям по процессуальним аспектам, институциональным структурам, критериям принятия решений, внутриведомственным инструкциям и пр. Это вызвано тем, что добротная система кибербезопасности в большей степени обусловлена культурой и заведомо упреждающей архитектоникой системы и организацией, нежели разовыми технологическими решениями.

Как и в случае с ES-C2M2, использование рамочной системы требует глубокого анализа группой сотрудников, которые владеют ключевыми концепциями кибербезопасности, и вот почему может потребоваться несколько пробных попыток, прежде чем персонал наработает навык уверенности. NARUC разработал упражнения-симулякры в помощь регуляторам при овладении этой методой оценки для того, чтобы получить предварительное представление о том, как работает эта система оценки прежде, чем она будет применена на практике.

Ниже представлено поэтапное руководство по использованию регуляторами Рамочной системы оценки кибербезопасности в целях генерирования и анализа качественных параметров данных, предоставляемых энергетическими компаниями. Для этого требуется использовать:
1) Первичный задел по кибербезопасности для государственных регуляторов, разработанный NARUC
2) Отдельная таблица Excel, которая прилагается к рамочной системе

ЭТАП 1. ВЫБРАТЬ 3+ ВОПРОСА ДЛЯ КОМПАНИЙ ПО КАЖДОЙ КЛЮЧЕВОЙ КАТЕГОРИИ

Рамка содержит 12 ключевых категорий, которые приведены ниже; они представляют собой ключевые компоненты, которые будут определять добротное функционирование систем кибербезопасности:
1. **Планирование**: означает, что реагирование не носит случайный, запоздалый или разобщенный характер
2. **Стандарты**: означает знакомство с наиболее оптимальными практиками и соблюдение требований
3. **Отчетность**: означает прозрачность и информированность
4. **Партнерские отношения**: означает "чем нас больше, тем мы сильнее "
5. **Закупки:** решаются вопросы цепочки поставок и инвестиционных приоритетов
6. **Кадры и должностные инструкции**: означает интегрированный подход к управлению рисками в масштабах предприятия целиком, включая людей
7. **Управление рисками:** означает взгляд на безопасность, при котором безопасность ставится выше соблюдения инструкций
8. **Внедрение:** указывает на наличие цикличного, продуманного процесса, который гарантирует эффективность
9. **Реагирование и восстановление:** для ситуаций, если/когда что-то пошло не так
10. **Процессуальные вопросы:** означает осведомленность в вопросах наиболее оптимальных практик и постоянное совершенствование
11. **Управление:** каким образом отчетность и прозрачность влияют на

подотчетность при исполнении служебных обязанностей

12. **Системы и рабочие циклы:** означает, что план является цикличным по своей природе и представляет собой постоянный процесс, а не разовую "галочку" в графе

Для применения этого инструментария регуляторам следует выбрать и задать компании три или более вопроса по каждой из **12 ключевых категорий**. Вопросы могут быть взяты из числа 107 вопросов Первичного задела, поскольку они были особо выбраны таким образом, чтобы дать в распоряжение регулятора достаточно информации по этим категориям.

Например, для категории “Планирование” регуляторы могут выбрать следующие три вопроса из Первичного задела:

1. Есть ли у вашей компании нормативный документ, стратегия либо должностная документация в вопросах кибербезопасности?
2. Проводилось ли рассмотрение вашего плана кибербезопасности на протяжении последнего года, и вносились ли в него изменения по мере необходомости?
3. Проводите ли вы регулярные тестирующие проверки того, как работает ваш план кибербезопасности? Проводится ли тестирование на внутриведомственной основе либо с привлечением третьих лиц?

Для категории “Поставки” такими вопросами могут быть:

1. Применяются ли критерии кибербезопасности при выборе смежников-поставщиков и оборудования?
2. Удостоверили ли документально и на независимой основе смежники-поставщики свои параметры кибербезопасности? Кто является удостоверяющей инстанцией и что служит подтверждением их квалификации?
3. Есть ли поставщики услуг из числа третьих лиц, чьи параметры кибербезопасности лежит за границами возможностей вашей организации с точки зрения мониторинга, понимания либо гарантии? Провела ли ваша организация расследование в отношении возможной уязвимости для вашей производственной деятельности, которую могут представлять собой такие услеги?

Регуляторам не следует ограничивать себя лишь тремя вопросами, либо номенклатурой вопросов, ограниченной Первичным заделом. Со временем NARUC рассчитывает на то, что инструментарий будет скорректирован и адаптирован под нужды и конкретные обстоятельства каждой конкретной комиссии; он и был спроектирован в расчете на такую гибкость и адаптивность.

ЭТАП 2. СОБРАТЬ ОТВЕТЫ КОМПАНИЙ ПО КАЖДОЙ КАТЕГОРИИ

На основе вопросов из раздела 1 регуляторы соберут и рассмотрят предоставленные компаниями ответы. Используя тот же пример, что приведен выше, образчики ответов по вопросам планирования могли бы выглядеть так:

1. Есть ли у вашей компании нормативный документ, стратегия либо должностная документация в вопросах кибербезопасности?

   У компании они есть, и таковые были в наличии с 2009 года, с тремя последующими поправками. Мы можем предоставить вам сводный вариант. Полная версия "Только для служебного пользования" доступна к ознакомлению без права выноса за пределы компании, при условии оформления обязательства о неразглашении содержания. Мы с готовностью пойдем на то, чтобы назначить время такого ознакомления для тех сотрудников комиссии, кому полагается знать эту информацию по служебной необходимости.

2. Проводилось ли рассмотрение вашего плана кибербезопасности на протяжении последнего года, и вносились ли в него изменения по мере необходимости?

   Наше последнее рассмотрение проводилось полгода назад и было одобрено Советом директоров. Не потребовалось внесения никаких принципиальных поправок в предыдущую редакцию 18-месячной давности, и были лишь уточнены подробности имплементации и графики.

3. Проводите ли вы регулярные тестирующие проверки того, как работает ваш план кибербезопасности? Проводится ли тестирование на внутриведомственной основе либо с привлечением третьих лиц?

   В соответствии с требованиями нормативных документов компании мы проводим тестирование некооторых компонентов нашего плана - как то, режима взаимопомощи в вопросах кибербезопасности - не реже раза в квартал. Мероприятия по обучению персонала и меры по реагированию подлежат внутриведомственному тестированию два раза в году. Выдерживается график соблюдения правил NERC. Внешние аудиты и тестирование защиты против взлома извне проводятся ежегодно. Полный график есть в наличии для ознакомления "Только для служебного пользования" без права выноса за пределы компании, при условии оформления обязательства о неразглашении содержания для персоналий комиссии, которым полагается знать эту информацию по служебной необходимости.

ЭТАП 3. ИСПОЛЬЗОВАНИЕ РАМКИ В ЦЕЛЯХ ОЦЕНКИ ГОТОВНОСТИ КОМПАНИЙ ПО КАЖДОМУ КЛЮЧЕВОМУ АСПЕКТУ

В рамках процесса рассмотрения, регуляторы будут рассматривать ответы компаний и давать оценку уровня готовности по каждой ключевой категории. Конкретно, регуляторы будут оценивать, где располагается данная компания по следующему спектру:

Для каждой области укажите, какого уровня ответ, на ваш взгляд, предоставили компании:

__ Неприменимо
__ Отсутствие осведомленности/проблема отвергается
__Только осведомленность о проблеме
__ Планируется внедрение

__ Частичное внедрение
__ Эпизод полного внедрения
__ Цикличное внедрение и совершенствование

Как и в случае с Уровнями индикации зрелости (УИЗ) в системе EC-C2M2, регуляторы будут выносить суждение касательно того, в какой степени компания продвинулась в каждой категории. Например, взяв в качестве примера планирование, регуляторы могут оценить, в какой степени реагирование со стороны компании носит случайный, запоздалый либо разобщенный характер.

Наблюдается ли ситуация, при которой в компании полностью отсутствует понимание того, почему планирование имеет важное значение, и/или же они целиком игнорируют сам вопрос как таковой (Отсутствие осведомленности?) Понимают ли они, что представляет собой планирование в вопросах кибербезопасности, но до сих пор не запланировали никаких мероприятий (только Понимание проблематики?) Или же они находятся на полпути к внедрению плана мероприятий, но еще не завершили его (Частичное внедрение)?

Оценка является субъективной, и потому рамка не диктует параметры того, где заканчивается один уровень и начинается следующий. Вместо этого регуляторам следует искать указатели того, (исходя из ответов, полученных на свои вопросы и на основе того, насколько они доверяют этим ответам), как далеко продвинулась компания в своей деятельности по каждой из ключевых категорий, а также задавать направление приоритетности последующих шагов.

При рассмотрении реакции со стороны компании у регуляторов могут возникнуть дополнительные вопросы, они могут быть не в полной уверенности относительно того, как оценивать компанию (частично ли они внедрили план мероприятий, либо целиком?), или же могут быть неудовлетворены некоторыми из ответов на заданные вопросы. Вот почему рамка включает в себя следующие два вопроса по каждой ключевой категории:

- Насколько вы уверены в готовности по вопросу кибербезопасности, исходя из ответов на данные вопросы?
- Какие аспекты вы хотели бы далее проработать совместно с компанией?

Эти уточняющие вопросы особенно важны не только для оценки текущего состояния компании, но и для понимания в целом общей картины положения компании в вопросах кибербезопасности. Если ответы, которые дает компания, не вносят ясность, либо есть разнобой во мнениях среди группы регуляторов в отношении того, как оценивать их нынешнее местонахождение, регуляторам следует определиться в отношении того, какая информация им требуется для достижения консенсуса и выйти с соответствующим запросом на компании.

ЭТАП 4. СВЕРСТАТЬ ОБЩИЙ АНАЛИЗ КОМПАНИИ НА ОСНОВЕ ОЦЕНКИ КАЖДОЙ КЛЮЧЕВОЙ КАТЕГОРИИ

Регуляторам следует задать уточняющие вопросы и добиться консенсуса в отношении того, как оценивать компанию по каждой из двенадцати категорий. В завершение этого процесса регуляторам надлежит свести воедино результаты своего анализа и рабочие

записи. Ниже приводится иллюстративный образчик того, как могут выглядеть некоторые разделы с черновыми заметками по первым двум категориям. Заметки ни в коем случае не претендуют на то, чтобы быть образцовой моделью - ни по объему, ни по содержанию, но, как представляется, они могут послужить примером того, как группа регуляторов может выйти на конкретную оценку:

1. Планирование: запланированное внедрение

Заметки регулятора: Представители компании сказали, что они верстают план, но не предоставили в своих ответах много конкретики. Представители регулятора колебались в своих оценках между "Осведомленность о проблеме" и "Планируется внедрение". Все-таки в компании есть сотрудник, ответственный за кибернетику, который работает над созданием плана, и они сообщили, что намерены привлечь консультанта со стороны для рассмотрения проблематики позднее в течение данного года. Исходя из этой информации представители регулятора сошлись во мнении, что речь идет о "Планируется внедрение", но мы планируем дополнительно контактировать с компанией в рамках следующего рассмотрения, чтобы получить более четкое представление о том, в какой степени они продвинулись в верстке и, позднее, внедрении плана.

1. Стандарты: Неприменимо

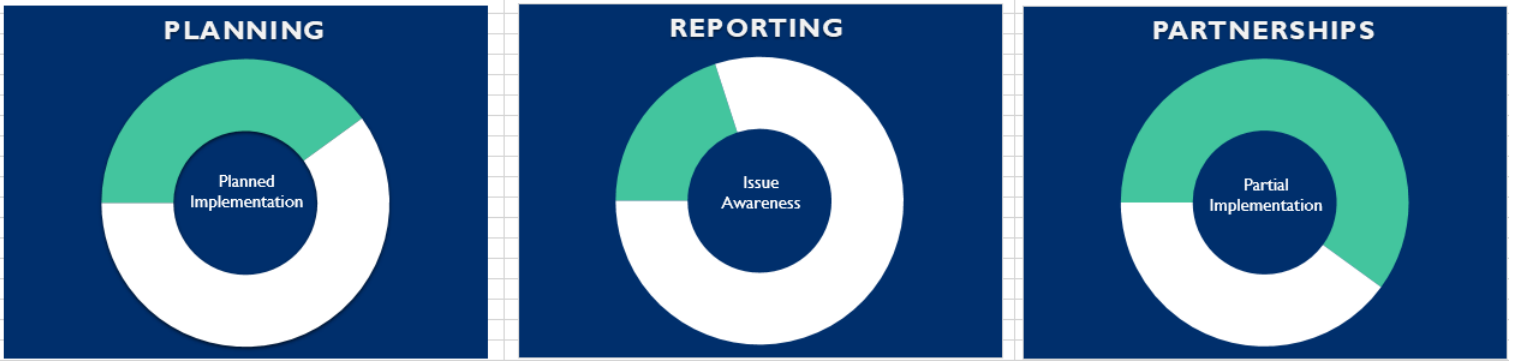
Заметки регулятора: В стране еще не были приняты стандарты, поэтому этот аспект не применим. Мы рассчитываем на то, чтобы работать с компаниями над верстской и внедрением базовых требований в следующем финансовом году.

ЭТАП 5. ИНСТРУМЕНТ ДЛЯ ВИЗУАЛЬНОГО ГРАФИКА

В отдельном документе в таблице Excel "Оценочная рамка кибербезопасности", которая прилагается к данному документу, USAID и NARUC разработали инструмент, позволяющий генерировать визуальную презентацию целостного анализа из Этапа 4.

Регуляторам остается лишь включить результаты рассмотрения в таблицу Excel, и будет сгенерирован полный визуальный график всех 12 категорий. Моментальный снимок трех таких категорий приводится ниже

Planning	Reporting	Partnerships
Not Applicable	Not Applicable	Not Applicable
Non-Awareness	Non-awareness/Dismissal	Non-awareness/Dismissal
Issue Awareness	Issue Awareness	Issue Awareness
Planned Implementation	Planned Implementation	Planned Implementation
Partial Implementation	Partial Implementation	Partial Implementation
Complete Implementation Iteration	Complete Implementation Iteration	Complete Implementation Iteration
Cyclical Implementation & Improvement	Cyclical Implementation & Improvement	Cyclical Implementation & Improvement
Planned Implementation	Issue Awareness	Partial Implementation



Примечание: Этот формат EXCEL сочленяется с графикой ES-C2M2 и будет применяться в качестве легкого для понимания наглядного пособия при оценке деятельности компании по всем ключевым категориям.

ЭТАП 6. ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ РАМОЧНОЙ ОЦЕНКИ ПРИ РАБОТЕ С КОМПАНИЯМИ В ЦЕЛЯХ ОПРЕДЕЛЕНИЯ ДАЛЬНЕЙШИХ МЕРОПРИЯТИЙ

Оценочная рамка кибербезопасности спроектирована таким образом, чтобы дать регуляторам представление о степени готовности компании. Если ES-C2M2 позволяет компаниям выявить свои внутренние точки уязвимости и недочеты, исходя из чего они разрабатывают план мероприятий, то оценочная рамка может содействовать регуляторам в понимании того, предпринимают ли компании действительно надлежащие меры. Если такие меры не предпринимаются, то рамка может послужить мотиватором и подспорьем компаниям в разработке своего собственного плана мероприятий на основе этих ключевых категорий.

Как таковая, рамка не только представляет собой инструмент мониторинга, но в особенности для стран, которые лишь приступают к разработке кибербезопасности, это также начало диалога с компаниями по тематике того, как наиболее оптимально планировать и проводить мероприятия в рамках цикличного процесса постоянного усовершенствования.

4. КОНТЕКСТ ИСПОЛЬЗОВАНИЯ РАМОЧНОЙ СИСТЕМЫ ОЦЕНКИ

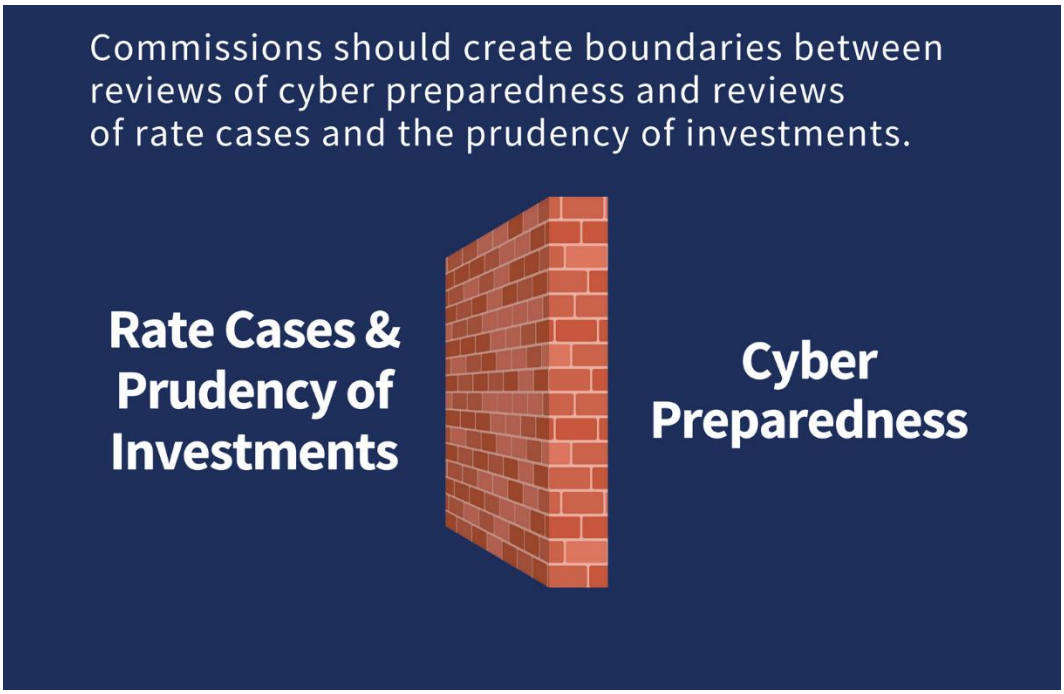
Регуляторам уместно задаваться вопросом - как эти инструменты оценки будут работать на практике. Опыт, накопленный экономическими регуляторами в США отличается

разнообразием, а потому не существует предписаний или образцового подхода как такового в вопросах применения. Тем не менее, в общем и целом, встречи проводились по месту деятельности компаний и вне контекста рассмотрения ходатайств о повышении тарифов либо ревизии обоснованности капиталовложений. Два параграфа, приводимые ниже, должны помочь дать регулятору представление о том, на что можно рассчитывать при проведении изначального анализа кибербезопасности компаний.

Анализ должен проводиться без излишней огласки и с учетом щепетильного отношения к сенситивной информации

Как упоминалось выше, регуляторы по преимуществу будут подходить к тематике кибербезопасности аналогично тому, как они подходят к прочим темам - то есть, формулируя вопросы и задавая планку ответов для компаний. Но при этом кибербезопасность представляет собой особые вызовы, которые требуют незначительной коррекции подхода со стороны регулятора. Во-первых, защита критической инфраструктуры тяготеет к сфере национальной безопасности. Поэтому регуляторы должны гарантировать, чтобы сбор сенситивной информации не был сопряжен с контекстом, в котором она может стать общедоступной - как, например, через посредство запроса в рамках Акта о свободе информации. Им надлежит также соблюдать осторожность и не запрашивать сенситивную информацию, сохранность которой они сами не в состоянии обеспечить - как то: планы компании по обеспечению кибербезопасности, конкретные графики, ФИО и должности сотрудников.

Соображения сенситивности и безопасности подразумевают, что к кибербезопасности следует подходить как к вопросу, требующему минимальной огласки и вне контекста слушаний по поводу повышения тарифов либо анализа программы капиталовложений. Вот почему в США многие регуляторы предпочли проводить такие рассмотрения вопросов кибербезопасности по месту производственной деятельности самих компаний, при полном понимании того, что будет соблюдаться конфиденциальность и сенситивные документы будут подлежать рассмотрению в режиме "ДСП без выноса с территории" либо в приватном порядке.



Такое разделение позволяет компаниям и регуляторам вести более откровенные и доверительные обсуждения. Возьмите, к примеру, случаи пересмотра тарифов, чреватые судебными тяжбами и не обязательно споспешествующие сотрудничеству и откровенности. Напротив - они представляют собой ристалища, где вопрос типа "Вы знаете, который сейчас час?" вероятнее всего повлечет за собой ответ "да", а не "10 часов". Решение о том, чтобы разделить эти два типа рассмотрений также позволяет уводить сенситивную информацию по кибербезопасности подальше от требований пролить на нее свет в контексте информирования общественности.

Планка обоснованных ожиданий при проведении изначальных рассмотрений вопросов кибербезопасности

Следует также подчеркнуть, что компании вероятнее всего находятся на различных стадиях зрелости в вопросах кибербезопасности. Крупные компании в США, например, уже свыше десяти лет обязаны придерживаться нормативов Защиты критической инфраструктуры (CIP) Североамериканской корпорации по надежности электроснабжения (NERC), в то время как прочие компании - как, например, мелкие распределительные компании - с большой степенью вероятности не задумывались над вопросами кибербезопасности вообще. Рамка спроектирована с прицелом на утилитарность и адаптивность для использования регуляторами при взаимодействии как с высокоискушенными, так и с неопытными компаниями.

Для компаний, которые до сих пор вообще не уделяли внимания кибербезопасности, первый круг вопросов может служить возможностью просто задать планку ожиданий. Поэтому регуляторам, быть может, стоит укоротить свои ожидания в отношении ответов компаний. В таких случаях, вопросы дадут возможность как компаниям, так и регуляторам совместно и наперед сформулировать цели и последующие шаги, а рамка затем может использоваться при будущих встречах для замера прогресса, которого добились эти компании в соответствии с этими согласованными следующими шагами.

5. РАМОЧНАЯ СИСТЕМА ОЦЕНКИ

При использовании данной рамочной системы оценки регуляторам надлежит следовать поэтапным инструкциям, перечисленным в Разделе 3

Рамочная система оценки кибербезопасности включает в себя 12 ключевых категорий:

- **Планирование:** указывает на то, что реагирование не носит случайный, запоздалый или разобщенный характер
- **Стандарты:** указывает на знакомство с важнейшими практиками и соблюдение требований .

- **Отчетность:** указывает на прозрачность, готовность к коммуникации, способность осуществлять обмен информацией
- **Партнерские отношения:** принцип «чем нас больше, тем мы сильнее».

- **Закупки: решаются вопросы цепочки поставок и инвестиционных приоритетов**
- **Кадры и внутренние регламенты:** указывает на интеграцию управления рисками на всех уровнях предприятия, включая сотрудников
- **Управление рисками:** взгляд на безопасность, при котором безопасность ставится выше соблюдения инструкций

- **Внедрение: указывает на наличие цикличного, продуманного процесса, который гарантирует эффективность**
- **Реагирование и восстановление: когда/если что-то пошло не так**
- **Процессуальные вопросы:** означает осведомленность в вопросах наиболее оптимальных практик и постоянное совершенствование
- **Управление:** каким образом отчетность и прозрачность влияют на подотчетность при исполнении служебных обязанностей

- **Системы и операции:** указывает на то, что план является цикличным и представляет собой процесс, а не просто единовременно проставленную «галочку».

По каждой из ключевых категорий укажите свое мнение относительно уровня ответов, предоставленных компаниями:

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Планирование: указывает на то, что реагирование не носит случайный, запоздалый или разобщенный характер

Какого уровня ответ был предоставлен компанией?

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Какие области вы бы хотели проработать с компанией глубже?

Sample Questions to Ask from the Primer

Стандарты: указывает на знакомство с важнейшими практиками и соблюдение требований

Какого уровня ответ был предоставлен компанией?

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Какие области вы бы хотели проработать с компанией глубже?

Sample Questions to Ask from the Primer

Отчетность: указывает на прозрачность, готовность к коммуникации, способность осуществлять обмен информацией

Какого уровня ответ был предоставлен компанией?

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Какие области вы бы хотели проработать с компанией глубже?

Партнерские отношения: указывает на понимание своей встроенности в общую сеть, способность опираться на принцип «чем нас больше, тем мы сильнее».

Какого уровня ответ был предоставлен компанией?

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Какие области вы бы хотели проработать с компанией глубже?

МТО и закупки: решаются вопросы цепочки поставок и инвестиционных приоритетов

Какого уровня ответ был предоставлен компанией?

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Какие области вы бы хотели проработать с компанией глубже?

Кадры и внутренние регламенты: указывает на интеграцию управления рисками на всех уровнях предприятия, включая сотрудников

Какого уровня ответ был предоставлен компанией?

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Какие области вы бы хотели проработать с компанией глубже?

Внедрение: указывает на наличие цикличного, продуманного процесса, который гарантирует эффективность

Какого уровня ответ был предоставлен компанией?

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Какие области вы бы хотели проработать с компанией глубже?

Реагирование и восстановление: когда/если что-то пошло не так

Какого уровня ответ был предоставлен компанией?

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Какие области вы бы хотели проработать с компанией глубже?

Процесс: более подробная информация о практиках компании (при необходимости модифицируйте)

Какого уровня ответ был предоставлен компанией?

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Какие области вы бы хотели проработать с компанией глубже?

Управление: указывает, как благодаря отчетности и прозрачности возникает ответственность за результат

Какого уровня ответ был предоставлен компанией?

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Какие области вы бы хотели проработать с компанией глубже?

Системы и операции: указывает на то, что план является цикличным и представляет собой процесс, а не просто единовременно проставленную «галочку».

Какого уровня ответ был предоставлен компанией?

__ Неприменимо

__ Отсутствие осведомленности/проблема отвергается

__ Только осведомленность о проблеме

__ Планируется внедрение

__ Частичное внедрение

__ Эпизод полного внедрения

__ Цикличное внедрение и совершенствование

Основываясь на ответах на эти вопросы, насколько вы уверены в готовности компании противостоять киберугрозам?

Какие области вы бы хотели проработать с компанией глубже?

С вопросами об этой публикации обращайтесь к Эрин Хаммел (ehammel@naruc.org) или Полу Стэку (pstack@naruc.org).

Национальная ассоциация регуляторов коммунальных предприятий (NARUC)
1101 Vermont Ave, NW, Suite 200
Washington, DC 20005 USA
Тел.: +1-202-898-2210
Факс: +1-202-898-2213
www.naruc.org