USAID
FROM THE AMERICAN PEOPLE

ОЦЕНКА ОБОСНОВАННОСТИ ИНВЕСТИЦИЙ В КИБЕРБЕЗОПАСНОСТЬ

Методические указания для органов регулирования энергетики

Май 2020 г.

Публикация подготовлена Национальной ассоциацией членов комиссий по регулированию коммунальных предприятий для рассмотрения Агентством США по международному развитию

ОЦЕНКА ОБОСНОВАННОСТИ ИНВЕСТИЦИЙ В КИБЕРБЕЗОПАСНОСТЬ
Методические указания для органов регулирования энергетики

Наименование проекта: Европейско-евразийское партнерство по кибербезопасности

Отдел-спонсор ЮСАИД: Бюро ЮСАИД по Европе и Евразии

Соглашение о сотрудничестве: AID – OAA-A-16-00049

Получатель: Национальная ассоциация членов комиссий по регулированию коммунальных предприятий (НАРУК)

Дата публикации: Май 2020 г.

Авторы: Элена Рагацци (руководитель проекта и редактор), при участии Альберто Стефанини, Даниэле Бенинтенди, Уго Финарди, Денниса К. Холстайна, под эгидой Исследовательского института устойчивого экономического развития Национального совета по исследованиям Италии (CNR-IRCrES)

National Association of Regulatory Utility Commissioners

Настоящая публикация осуществлена благодаря щедрой поддержке народа США, предоставленной через Агентство США по международному развитию (ЮСАИД). За содержание несет ответственность Национальная ассоциация членов комиссий по регулированию коммунальных предприятий. Содержание может не отражать мнения ЮСАИД и Правительства США.

Содержание

Перечень иллюстраций

Перечень таблиц

Перечень сокращений

APT	Advanced persistent threat
C2M2	Cybersecurity Capability Maturity Model
CAPEX	Capital expenses
CMM	Capability maturity model
CMMI	Capability maturity model integration
CNR	Consiglio Nazionale delle Ricerche (National Research Council of Italy)
EPRI	Electric Power Research Institute
GENCO	Generation operator
ICS	Industrial control system
IEC	International Electrotechnical Commission
IRCrES	Research Institute on Sustainable Economic Growth
ISA	International Society of Automation
IT	Information technology
KPI	Key performance indicator
ML	Maturity level
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OPEX	Operational expenses
PBR	Performance-based regulation
РУУ	Развитая устойчивая угроза
	Модель оценки уровня развития системы кибербезопасности
$З_{Кап}$	Капитальные затраты
	Модель оценки уровня развития
	Интеграция модели оценки уровня развития
НСИ	Национальный совет по исследованиям (Италия)
	Исследовательский институт электроэнергетики
	Оператор генерирующих объектов
АСУ ТП	автоматизированная система управления технологическими процессами
	Международная электротехническая комиссия
	Исследовательский институт устойчивого экономического развития
	Международное общество автоматизации
ИТ	Информационные технологии
КПЭ	Ключевой показатель эффективности
УЗ	Уровень развития
НАРУК	Национальная ассоциация членов комиссий по регулированию коммунальных предприятий
НЕРК	Национальная корпорация по вопросам бесперебойности электроснабжения
	Национальный институт стандартов и технологии
$З_{Тек}$	Текущие затраты
РППЭ	Регулирование по показателям эффективности

1 Общие положения и назначение «Методических указаний»

Настоящие «Методические указания» (МУ) разработаны для Национальной ассоциации членов комиссий по регулированию коммунальных предприятий при финансовой поддержке Агентства международного развития США (ЮСАИД) в рамках Европейско-евразийского партнерства по кибербезопасности.

В декабре 2016 г. ЮСАИД и НАРУК начали работу по кибербезопасности с целью передачи регулирующим органам энергетики Армении, Грузии, Молдовы и Украины технических средств и возможностей, позволяющих энергокомпаниям предотвращать и нейтрализовать кибератаки, а также совершенствовать и поддерживать общую энергобезопасность в регионе. Перечень ресурсов кибербезопасности, разработанных ЮСАИД и НАРУК см. в сноске.[1]

Регулирующие органы энергетики играют особую роль в сфере кибербезопасности. Хотя за реализацию мер кибербезопасности отвечают обычно операторы энергосистем, регулирующие органы обязаны добиваться, чтобы средства, вложенные в кибербезопасность, были рациональными, обоснованными и результативными. Цель «Методических указаний» -- содействие регулирующим органам в расчете тарифов на основе такого подхода к регулированию, который обеспечивал бы должный уровень кибербезопасности энергосистем, а также руководствовался современной литературой и практикой. «Методические указания» помогут органам регулирования ответить на следующие вопросы:

- Какие общие принципы регулирования лучше всего подходят для оценки обоснованности расходов на кибербезопасность?
- Как выявить затраты на кибербезопасность, провести их сравнительный анализ и установить соответствующие нормативы?
- Как определить адекватность мер противодействия киберугрозам?
- Как оценить рациональность затрат, связанных с выбранными мерами противодействия?
- Возможно ли оценить результативность расходов на кибербезопасность?
- Кто должен выявлять, сравнивать с нормативными показателями, измерять и оценивать меры противодействия в условиях различных режимов регулирования?

[1] Материалы, разработанные НАРУК при поддержке ЮСАИД, включают:
«Пособие по разработке стратегии кибербезопасности в Черноморском регионе», май 2017 г. (NARUC 2017a)
«Общие принципы оценки кибербезопасности для регулирующих органов Черноморского региона», сентябрь 2017 г. (NARUC 2017b)
Кроме того, Центр партнерства и инноваций (ЦПИ) НАРУК разработал нижеперечисленные материалы, ряд положений которых изначально создавались при поддержке ЮСАИД для Европейско-евразийского региона:
«Пособие по разработке стратегии кибербезопасности», октябрь 2018 г. (Cadmus Group 2018)
«Кибербезопасность. Вводный курс для органов государственного регулирования энергокомпаниями», январь 2017 г. (Keogh and Thomas 2017)
«Понимание готовности в кибербезопасности: Вопросы для энергокомпаний», июнь 2019 г. (Costantini and Acho 2019)
«Средства оценки готовности в кибербезопасности», июнь 2019 г. (Cadmus Group 2019)

Настоящие «Методические указания» — первый документ такого рода. Он наглядно демонстрирует лидерство ЮСАИД и НАРУК в расширении возможностей органов регулирования в поддержке и поощрению устойчивости энергосистем, которая достигается посредством обоснованных и эффективных капиталовложений в кибербезопасность на подведомственных предприятиях. В настоящих «Методических указаниях» изложены общие принципы, процессы и методика, но не содержится списков конкретных советов и готовых рецептов.

По мере того, как энергосистемы в регионе модернизируются, переводятся на цифровую основу и объединяются, в них обнаруживаются всё новые уязвимые точки, которые могут быть использованы при кибератаках. Атаки на электрические сети и системы могут иметь серьезные последствия для безопасности государства, его экономики и благосостояния населения. Они могут угрожать любому государству мира. Хотя настоящие «Методические указания» разработаны для региона Европы и Евразии, многие содержащиеся в них сведения имеют универсальную применение. НАРУК призывает регулирующие органы США и других стран изучить их применимость с учетом собственных внутренних обстоятельств и условий.

1.1 Благодарности

НАРУК выражает благодарность перечисленным ниже специалистам за ценные замечания, время и профессиональные знания, уделенные при разработке, пересмотре и редактировании настоящего документа.

Стефано Бракко, специалист по безопасности и распорядитель знаний, Европейское агентство по взаимодействию органов регулирования в энергетике (АВОРЭ)
Джеф Марке, главный экономист, управление государственного советника штата Миссури
Энн Рендал, уполномоченная Комиссии по коммунальным услугам и транспорту штата Вашингтон
Дэн Скриппс, уполномоченный Комиссии по государственным услугам штата Мичиган
Мохаммед Зумла, глава Уполномоченного органа по сетям и информационным системам (СИС), Управление рынков газа и электроэнергии
Пол Стек и Крисси Годфри, бывшие сотрудники НАРУК
Хишэм Чуэйки и Коллин Боровски, НАРУК.

Кроме того, НАРУК выражает благодарность за содействие нижеперечисленным государственным регулирующим органам:

Комиссия по регулированию государственных услуг (КРГУ) Республики Армения
Национальная комиссия по энерго- и водоснабжению (НКЭВС) Республики Грузия
Национальное агентство по регулированию в энергетике (НГАРЭ) Республики Молдова
Национальная комиссия по регулированию в сфере энергетики и коммунальных услуг (НКРЭКУ) Украины

Публикация выпущена при финансовом содействии Отделения энергетики и инфраструктуры Бюро по Европе и Евразии

2 Введение. Основы корректного применения «Методических указаний»

Кибербезопасность — расплывчатый термин, который зачастую используется в разных значениях. В глоссарии Национального института стандартов и технологий США (NIST) этот термин определяется очень широко посредством ряда взаимосвязанных терминов, а именно, «способность защищать или обеспечивать защиту использования киберпространства от кибератак», в то время как кибератака определена как «атака через киберпространство, направленная на использование корпорацией киберпространства с целью нарушения, отключения, уничтожения или злонамеренного управления вычислительной средой или инфраструктурой; либо нарушения целостности данных или хищения контролируемой информации»; при этом киберпространство названо «взаимозависимой сетью инфраструктур информационных технологий, включающей Интернет, телекоммуникационные сети, компьютерные системы и встроенные процессоры и контроллеры в критически важных отраслях» (NIST, n.d.b).

В настоящих «Методических указаниях» применяется концепция кибер¬безопасности согласно глоссарию «Вводного курса» НАРУК (Keogh and Thomas 2017, 32ff.), где дано следующее определение инцидента кибербезопасности: «злонамеренное действие или подозрительное событие, которое: (1) скомпрометировало или было попыткой скомпрометировать ПЭБ (периметр электронной безопасности) или ПФБ (периметр физической безопасности), или (2) нарушило или было попыткой нарушить работу КС-ЭС (кибернетической системы электрических сетей)».

Концепция кибербезопасности тесно связана с концепцией информационной безопасности, которая впервые была введена в стандарте BS7799 (первая редакция опубликована Британским институтом стандартов/BIS в 1995 году).[2] В основе информационной безопасности лежит обеспечение безопасности информации, а именно, сохранение конфиденциальности, целостности и доступности информации, гарантирующее, что информация не будет каким-либо образом скомпрометирована в случае возникновения критических нарушений штатного режима. При работе с критически важными системами самые разрушительные атаки, способные оказать наибольшее влияние на систему, — это такие атаки, которые нацелены на нарушение доступности. Они препятствуют реализации ряда функций, искажают или отключают их. Тем не менее, нарушение конфиденциальности и целостности данных, особенно данных удаленных систем, например, систем измерения или удаленного доступа к средствам защиты, автоматизации и управления, также может нанести значительный ущерб или быть средством подготовки более разрушительных атак. Затем вышли стандарты, ориентированные на кибербезопасность объектов критической инфраструктуры, системы управления и связи. В них содержались определения, в основном, согласованные с вышеприведенным.[3] При этом в каждом из них кибербезопасность определялась через рабочие термины соответствующей предметной области, иными словами, приводился ряд указаний, реализация которых гарантировала бы определенный уровень защиты рассматриваемых целевых систем. НАРУК подошла к этому

[2] Подробнее см. Приложение 2, раздел 5.

[3] Например, «Стандарты по защите критической инфраструктуры», разработанные Североамериканской корпорацией по вопросам бесперебойности электроснабжения (НЕРК) (NERC, n.d.), стандарт IEC 62443 Международной электротехнической комиссии (IEC) (IEC 2009), Общие принципы совершенствования кибербезопасности критической инфраструктуры NIST (NIST 2018) и пр.

вопросу сходным образом в издании «Кибербезопасность. Вводный курс для органов государственного регулирования энергокомпаниями». В настоящее время выпущена редакция 3.0 (Keogh and Thomas 2017).

Средства управления энергосистемой уязвимы для кибератак, которые могут серьезно повлиять на них и помешать их работе. Соответствующие события могут привести к нештатным режимам крупных сегментов энергосистемы и затруднить ремонт. Это, в свою очередь, имеет огромный социальный эффект, поэтому в мировой энергетике обеспечение защиты критически важных инфраструктур приобрело как никогда важное значение. Меры противодействия кибератакам разработаны, но операторам и директивным органам довольно сложно предвидеть затраты на внедрение и полезный эффект, что затрудняет реализацию этих мер. С учетом этого, большую роль могут сыграть регулирующие органы, поскольку они вправе устанавливать правила и предоставлять экономические стимулы для принятия мер противодействия угрозам в киберпространстве. Но тема эта сложная, поэтому регулирующие органы должны тщательно продумать вопрос рациональности инвестиций в кибернетическую сферу и механизм окупаемости через тарифы. Оценке подлежат как рациональность решений (выбор мер, которые будут реализованы), так и уровень затрат (не вкладывают ли операторы в кибербезопасность слишком мало или слишком много?).

Настоящие «Методические указания» задуманы как практическое средство, которое органы регулирования могут использовать для разработки таких тарифов, которые бы способствовали усилиям энергокомпаний по повышению своей готовности в сфере кибербезопасности и безопасности энергосистем. Данные рекомендации, однако, не следует рассматривать в качестве обязательных. Предлагаемые методы следует соотносить с конкретными обстоятельствами, в частности, с методикой регулирования коммунальных услуг в стране, а также с угрозами и уязвимыми местами энергосистемы, которые весьма разнообразны и постоянно изменяются. В данном разделе кратко изложены некоторые методы применения предложенных средств в рамках различных режимов регулирования.[4] Далее обсуждается, как следует разрабатывать стратегию кибербезопасности для противостояния постоянно возникающим угрозам.

[4] По аналогии, приведенные термины могут быть применены и в других отраслях энергетического сектора, например, в нефтегазовой отрасли).

2.1 Повышение уровня готовности к киберзащите в условиях разных режимов регулирования

Органы регулирования энергетики во всем мире играют решающую роль в установлении таких тарифов, которые уравновешивали бы интересы потребителя и одновременно давали энергокомпаниям возможность получать достаточную прибыль. Существуют разные методы расчета тарифов, каждая из которых имеет свои преимущества. Однако, несмотря на то что число угроз кибератак на энергосистемы очень быстро растет, на сегодня у органов регулирования нет практических средств, которые помогли бы им оценить, как соотносятся расходы энергокомпаний на повышение безопасности энергосистем с целью предотвращения кибератак с одной стороны, с обычными расходами на совершенствование инфраструктуры энергосистем, с другой.

Есть две распространенных методики расчета тарифов, которые применяют органы регулирования. Подход, направленный на поощрение инвестиций в кибербезопасность, можно применять с обеими методиками.

ЦЕЛЬ ДАННОГО РАЗДЕЛА...

…не в том, чтобы учить рыб плавать. Принципы, положенные в основу регулирования, хорошо известны органам регулирования.
Однако не самоочевидно, что различные средства, отрывки информации и подходы, изложенные в данном документе, могут выполнять разные функции в условиях разных режимов регулирования и по-разному использоваться заинтересованными сторонами. Более того, в мире постоянно возникающих разнообразных угроз и проблем различные средства следует согласовывать с постоянно меняющимися стратегиями.

1. Регулирование по показателям эффективности (РППЭ)

   Иначе называется «регулирование на основе стимулирования». Данная методика ориентируется, прежде всего, на измеримые плановые и фактические показатели.

2. Стоимость услуг

   В соответствии с этой методикой, органы регулирования определяют требования к доходам, т.е. к сумме, которую энергокомпания должна получить с потребителей, чтобы возместить расходы и получить разумную прибыль.

Реальность намного сложнее, чем подобная «черно-белая» картина, и содержит множество вариантов. Однако подобное упрощение помогает понять, что роль регулирующих органов может сильно различаться в разных условиях. В частности, эти две методики предполагают разные роли для органов регулирования (равно как и других действующих лиц) в отношении всех видов деятельности, описанных в настоящих «Методических указаний» (определение затрат, оценка затрат и количественные показатели).[5]

2.1.1 Регулирование по показателям эффективности (РППЭ)

Согласно методике РППЭ, оператор (распределительных сетей или магистральных сетей) должен достичь плановых показателей, которые устанавлены органом регулирования

[5] Потому этот момент и рассматривается не только в главе 5, посвященной нормативным подходам, но и здесь.

и которые определяют качество обслуживания. Для этого требуется защита от киберугроз. После того, как регулирующий орган установил плановые показатели, он действует по методу «кнута и пряника» в его самых разных формах: санкции за невыполнение, поощрение за перевыполнение, фиксированные или понижающиеся тарифы. Операторы самостоятельно выбирают наиболее эффективную стратегию выполнения плана с учетом системы стимулов, заданной органом регулирования, и собственных целевых показателей рентабельности.[6] Эффективная система стимулов — это система, которая позволяет вносить коррективы в случае «несостоятельности рынка» и делает защиту государственных и общественных интересов целью и для коммерческих компаний.[7] Регулирующий орган проверяет выполнение плана, не вникая в детали, касающиеся вложенных компанией средств и понесенных ею расходов.

По методике РППЭ регулирующий орган задает показатели оценки эффективности кибербезопасности (включая защиту от киберугроз и требования готовности) и устанавливает их минимальные значения, а затем применяет принятую систему стимулирования (например, снижение тарифов, если показатель не достигнут, или премирование, если оператор демонстрирует более высокую эффективность). Расходы на кибербезопасность распределительных и магистральных сетей не выделяются из других расходов на передачу и распределение электроэнергии. Компании сами вольны решать, как обеспечить требуемый уровень защиты, т.е. во что вложить средства, какой подход применить (управление рисками или соблюдение нормативных требований), а также каким процедурам и какому порядку следовать.

Регулирующий орган не выбирает, какие расходы компенсировать и не проверяет, соответствуют ли эти расходы представленным планам. Он просто смотрит, были ли достигнуты согласованные целевые показатели. Никаких планов капитальных вложений и аудитов не требуется, зато большое внимание уделяется эффективности, что придает особую важность методам ее измерения (характеристикам эффективности).

В целом, РППЭ рассматривается как средство надзора за рынком коммунальных услуг, которое позволяет корректировать несостоятельность рынка, не затрагивая полезные рыночные механизмы, и ориентироваться на показатели эффективности. Как правило, применение данной методики позволяет снизить затраты, относимые на потребителей, поскольку тарифы на передачу и распределение остаются низкими и меньше влияют на потребительскую стоимость. Однако как эта система повлияет на защиту от рисков кибербезопасности? Какие преимущества и какие сложности, связанны с этой системой?

[6] Стимулы могут быть и отрицательными, т.е. штрафами.

[7] Несостоятельность рынка — ситуация, при которой рыночная конкуренция не приводит к оптимальному распределению ресурсов. Возможность несостоятельности рынка обосновывает необходимость отраслевой политики, в частности, стимулов, регулирования, финансирования, государственных закупок и прямого вмешательства государства. Хорошим примером общественного блага (по отношению к которому возможна несостоятельность рынка) является оборона: по факту его предоставления (и понесенных расходов) невозможно лишить кого-либо возможности пользоваться благом, даже в случае отказа платить за него. Это полезная услуга, которая имеет стоимость, но ни одно действующее на рынке лицо не заинтересовано в ее оказании, поскольку не может продавать ее на рынке и покрывать затраты.

Результаты проекта применения Системы новых стандартов по безопасности к органам управления энергосистемой ЕС и другим критическим объектам (ESSENCE) (см. Приложение 2) явственно подтверждают сказанное. Они показывают, что экономический эффект избегания одной кибератаки полностью компенсирует расходы на обеспечение соблюдения стандартов. При этом выгоду получает всё общество (домашние хозяйства, компании-потребители и энергокомпании, хотя и в незначительной степени), тогда как все затраты несет оператор Именно для исправления такого положения дел и предоставления экономической выгоды компаниям, действующим во имя общественного блага, и предназначено стимулирование.

Рассмотрим «за» и «против» данной методики с точки зрения повышения уровня киберзащиты энергосистемы.

Как и в случае с любой другой стратегической целью, поставленной органом регулирования (например, повышение надежности или качества обслуживания), РППЭ оставляет разработку оптимальной стратегии кибербезопасности на усмотрение оператора: например, обеспечить соблюдение стандарта (и если да, то какого) или действовать по схеме управления рисками.

Таким образом, РППЭ не требует от органов регулирования лишних действий, что позволяет обходиться небольшим штатом сотрудников и, соответственно, обойтись небольшими затратами (которые в конечном итоге отражаются в тарифах для потребителей). Органы регулирования должны иметь минимальную компетенцию в области кибербезопасности (в основном для определения показателей эффективности), поскольку согласования инвестиции в кибербезопасность от них не требуется. Задача органов регулирования в данном случае — определять целевые показатели эффективности и стимулировать правильное отношение к кибербезопасности. Для этого можно привлекать сторонних специалистов и консультироваться с самими операторами. Наконец, в рамках данной методики органы регулирования могут изыскать пути обеспечения оптимального подхода к кибербезопасности, даже когда за нее отвечает другая организация.[8]

Несмотря на все перечисленные достоинства, следует помнить о некоторых сложностях и ограничениях, которые могут быть связаны с созданием стратегии кибербезопасности по данной методике. В целом, РППЭ требует, чтобы все заинтересованные стороны имели достаточно высокий уровень производственной зрелости и могли выступать в качестве конкурентоспособных участников рынка. Лучше всего предложенная методика действует в энергосистемах с большим опытом эксплуатации. На развивающихся же энергорынках ее следует рассматривать как идеальный подход на перспективу, внедрить который будет несложно по прошествии определенного времени, а не как неотложную новацию, которую необходимо внедрить немедленно и без оценки рисков, сопряженных с резкими изменениями.

В данном разделе:

- Вкратце рассмотрены варианты применения средств, доступных регулирующим органам согласно различным методикам регулирования.
- Представлены в деталях стратегии противодействия развитым устойчивым угрозам.
- Приведена сводная таблица рассматриваемых вопросов, в которой описаны роли регулирующих органов и компаний по двум методикам.

К вопросам кибербезопасности методика РППЭ пока не применялась. Здесь нет проторенных путей, это, скорее, неосвоенная территория. Дополнительную сложность вносит то, что регулирующие органы постоянно экспериментируют с показателями эффективности. В основе РППЭ лежит оценка показателей, поскольку именно они выступают инструментом совершенствования (речь идет об отношении к кибербезопасности, как оно отражено в государственной стратегии) и стимулировать компании, достигающие установленных показателей, посредством компенсации их усилий. Весьма важно определить

[8] Регулирующий орган, ответственный за кибербезопасность, определяет стратегию, ставит задачи и указывает цели, которые должны достигаться. Регулирующий орган, ответственный за тарифы в энергосистемах, строит систему стимулирования, побуждающую операторов к развитию в нужном направлении. Обратимся к процессу принятия решения (пункт 5.3, более конкретно, Рис. 10. Этапы 1 и 2 реализуются в основном регулирующим органом, ответственным за кибербезопасность, а этапы 3, 4 и 5 — в основном операторами энергосистемы. Пересмотр показателей по результатам обсуждается ими совместно.

соответствующие показатели и установить порядок их измерения или расчета, но это как раз является пока не освоенной территорией.

2.1.2 Регулирование по стоимости обслуживания («затраты-плюс»)

Согласно данной методике регулирования, тарифы покрывают все затраты компаний-поставщиков электроэнергии плюс справедливую прибыль на вложенный капитал. В модели «затраты-плюс» стимулирование повышения эффективности не предусмотрено. В связи с этим, существует несколько ее модификаций с различными вариантами «кнута и пряника», которые позволяют повысить заинтересованность операторов.

В данной методике расходы на кибербезопасность ничем не отличаются от других затрат и капиталовложений, которые должны быть согласованы с органом регулирования.

В рамках этой методики органы регулирования должны иметь подготовку (и компетентный штат) в сфере кибербезопасности, чтобы соответствующим образом согласовывать капиталовложения в кибербезопасность. Расходы на кибербезопасность должны быть определены, оценены относительно контрольных показателей и проверены. Введение на стратегии наращивания инвестиций в кибербезопасность может сопровождаться разработкой особой процедуры их согласования, которая упростит определение соответствующих затрат. К работе регулирующего органа могут быть привлечены другие компетентные государственные органы (если таковые имеются).

Показатели эффективности необходимы для отчетности, которая позволит усовершенствовать стратегию кибербезопасности и процедуру согласования инвестиций в следующем отчетном периоде, но не для того, чтобы ставить под сомнение отдельные статьи расходов оператора, которые были согласованны с органом регулирования ранее в ходе принятия текущего инвестиционного плана. Иными словами, в рамках данной методики регулирующий орган не имеет права сначала утвердить план инвестиций, а затем отозвать финансирование, поскольку подобная практика показала свою неэффективность. Как только регулирующий орган утвердил определенные капиталовложения, на него возлагается совместная с оператором ответственность за принятое решение. Таким образом, согласно методике «затраты-плюс», если инвестиции энергокомпаний были согласованы с органом регулирования, показатели эффективности не могут и не должны использоваться для оценки отдельных текущих инвестиций, но только для совершенствования стратегии кибербезопасности и лучшего выбора инвестиций в будущем.

2.1.3 Методики регулирования. Заключение

Разным методикам регулирования соответствуют разные роли органов регулирования и операторов. Их иллюстрирует Таблица 1.

Основой РППЭ являются показатели.

- **Регулирующий орган** определяет **показатели** – **цели**, которые должны быть достигнуты и которые определяются **числовыми значениями** показателей и **процедурами** получения необходимой информации и методики их расчета. Для этого регулирующий орган **запрашивает данные** и **проверяет** их **посредством** аудитов или **проверок.** Проверки устанавливают достоверность полученных данных.

- **Оператор (энергокомпания)** произвольно выбирает **стратегию кибербезопасности**, которая обеспечит компании достижения целей, заданных органом регулирования. Оператор определяет капиталовложения в соответствии с выбранной им стратегией и сравнивает их с контрольными показателями.

Методика регулирования «затраты-плюс», главным образом, построена на определении затрат, их анализе относительно контрольных показателей и на согласовании.

- **Регулирующий орган** определяет затраты, сравнивает их с контрольными показателями, согласует план и следит за его исполнением. Показатели эффективности используются исключительно в целях совершенствования будущих инвестиционных планов («планирование на основе фактов»).

- **Оператор (энергокомпания)** несет издержки и вкладывает средства, согласованные с органом регулирования, и использует показатели эффективности для оценки эффективности выбранной стратегии.

Таблица 1. Роль органов регулирования и операторов согласно методикам «затраты-плюс» и «регулирование по показателям эффективности»

	КТО (роли)	
ЧТО (действия)	**Затраты-плюс**	**РППЭ**
Определение стратегии кибербезопасности	☑ Директивный орган (общие цели) ☑ Регулирующий орган (практическая стратегия кибербезопасности) ☒ Оператор лишь следует стратегии кибербезопасности	☑ Директивный орган (общие цели) ☑ Регулирующий орган (показатели, определяющие данные цели) ☑ Оператор (практическая стратегия кибербезопасности)
Определение затрат	☑ Регулирующий орган (определяет затраты, включенные в инвестиционный план и подлежащие согласованию) ☑ Оператор составляет отдельный отчет по затратам на кибербезопасность исключительно по требованию	☒ Регулирующий орган не дает оценку инвестициям ☑ Оператор самостоятельно определяет наиболее экономически эффективные инвестиции для достижения целей
Сравнение затрат с опорными значениями	☑ Регулирующий орган (сравнивает затраты, включенные в план капиталовложений и подлежащие согласованию, с контрольными показателями) ☒ От оператора не требуется сравнивать затраты с контрольными показателями; тем не менее, он может это сделать с целью повышения вероятности согласования инвестиции	☒ Регулирующий орган не оценивает затраты ☑ Оператор определяет наиболее экономически эффективные инвестиции в плане достижения целей
Характеристики эффективности	☑ Регулирующий и директивный органы могут использовать контрольные показатели для сравнительного анализа разных типов инвестиций и выработки	☑ Регулирующий орган применяет установленные показатели, чтобы направить капиталовложения компаний в желательном направлении

ЧТО (действия)	КТО (роли)	
	Затраты-плюс	**РППЭ**
	более эффективной стратегии кибербезопасности на будущее. ☑ Оператор может использовать установленные показатели для внутреннего управления рисками	☑ Оператор может использовать установленные показатели для внутреннего управления рисками

■ Основная роль ■ Участие ■ Не имеет отношения

2.2 Новые угрозы требуют новых стратегий противодействия

Полного переченя мер противодействия киберугрозам, как и совершенной стратегии защиты энергосистемы, не существует. Новые угрозы возникают постоянно, а значит, чтобы их нейтрализовать, требуются новые или адаптивные стратегии защиты. Новые стратегии защиты следует учитывать в процессе разработки системы кибербезопасности, что является исходным этапом подхода к обеспечению кибербезопасности со стороны регулирующего органа.

Речь идет не только об освоении новейших средств защиты сетей, но и об изменении отношения компаний, которые, будучи потребителями и поставщиками важнейших услуг, должны принять самую активную позицию в защите киберпространства. Обычно, чтобы предотвратить кибератаки, компании развертывали специальные средства сетевой защиты, направленные на снижение рисков, обусловленных уязвимостью отдельных компонентов системы. Однако в данном случае разумнее применять упреждающую стратегию, то есть, действовать активно.

Специалисты подчеркивают, что самыми опасными являются так называемые «развитые устойчивые угрозы» (РУУ), поскольку чрезвычайно сложно как выявить их, так и организовать против них защиту.[9] Именно поэтому РУУ пользуются особой популярностью среди киберпреступников. Проще говоря, РУУ — это атака, в ходе которой неавторизованный пользователь получает доступ к системе и пребывает в ней в течение длительного времени, оставаясь необнаруженным. Действуя таким образом, хакеры получают постоянный доступ к секретным данным, хранящимся на серверах оператора, и могут реализовывать долгосрочные стратегии атак. Осуществление РУУ требует серьезных затрат и усилий со стороны хакера. Поэтому за киберпреступниками, осуществляющими подобные атаки, часто стоят организации, которые располагают средствами и квалифицированным персоналом и управляют целым рядом подобных стратегий и атак. Трудозатраты и время необходимы, чтобы собрать достаточный объем сведений, разработать метод запуска атаки этого типа и найти уязвимые точки для проникновения на объект.

Жизненный цикл кибератаки проходит по типу модели «килл-чейн» (*kill-chain*). Чтобы защититься от развертывания РУУ, необходимо внимательно проанализировать действия атакующей стороны на каждом этапов килл-чейн. Это непростая задача. Для ее решения требуются высокий уровень зрелости и системный подход. Согласно модели килл-чейн, чтобы атака была успешной, хакер должен пройти все восемь этапов ее жизненного цикла. Соответственно, чтобы не допустить успешного развития атаки, защищающаяся сторона

[9] Определение РУУ см. (NIST, n.d.a). Более подробно см. Huang and Zhu 2019; Huang and Zhu 2020.

должна либо сорвать ее на любом из восьми этапов, либо нарушить последовательность этапов. Восемь этапов (успешной) кибератаки приведены ниже.

1. *Первичная разведка*. Атакующая сторона определяет операционные системы, средства безопасности, прикладные программы, протоколы, адреса и другие рабочие характеристики системы.

2. *Первичная компрометация*. Атакующая сторона использует эксплойт или атаку для изучения средств киберзащиты и их взлом или обход. Для достижения компрометации могут применяться методы психологической манипуляции (англ. *social engineering*), фишинг, выпытывание и пр.

3. *Закрепление*. Атакующая сторона устанавливает (создает) постоянное присутствие в комплексе ИТ или эксплуатационной технологии (ЭТ) энергоблока, возможно, путем установки закладки (*back-door*), утилит или вредоносных программ для сохранения доступа.

4. *Повышение уровня полномочий*. Атакующая сторона обеспечивает более широкий доступ к системам и данным посредством хищения идентификационных данных, повышения прав доступа, эксплуатации уязвимостей программного обеспечения.

5. *Внутренняя разведка*. Атакующая сторона исследует другие системы и сети, чтобы построить схему информационно-вычислительного комплекса в целом, определить роли и обязанности ключевых специалистов по ИТ и ЭТ, а также найти интересующие ее ценные данные, необходимые для выполнения сценариев атаки.

6. *Расширение присутствия.* Атакующая сторона переходит от системы к системе в сетях ИТ и ЭТ, пользуясь возможностями совместного доступа, расписаниями задач, а также средствами и программами-клиентами удаленного доступа.

7. *Поддержание присутствия*. Атакующая сторона поддерживает постоянный доступ и развивает деятельность в сетях ИТ и ЭТ, пользуясь закладками и средствами удаленного доступа.

8. *Завершение операции*. Атакующая сторона достигает целей атаки, таких как хищение конфиденциальных данных или выполнение сценария, который отключает критически важные функции, нарушает искажает их исполнение или препятствует ему.

С целью предотвращения кибератак компании обычно развертывали традиционные средства сетевой защиты. К ним относятся, например, межсетевые экраны (фаервол), системы обнаружения и предотвращения вторжений, антивирусные программы и проч. Традиционные средства направлены на уязвимые места системы, которые входят в общую систему риска. Их развертывание является частью эшелонированной защиты (*defense-in-depth*), допускающей вероятность успешного вторжения. Здесь важно отметить, что долгий опыт свидетельствует о недостаточности данной стратегии для отражения РУУ. Хорошо обеспеченные и квалифицированные противники обладают терпением, навыками и ресурсами для организации многолетних атак, направленных на эксплуатационные сети, интеллектуальные электронные устройства и автоматизированные рабочие места. Для достижения своих целей они применяют самые современные средства и методы, специально разработанные для обхода существующих средств безопасности и маскировки присутствия.

Защищающейся стороне (сотрудникам отдела безопасности компании или единого оперативного центра безопасности) необходимо постоянно повышать уровень зрелости системы кибербезопасности, используя самые передовые средства и стратегии. Зрелая система кибербезопасности, кроме всего прочего, также способна действовать на

опережение, подбирать и эффективно эксплуатировать средства защиты как кибернетических, так и физических систем. Рекомендуется систематически проводить проверки с целью выявления уязвимых мест в текущих системах защиты с точки зрения эффективности отражения РУУ. Необходимо также своевременно собирать, устанавливать приоритетность и обрабатывать данные.

Подводя итог вышеизложенному, защищающейся стороне следует перейти от менталитета «осадной» обороны к активной профилактике, которая, в свою очередь, потребует средств реконструкции сценария вторжения на каждом из этапов килл-чейн. Реконструкция необходима для прогнозирования последующих действий атакующей стороны и создания стратегии их нейтрализации. Это позволяет нарушить последовательность килл-чейн, ослабить или полностью разрушать ее, ввести в в заблуждение атакующую сторону.

3 Оценка расходов энергокомпаний на кибербезопасность: определение затрат и сравнение их с контрольными показателями

ЦЕЛЬ ДАННОГО РАЗДЕЛА…

…помочь органам регулирования оценить, насколько эффективны меры проотиводействия киберугрозам и повышения безопасности энергосистемы, выбранные энергокомпаниями, и соответствует ли им объем выделенного финансирования. В разделе обсуждаются различные категории мер противодействия и приводятся сведения о сопутствующих затратах.

Определение ⟵ ⟶ Сравнительный анализ

Данный раздел поможет органам регулирования понять, насколько эффективны капиталовложения энергокомпаний в решение проблем кибер-безопасности с точки зрения повышения уровня безопасности энергосистемы.[10] Поскольку инвестиции в решение проблем кибербезопасности часто относят на другие категории расходов в силу их недостаточной обособленности, выделить такие расходы из текущих или общих инвестиционных затрат может оказаться непросто. В настоящем разделе перечислены разделы, в которых следует искать расходы на кибербезопасность с целью обоснования их необходимости для повышения возможностей кибербезопасности применительно к ресурсам, определенным в ходе оценки рисков. С точки зрения регулирующих органов, основной вопрос – это вопрос о **рациональности принятых решений**: насколько меры и средства безопасности, которые планируют ввести коммунальные предприятия, адекватны с точки зрения нейтрализации выявленных рисков?

В данном разделе:

- Представлены принципы определения и расчета затрат и подходы к этим вопросам.
- Описаны наиболее важные и широко применимые меры противодействия киберугрозам по каждой категории затрат.
- Рассмотрены сложности их определения.
- Приведена информация по сравнительному анализу с использованием контрольных значений; количественные данные проанализированы с точки зрения применимости в других условиях.

Существует обширная литература, посвященная актуальным мерам противодействия киберугрозам, но в ней ничего не говорится о том, как органам регулирования определять конкретные статьи расходов, выделенных на кибербезопасность в инвестиционных планах. В частности, в существующей литературе, чей краткий список помещен в «Техническом обзоре» в приложении к настоящему документу, не содержится никаких указаний на то, какие существуют статьи расходов на кибербезопасность (например, фонд оплаты труда, стоимость программного обеспечения и лицензий, модернизация технических средств). В большинстве публикаций излагаются общие теоретические принципы, приложимые ко многим сферам, но приведено крайне мало данных об их применении на практике. Наиболее конкретные сведения о расходах на кибербезопасность заимствованы из документа

[10] Термин «электросеть» (*grid*) в данном разделе включает магистральные и распределительные сети. Термин «сеть» (*network*) имеет более широкий смысл и используется как для магистральных и распределительных электросетей, так и для сетей коммуникационно-технологического управления.

«Новые стандарты безопасности», разработанного в рамках проекта ЕС «Контроль над сетями и другим критическими объектами (ESSENCE)».[11]

Оценка затрат на кибербезопасность требует сравнения с контрольными показателями. Первым этапом такого сравнения является определение базового уровня, т.е. минимальных категорий затрат. После обсуждения минимальных категорий затрат в разделе представлены сведения, призванные помочь органам регулирования в определении категорий расходов на кибербезопасность. Определив необходимые категории расходов, органы регулирования устанавливают **адекватный объект капиталовложений** и **проверяют,** соответствуют ли они размеру оператора, уровню угроз, которым подвергается оператор, и рыночным ценам

В разделах 3.1–3.4 вводятся общие принципы определения мер противодействия киберугрозам и демонстрируются возможные подходы их применения. В заключительных разделах 0—0 содержатся практические сведения, обсуждаются основные аспекты безопасности и некоторые контрольные значения расходов, которые могут быть использованы для сравнения. Более подробно см. Приложение 2.

3.1 От определения затрат к их расчету

Авторитетного справочника по затратам в области кибербезопасности в энергетике на сегодня не существует. Мероприятия, необходимые для защиты энергосистемы, эволюционируют и зависят от множества аспектов, в частности, ситуации в стране и уровня зрелости организаций.

Рис. 1. Последовательность анализа при определении и количественной оценке затрат

При определении затрат следует использовать подход, схема которого показанна на Рис. 1. Автоматизированные системы управления технологическими процессами (АСУ ТП)[12] как производителей электроэнергии, так и магистральных и распределительных сетей, имеют серьезные уязвимые места (2), которые используют в своих атаках киберпреступники. Анализ уязвимых мест и анализ угроз (1), связанных с конкретными сценариями атак, позволяет

[11] См. (CNR-IRCrES, n.d.)

[12] В настоящее время проблемы, свойственные АСУ ТП, присутствуют и во множестве платформ ИТ, которыми пользуются операторы.

понять, какие средства и узлы системы подвержены наиболее высокому риску (3). Стандарты, передовой опыт и соответствующие инструкции (4) помогают определить основные организационные и технические меры противодействия киберугрозам (5), необходимые для достижения такого уровня безопасности инфраструктуры, который мог бы нейтрализовать возможные атаки. Конечным результатом является оценка объема средств, необходимых для реализации (инвестиционные капитальные затраты —$З_{Кап}$) и для текущего обеспечения (годовые операционные затраты — $З_{Опер}$) принятых мер противодействия киберугрозам (6).[13]

Существуют два подхода к применению мер кибербезопасности в электросетях:

- Создание **контрольного списка действий**, направленных на устранение известных рисков, которого в обязательном порядке придерживаются операторы (**подход, основанный на регуляторных требованиях**).

- **Определение приоритетных мер** на основе систематического пересмотра ответа на вопрос: «Как еще более повысить уровень безопасности моей системы?» или, точнее: «Каким рискам подвержена моя система, и как обеспечить контроль над этими рисками?» (**подход на основе рисков**).

Названные подходы взаимно дополняют друг друга и каждый из них имеет свои достоинства. Первый подход, основанный на **регуляторных требованиях**, позволяет быстро и просто определить нужные меры противодействия, так как он опирается на действующие стандарты и рекомендации (например, «Стандарты по защите критической инфраструктуры» НЕРК, «Общие принципы NIST», IEC 62443,), в которых предложены различные меры и сопряженные с ними расходы. Упомянутые стандарты являются важнейшим источником сведений, приведенных в разделе 0, в котором рассмотрены основные статьи расходов, связанных с защитой энергосистем. С другой стороны, в основе **подхода на основе рисков** лежат защищаемые ресурсы, и этот подход помогает органам регулирования определить, какие капиталовложения будут наиболее эффективны и экономичны, исходя из того, что инвестиции нужны там, где риск выше.

Категории затрат определяются в общем виде с небольшими различиями для операторов разных типов. Однако невозможно опираться на общий метод, например, применять фиксированные показатели в следующих случаях:

- выбор правильного **критерия приоритетности** (с каких инвестиций начинать в стране, где бюджета недостаточно для покрытия всех потребностей);

- **количественная оценка** необходимых ресурсов для защиты энергосистемы или ее отдельных подсистем, например, национальных генерирующих компаний и магистральных линий электропередачи или региональных распределительных сетей.

- решение о том, какие меры противодействия относятся к базовому уровню и не нуждаются в стимулировании, так как являются повсеместными.

Оценка критически важных активов, требующих защиты (и оценка соответствующих инвестиций в обеспечение безопасности и затрат на ее поддержание) сложнее в сфере производства и распределения электроэнергии (из-за наличия нескольких операторов и ряда

[13] Совокупность затрат представляет сумму текущих затрат и доли инвестиционных затрат на соответствующий год.

ресурсов с присущим им высоким уровнем сложности). Выбор того, какие объекты инфраструктуры нуждаются в защите, определяется масштабом объектов (энергосистемы устойчивы в случае неисправностей небольших энергоблоков), режимом эксплуатации (холодный резерв имеет низкий приоритет независимо от объемов) и особенностей обслуживаемых ими социально-экономических систем. Оценку можно проводить после анализа «полезного эффекта», описанного в разделе 3.3. Наличие нескольких конкурирующих операторов в производстве и розничной продаже электроэнергии предполагает, что оценка должна проводиться не самим оператором, а директивными или регулирующими органами при определении стратегии кибербезопасности энергосистемы.

Оценка затрат включает расчет стоимости приобретения оборудования, например АСУ ТП, и связанных с ним систем резервного копирования, определение категорий специалистов, необходимых для реализации мер противодействия, а также их часовой ставки и требуемого количества часов работы. Совокупные затраты на первоначальное внедрение ($З_{Кап}$) следует дополнить текущими затратами на поддержание каждой из реализуемых мер противодействия киберугрозам.

Почти для всех мер противодействия совокупные затраты состоят из множества элементов, поэтому они не отражаются в бухгалтерском учете как одна позиция. Они включают не только аппаратное и программное обеспечение, консультации, обучение имеющегося и наем нового персонала, но и нематериальные активы, такие как новые правила и процедуры и перестройка систем. Во многих случаях меры противодействия киберугрозам могут быть частично скрыты (даже от оператора) в других позициях бухгалтерского учета более общего характера. Затраты на персонал, связанные с кибербезопасностью, как правило, крайне сложно выделить из общего фонда оплаты труда. На более детализированном уровне некоторые меры кибербезопасности основываются на процессах, то есть влекут за собой текущие, а не капитальные затраты. Соответственно, они не сопряжены с прямыми издержками, но могут повлечь за собой снижение эффективности, поскольку некоторые виды работ (например, требующие доступа персонала на режимные объекты) будут занимать больше времени. В других случаях для соблюдения требований стандартов понадобится привлекать более квалифицированных (и более высокооплачиваемых) сотрудников. Еще один пример — закупка товаров и услуг для модернизации энергосистемы. Приобретение более мощного и дорогого оборудования или программного обеспечения может дать полезный эффект с точки зрения защиты от кибератак, так как подобная техника зачастую снабжена встроенными средствами кибербезопасности; однако, эти встроенные средства обычно не относятся к расходам на кибербезопасность. С практической точки зрения можно предложить следующие соображения:

- Регулирующий орган сможет собирать сведения о расходах на кибербезопасность, только если они отделены от других расходов и капиталовложений. Регулирующий орган может сделать вывод о том, что оператор принял меры противодействия киберугрозам, проанализировав его документацию, в частности, сертификаты поставщика. Но дали ли эти меры экономический эффект, можно заключить, только если они были заранее предусмотрены.

- Оператора следует заранее поставить в известность о том, какая информация и на каком уровне детализации может быть затребована органом регулирования. Общий бухгалтерский учет может не дать всей требуемой информации.

- Оператор должен оказывать максимальное содействие органам регулирования в получении информации.

- Для оценки затрат на обеспечение кибербезопасности наиболее подходит метод предварительно оговоренных условий (см. раздел 5.2). В рамках этого подхода, заранее оговариваются как характер инвестиций в кибербезопасность, так и категории

затрат, под которые будет выделяться финансирование, а также сведения, необходимые для обоснования затрат.

3.2 Определение приоритетов

Изучая действующие стандарты, бывает трудно понять, какие требования важно выполнить незамедлительно, а какие можно отложить на будущее. Стандарты кибербезопасности позволяют организациям применять эффективные приемы обеспечения безопасности, чтобы свести к минимуму число успешных кибератак. Стандарт кибербезопасности обеспечивает комплексный, систематический и практический подход, гарантирующий определенный уровень защиты, если оператор реализует все требуемые меры противодействия киберугрозам. Тем не менее, не все мероприятия одинаково важны. Некоторые из них имеют обеспечительный характер, то есть без них другие меры противодействия не будут результативными.

Рис. 2. Приоритеты при стратегическом планировании кибербезопасности и защиты

Прежде всего, как показано на рис. 2, следует определить цели кибербезопасности и составить план их достижения. Для этого должны быть приняты конкретные стратегия и архитектура, организована структура управления реализацией стратегии и ее обеспечением.

На втором месте по приоритету стоят персонал и рабочие процессы. Важнейший момент — обеспечение персоналом. Во-первых, все сотрудники должны быть осведомлены о рисках кибербезопасности и о значении должного использования соответствующих ресурсов. Персонал должен быть достаточно квалифицированным, чтобы избегать таких киберугроз, как фишинг и вредоносные программы, либо нейтрализовать их воздействие, а также не допускать ненадлежащего применения техники, например, не пользоваться USB-носителями и аналогичными средствами для обмена данными, не подключать личные устройства к служебной сети и проч. Чтобы в полной мере воспользоваться преимуществами технологий и техники защиты, установленных на предприятии, необходим квалифицированный персонал. Следующая приоритетная проблема – как подобрать сотрудников, как руководить ими и осуществлять на ними надзор, поскольку сотрудники могут стать причиной нарушения безопасности не только из-за неправильного использования физических или информационных ресурсов, но и умышленно. На практике действия оператора по решению второй проблемы заключаются во вложении соответствующих средств в подбор персонала, его обучение и повышение его осведомленности, а также в надлежащие процессы контроля над информацией.

Высокую приоритетность также имеют ***критически важные ресурсы***, от которых зависит функционирование объектов критической инфраструктуры, которые часто называют

«жемчужины в короне».[14] Не менее важно защитить саму систему, включая сеть, к которой подключены различные устройства (например, средства управления и «интеллектуальные» счетчики), а не только устройства как таковые. Определить, какие именно ресурсы подлежат защите, можно по их функциям, посредством анализа топологии сети и каналов ее соединения с внешним миром. Этот последний шаг подразумевает адекватную защиту всех соответствующих объектов инфраструктуры. При этом следует избегать инвестиций, при которых затраты на защиту превышают потенциальный полезный эффект. Это соображение подчеркивает важность анализа полезного эффекта (см. п. 3.3) при определении приоритетности затрат.

Заключительное замечание по определению затрат: всё вышеописанное сопряжено с затратами. С затратами сопряжены безопасность физических ресурсов, обучение персонала на постоянной основе, привлечение *обученного* персонала, разработка и обеспечение соблюдения процедур, благодаря которым можно считать персонал «заслуживающим доверия». Органы регулирования должны помнить об этом и учитывать всю совокупность затрат. Проблема в том, что, если возмещать только капитальные затраты, у операторов может возникнуть соблазн игнорировать важные приоритеты, связанные с текущими затратами и затратами на обслуживание системы киберзащиты.

3.3 Анализ полезного эффекта

Оценить пользу от внедрения мер противодействия киберугрозам — то же, что оценить отрицательные последствия успешной кибератаки. Польза (полезный эффект) – это возможность избежать отрицательного воздействия атаки или свести его к минимуму.

Если затраты определяются посредством расчетов, оценка пользы требует анализа технических и экономических допущений. Почему органу регулирования или оператору электрической сети необходимо оценивать последствия успешной кибератаки? Зачем тратить силы на оценку полезного эффекта от внедрения мер противодействия, если эта оценка громоздка и методически сложна? Для этого есть две причины.

- *Подотчетность*: обоснование финансирования инвестиций в кибербезопасность для государства и общественности.
- *Определение приоритетов*: ограниченные средства должны направляться на ресурсы, связанные с высокой степенью риска, или на сценарии с высокой отдачей. Для этого необходимо оценить вероятность события, последствия этого события для энергосистемы, а тажке его экономические последствия на общество в целом.

[14] Хотя существует несколько определений объектов критической инфраструктуры, официальные источники едины в том, что энергосистемы входят в их число. Согласно Министерству внутренней безопасности США, «критическая инфраструктура — совокупность физических и кибернетических систем и ресурсов, которые настолько важны для США, что их отказ или разрушение могут оказать пагубное воздействие на физическую и экономическую безопасность или здоровье и благополучие населения» (DHS, n.d.). На сайтах Агентства национальной безопасности США и Агентства по кибербезопасности и инфраструктуре (CISA) представлен список из 16 критических отраслей инфраструктуры, в котором есть и энергетические системы (CISA, n.d.). В Европе принята Директива Совета Европы 2008/114/ЕС (EU 2008), действие которой распространяется на энергетику и транспорт. В ней установлен порядок определения европейских объектов критической инфраструктуры (ЕОКИ) и признания их таковыми, а также общий подход к оценке необходимости повышения степени их защиты.

Рис. 3. Последствия кибератаки — техническая оценка

Техническую оценку последний кибератаки иллюстрирует Рис. 3. Прежде всего, следует оценить воздействие на комплекс ИТ. Для этого необходимы знания в сфере кибербезопасности. Если имеющиеся меры противодействия не заблокировали атаку, следует оценить также воздействие на энергосистему. Для этого необходимы как знания в сфере кибербезопасности (для оценки скорости распространения и глубины проникновения атаки, а также времени, которое необходимо для ее блокирования) и инженерных знаний в энергетике (для оценки последствий для энергоснабжения).

Последствия кибератаки на энергосистему следует перевести на язык экономических показателей, которые можно будет использовать при анализе затрат и полезного эффекта (3.4). Оценка,[15] проиллюстрированная на Рис. 4, выполняется по трем описанным далее направлениям.

- *Последствия для операторов энергосистемы*. Обусловлены главным образом сокращением доходов (для всех поставщиков: энергокомпании, операторы распределительных и магистральных сетей), в связи с недоотпуском или недопоставкой потребителям электроэнергии. Чтобы уточнить оценку, необходимо учесть ущерб репутации и, возможно, повреждение оборудования.
- *Последствия для производственных энергопотребителей*. В данном случае убытки обусловлены остановкой производственного процесса (учитывается цена недоотпуска электроэнергии). При оценке следует учитывать также, насколько зависят от энергоснабжения отрасли тяжелой промышленности. Чтобы уточнить оценку, необходимо учесть ущерб репутации и, возможно, повреждение оборудования и расходных материалов.
- *Последствия для бытовых энергопотребителей.* Последствия выражаются в том, что потребители не могут должным образом обеспечить свои ключевые бытовые нужды или досуг.
- Следует также учитывать порчу потребляемой продукции. Чтобы точнее оценить экономические последствия, необходимо понимать, насколько важна для потребителей деятельность, зависящая от электроснабжения. Для этого можно провести опрос

[15] Оценка содержит ряд технических моментов, подробно описанных в Bruno et al. 2014. В отчете представлен также ряд полезных ссылок на статьи по методике и аналитике. На Рис. 4 основное воздействие выделено красным, вторичные воздействия — белым.

представительной выборки бытовых потребителей, сформулированный по методу «предпочтений».[16] Собранные данные затем преобразуются с помощью эконометрических моделей в стоимостные показатели.

Рис. 4. Последствия кибератаки — экономическая оценка

3.4 Затраты и полезный эффект от внедрения мер противодействия киберугрозам

Ниже рассмотрен подход к комплексному экономическому анализу мер кибербезопасности в электроэнергетике.[17] Задача состоит в том, чтобы оценить перспективность политики определенного типа, например, регулирования, требующего от операторов принятия определенных мер (например, заданных в государственном стандарте). Для этого затраты на внедрение мер сравниваются с возможным полезным эффектом от их внедрения для энергосистемы. С этой целью применяется методика анализа последствий (см. раздел 4.2), в частности, оценка последствий внедренных мер для определенного переменного показателя. Чтобы выделить воздействие на эту переменную именно политики, а не других факторов, следует сравнить две аналогичные ситуации, которые различаются только тем, присутствует ли в них регулирование или нет. Первая часть оценки касается *применения регуляторных требований*. Сравнивается следующее:

- *Ситуация в отсутствие регулирования*, в которой каждый оператор самостоятельно выбирает уровень защиты своей системы и вкладывает средства в соответствующие меры противодействия, которые составляют затраты на безопасность.
- *Ситуация наличия регулирования*, в которой регулирующий орган задает минимальный уровень защиты, например, посредством стандарта, либо перечня мер противодействия киберугрозе, либо установленным обязательным показателям эффективности. Предполагается, что в этом случае затраты на безопасность будут

[16] Т.е. основанный на методах, в рамках которого физическим лицам задают вопросы, содержащие прямую или косвенную экономическую составляющую.

[17] Более подробное изложение, в частности, поэтапные указания по применению данного подхода и упражнение на гипотетическом примере, приведены в Приложении 1.

выше. В противном случае не было бы необходимости в регулировании, а компании уже имели бы качественную стратегию защиты.

Однако меры безопасности значительно сложнее поддаются оценке, чем другие сферы регулирования. Причина этому в том, что в условиях регулирования, затраты на безопасность возникают в любом случае, но соответствующий полезный эффект проявляется только в случае кибератаки, которую удалось нейтрализовать или смягчить благодаря мерам безопасности. Чтобы оценить полезный эффект, необходимо провести вторую часть оценки, в которой учитывался бы сценарий атаки. Состояние энергосистемы оценивается в двух ситуациях: под действием кибератаки и при отсутствии кибератаки. Сочетание двух направлений оценки дает четыре сценария. В каждом из них, согласно табл. 2, подлежит расчету следующее.

- Затраты на текущее обеспечение средств безопасности. Они должны быть одинаковые во всех столбцах, за исключением затрат на неотложные меры реагирования на атаку (т.н. «затраты на восстановление»).
- Оборотные денежные средства, связанные с производством электроэнергии в различных ситуациях, например:
  - Затраты на производство (или закупку) электроэнергии и затраты на энергоснабжение (затраты в нормальных условиях с одной стороны – и затраты, когда из-за атаки возникают нарушения, способные повлиять на оперативное управление энергоснабжением). *В этом случае атака нарушает работу системы, но не приводит к отключениям.*
  - Воздействие перерывов в электроснабжении на экономику и общество. *В этом случае атака нарушает работу системы настолько значительно, что это приводит к отключениям.*

Таблица 2. Сценарии атак и анализ затрат и результатов

		Регулирование	
		ОТСУТСТВУЕТ. Каждый оператор внедряет меры противодействия кибератакам по своему усмотрению.	**ПРИСУТСТВУЕТ.** Операторы обязаны внедрить одни и те же меры противодействия.
Сценарий атаки	Серьезной атаки на систему **НЕТ**[18]	I — Регулирования нет – атаки нет	III — Регулирование есть – атаки нет
	Атака **ЕСТЬ**, она идет и может нарушить работу системы	II — Регулирования нет – атака есть	IV — Регулирование есть – атака есть

В Таблица 3 (ниже) перечислены стоимостные показатели и порядок их расчета. Во всех расчетах следует рассматривать не одного оператора, а энергосистему целиком. Это, конечно, несколько усложняет оценку, т.к. затраты и положительный эффект от принятых мер киберзащиты должны оцениваться с учетом событий во всей производственной цепочке,

[18] Под серьезной атакой подразумевается атака, которая ставит под угрозу работу системы и может обойти существующие меры противодействия.

даже когда в ней заняты несколько разных операторов. Анализ отдельной части системы не только неполон, но в некоторых случаях может дать результаты, вводящие в заблуждение. Например, атака может вызвать сокращение объемов производства электроэнергии и, как следствие, рост цен на электроэнергию на местном рынке. Вследствие этого, доходы отдельных компаний могут возрасти, и в результате у них появится соблазн использовать сложившуюся ситуацию, воспрепятствовав восстановлению нормальных условий эксплуатации.

Таблица 3. Экономические показатели для анализа затрат и полезного эффекта

1 Пока-затель	2 Сценарий	3 Категория затрат	4 Информация, полученная путем моделирования	5 Дополнительная информация из других источников	6 Показатель и тип информации
A	**I — Регулирования нет – атаки нет**	Годовые текущие затраты на энергоснабжение	Сколько стоят поставки электроэнергии без регулирования и без атаки?		Совокупные затраты на производство (либо закупочная стоимость) электроэнергии (производство+импорт), учитываемые в сценарии
B	**I — Регулирования нет – атаки нет**	Годовые затраты на средства безопасности		Сколько стоит эксплуатация средств безопасности?	Затраты на внедрение и обеспечение мер противодействия кибератакам при текущем уровне защиты от них. Включают как текущие затраты (персонал, материалы), так и амортизацию.
C	**II — Регулирования нет – атака есть**	*Отключений нет* Увеличение текущих затрат на энергоснабжение (в нештатном режиме)	Сколько стоят поставки электроэнергии в случае атаки?		Совокупные затраты на производство (либо закупочная стоимость) электроэнергии, задаваемые в сценарии, в сравнении с штатным режимом.[19]
D	**II — Регулирования нет – атака есть**	*Отключения есть* Затраты, обусловленные отключением	Какой регион затрагивает отключение энергоснабжения? Какова длительность отключения?	Каковы характеристики отключенных потребителей?	Затраты, обусловленные отключением, разделяются на затраты операторов энергосистемы, затраты других компаний и затраты домашних хозяйств.[20]
E	**II — Регулирования нет – атака есть**	Затраты на неотложные мероприятия.		Сколько будет стоить восстановление после атаки?	Данный показатель связан с проведением неотложных мероприятий по реагированию на атаку (затраты на восстановление).

[19] Прогнозируемое повышение затрат, обусловленное нештатным режимом энергоснабжения и необходимостью переключаться на более дорогостоящие источники или электростанции.

[20] Их величины зависят от характеристик потребителей, времени, места и длительности отключения. Здесь оцениваются в основном прямые и косвенные затраты, обусловленные перерывом в энергоснабжении. Их влияние зависит от типов потребителей электроэнергии. Таким образом, необходимо собрать много разнородной информации: количество затронутых отключением потребителей и их местонахождение, типы потребителей (промышленные разных масштабов, торгово-сервисные, бытовые, сельскохозяйственные), данные для оценки экономического и социального воздействия (стоимость недоотпуска электроэнергии. готовность принять ситуацию). См. пункт 3.3.

1 Пока-затель	2 Сценарий	3 Категория затрат	4 Информация, полученная путем моделирования	5 Дополнительная информация из других источников	6 Показатель и тип информации
F	**III — Регулирование есть – атаки нет**	Годовые текущие затраты на энергоснабжение	Сколько стоит энергоснабжение при регулировании в отсутствие атаки?		Совокупные затраты на производство (либо закупочная стоимость) электроэнергии (производство+импорт), задаваемые в сценарии.[21]
G	**III — Регулирование есть – атаки нет**	Годовые затраты на средства безопасности		Сколько придется потратить на поддержание систем безопасности при наличии регулирования?	Затраты на внедрение и поддержание мер противодействия кибератакам при уровне защиты от них, соответствующем требованиям регулирующих органов. Включает как текущие затраты (персонал, материалы), так и амортизацию материальных ценностей[22]
H	**IV — Регулирование есть – атака есть**	*Отключений нет* Увеличение текущих затрат на энергоснабжение (в период нарушения работы	Сколько стоят поставки электроэнергии при наличии регулирования в случае атаки?		Совокупные затраты (на генерацию или закупки) электроэнергии, учитываемые в сценарии.
I	**IV — Регулирование есть – атака есть**	*Отключения есть* Затраты, обусловленные отключением	Какой регион затрагивает отключение энергоснабжения? Какова длительность отключения?	Каковы характеристики отключенных потребителей?	Затраты, обусловленные отключением, разделяются на затраты операторов энергосистемы, затраты других компаний и затраты домашних хозяйств (см. раздел 3.3).[23]
J	**IV — Регулирование есть – атака есть**	Затраты на неотложные мероприятия.		Сколько будет стоить восстановление после атаки?	Затраты на проведение неотложных мероприятий по реагированию на атаку (затраты на восстановление).

[21] Данный показатель может быть выше, чем при отсутствии регулирования, так как могут требоваться средства резервирования или более трудозатратные процедуры.

[22] Предполагается, что затраты на безопасность будут выше, в частности, увеличится амортизация вследствие необходимости инвестиций для соблюдения требований регулирующих органов.

[23] Предполагается, что отключение можно предотвратить или, по меньшей мере, снизить обусловленные им затраты в отсутствие регулирования (благодаря уменьшению длительности отключения и числа отключенных потребителей).

Второй столбец Таблица 3 соответствует сценариям оценки, которые содержатся в Таблица 2. В третьем столбце показаны типы затрат (воздействия), которые должны быть рассмотрены. Это затраты на электроэнергию (производство, закупка и поставка) в случае, если атака нарушает работу системы, но не приводит к отключениям, и воздействие на экономику в случае отключения электроснабжения, плюс затраты на меры безопасности (при наличии или при отсутствии регулирования, включая затраты на восстановление). Значения следует рассчитывать для каждого конкретного случая. В частности, затраты на меры противодействия киберугрозам могут различаться очень существенно в зависимости от уровня реализации. Гипотетическая ситуация, в которой меры безопасности не принимаются, соответствует нулевым затратам на безопасность (показатель B, Таблица 3). Затраты на безопасность включают как годовые текущие затраты на управление и обслуживание, так и амортизацию инвестиций.

Информация для расчетов поступает из источников двух разных типов:

- Моделирование, показывающее, что произойдет в энергосистеме в заданной ситуации (время, дата, местоположение) при атаке и без нее. Модель позволяет получить значения перетоков электроэнергии и затрат на энергоснабжение, а также понять последствия отключения электроэнергии, вызванного нештатным режимом.

- Информация, поступающая из других источников, касающаяся категорий потребителей, затронутых отключением электроэнергии, а также затрат на технические и организационные меры безопасности.

Заключительная оценка состоит в сравнении разных показателей, как показывает

Таблица 4.

Таблица 4. Показатели, которые используются в оценке последствий

Расчет	Показатель	Дополнительные замечания
H + I + J	Что происходит при атаке при регулировании?	В эти показатели входит социально-экономические последствия отключений, затраты на поставки электроэнергии (если отключены не все потребители) и затраты на восстановление (затраты, связанные с мероприятиями по восстановлению штатного режима).
C + D + E	Что происходит при атаке в отсутствие регулирования?	
(H + I + J) - (C + D + E)	**ПОЛЕЗНЫЙ ЭФФЕКТ (измеряется в расходах, которые удалось избежать)**	**Отрицательное прогнозируемое значение (экономия затрат, снижение издержек и отрицательных последствий, благодаря более высокому уровню безопасности, достигнутому за счет регулирования).**
F - B	Увеличение затрат на безопасность в связи с введением регулирования	Включает ежегодные затраты и амортизацию капиталовложений. Теоретически, показатель B может иметь нулевое значение в случае «отсутствия защиты». Прогнозируемое значение – положительное.

Расчет	Показатель	Дополнительные замечания
G - A	Приращение затрат на энергоснабжение в связи с введением регулирования	Это возможно, если требуются дополнительные резервные мощности или необходим переход на более жесткие условия эксплуатации.
(F + G) - (A + B)	**ЗАТРАТЫ на выполнение требований регулирования**	**Прогнозируемое значение положительное (повышение затрат на безопасность).**

3.5 Руководство системой кибербезопасности

Анализ и обсуждение основных типов мер безопасности помогает регулирующим органам уточнить категории расходов в инвестиционных планах и оценить приемлемость и оправданность капиталовложений энергокомпаний в кибербезопасность.

Международные стандарты безопасности, передовой опыт и основные принципы работы (обычно связанные с безопасностью АСУ ТП в энергетическом секторе) определяют технические требования в различных областях обеспечения безопасности. В стандартах перечислены единые инженерные или технические критерии, технологии и методы работы.

О сложности контроля за процессами производства, передачи и распределения электроэнергии свидетельствует огромное число стандартов по безопасности энергосистем, при этом области обеспечения безопасности классифицируются по-разному. Ясно, что такой быстрый и хаотичный рост числа различных стандартов и руководств по кибербезопасности электроэнергетических систем, мешает энергокомпаниям понять, что именно от них требуется. Кроме того, это создает трудности для тех, кто хочет рассказать о своих параллельных усилиях в этой области. В проекте ESSENCE подчеркивается, что в случае, когда закон не предусматривает обязательного использования конкретного стандарта, обычной практикой является мягкое соблюдение положений одного или нескольких стандартов, однако в большинстве случаев стандарты, регулирующих производство и передачу электроэнергии, далеко не одно и то же. Хотя правила, которым должны следовать энергокомпании, не столь различны, классификация мер безопасности совпадает не полностью. Различия в стандартах безопасности ведет к различиям в мерах противодействия кибератакам, которые к тому же по-разному классифицируются. Полный список типов мер безопасности и сравнение принятых классификаций даны в Приложении 2.

В следующих разделах описаны наиболее характерные типы мер противодействия кибератакам. Перечень заимствован, главным образом, из стандарта ISA-99.02.01-2009 Международного общества по автоматизации (ISA), позднее положенного в основу стандарта IEC 62443-2-1. Он не претендует на полноту и преследует две цели. Первая – провести обзор мер противодействия киберугрозам, которые следует использовать, чтобы существенно повысить уровень безопасности. Вторая — познакомить читателей с разнообразием применяемых энергокомпаниями стандартов безопасности.

3.5.1 Организационное обеспечение системы кибербезопасности

В силу актуальности этого вопроса для стран с переходным типом экономики, затраты на организационное обеспечение системы кибербезопасности следует упомянуть отдельно. Основные затраты операторов на повышение уровня безопасности связаны с актуализацией и организационными процессами (принципы, регламент и распоряжения по

организации работ) и подготовкой персонала (осведомленность и способность своевременно реагировать).[24]

По своей природе затраты на организационное обеспечение могут быть не столь очевидны, как затраты на другие меры противодействия. Тем не менее, они могут составлять существенную долю совокупных затрат, особенно в случаях, когда необходимы шаги по повышению уровня кибербезопасности. В разделе 3.2 указано, что первоочередная задача – создание структуры управления, и лишь затем следует решать задачи, связанные с персоналом и внутренним регламентом. Необходимость актуализации и обеспечения рабочих процессов и уровня подготовки персонала (осведомленность, своевременность и т.д.) влечет дополнительные расходы, как будет показано на практических примерах в следующем разделе. Отсутствие соответствующей системы руководства может пагубно сказаться на эффективности систем безопасности, а поведение плохо обученного персонала может свести их полезный эффект к нулю. Хорошо проработанный регламент сам по себе является мерой противодействия киберугрозам. Таким образом, уровень развития в немалой степени определяется уровнем руководства в области кибербезопасности и является необходимым условием ее эффективности.

Связанные с общим руководством меры безопасности, основные категории которых даны в Таблице 5, как правило, отличаются низкой масштабируемостью. По этой причине, крупным и средним предприятиям (крупным электроэнергетическим компаниям, операторам магистральных сетей и проч.) следует создать отдельное подразделение, отвечающее за кибербезопасность. При этом малые предприятия могут воспользоваться услугами объединенного центра обеспечения безопасности.

[24] Это четко обозначено в соответствующих стандартах. Согласно НЕРК, «цель программы управления безопасностью (ПУБ) – гарантировать, что организация разрабатывает и обеспечивает выполнение принципов, стандартов и внутреннего регламента, охватывающих все аспекты системы безопасности» (NERC 2016, 4). В документе NIST «*Основные принципы повышения уровня кибербезопасности ключевых объектов инфраструктуры*» рассматриваются вопросы руководства системой кибербезопасности и дается следующее определение: «Принципы, регламенты и технологии, предназначенные для руководства организацией и контроля за соблюдением требований в нормативно-правовой сфере, в сфере экологии, эксплуатации и управления рисками, хорошо усвоены и определяют систему контроля за рисками, связанными с кибербезопасностью» (NIST 2018, 25–26).

Таблица 5. Области применения мер противодействия, связанных с руководством системой кибербезопасности

Программы обеспечения безопасности. Указания, относящиеся к концепции, целям, задачам, стратегиям, направлениям развития и планам систем безопасности.
Организация системы безопасности. Требования, касающиеся внутренних и внешних (относящихся к сторонним организациям) функций, обязанностей и структур, обеспечивающих безопасность.
Принципы обеспечения безопасности. Положения, касающиеся принципов, плана действий и регламента по обеспечению безопасности.
Управление рисками. Требования, относящиеся к принципам и методике управления рисками.
Управление активами. Положения, касающиеся управления активами с целью обеспечить их защиту и сохранность.

3.5.2 Укрепление системы

Укрепление системы — это процесс ее проверки и повышения надежности. Реализуется путем применения особых технологий, позволяющих уменьшить площадь участка, не защищенного от возможного нападения. Поскольку большинство систем до сих пор уязвимы из-за возможности внешнего доступа, их укрепление необходимо, даже при наличии таких средств безопасности, как антивирусные программы и блокировщики шпионских программ. Возможные пути усиления защиты: отбор необходимых услуг, регулярное обновление программного обеспечения, оптимизация системных настроек, отключение ненужных пользователей, закрытие сетевых портов, установка систем обнаружения и предотвращения вторжений, применение межсетевых экранов. Затраты на усиление защиты могут распределяться по разным категориям расходов, как показано в Таблица 6.

Некоторые термины (например, управление конфигурациями или бесперебойность деятельности) не требуют пояснений. Однако значение других целесообразно прокомментировать.

- *Предотвращение внедрения вредоносных программ* требует наличия всесторонней и актуальной информации об уязвимых участках системы на фоне имеющихся угроз (кто атакующая сторона, как она предпочитает действовать, характерные методы атак и пр.).
- *Криптография* — сфера, в которой технологический прогресс сделал огромный рывок и дал возможность взламывать коды криптографических схем, еще недавно считавшихся абсолютно надежными.
- *Управление доступом*, как физическим, так и электронным, должно строиться с учетом различных категорий персонала, имеющим доступ на производственные объекты, например, работники предприятия, обслуживающий и ремонтный персонал, руководство предприятия, администраторы, бизнес-контролеры и аудиторы.

- *Обеспечение и повышение уровня соблюдения нормативов* требуют знаний о действующих стандартах и руководствах, которые планируется использовать. Комплексная база действующих стандартов постоянно обновляется.
- *Сетевая безопасность* реализуется отдельно от *безопасности объекта* (т.е., общестанционный контроль). Это особо подчеркивается в стандарте IEC 62443, ключевой концепцией которого является оценка каналов передачи данных и информации в модулях разного назначения сложной АСУ ТП.[25]

Очевидно, что большинство перечисленных категорий не являются полностью независимыми, но взаимосвязаны. Так, взаимосвязаны организация охраны труда и техники безопасности, уровни безопасности, знания персонала о текущем состоянии кибербезопасности и предоставление доступа на объекты.

Таблица 6. Типы затрат на укрепление системы

Предотвращение вредоносных программ	Охрана труда и техника безопасности
Управление конфигурациями	Физическая и экологическая безопасность
Криптография и управление ключами	Управление непрерывностью бизнес-процессов
Резервное копирование и восстановление	Управление в нештатных ситуациях
Безопасность сетей и объектов	Обеспечение и повышение уровня соблюдения нормативов
Приобретение, развитие и техническое обслуживание систем	Управление доступом

3.6 Оценка затрат на меры противодействия киберугрозам

В литературе имеется крайне мало данных о расходах, связанных с соблюдением действующих стандартов по кибербезопасности. Исключением является проект ESSENCE, поскольку в нем приводится расчет затрат, связанных с ключевыми организационными и техническими мерами повышения безопасности объектов инфраструктуры (генерация и передача), на примере конкретных ситуаций (Calabrese, Finardi, Ragazzi 2014). В данном разделе представлены результаты расчетов с максимальной детализацией, которая возможна с учетом конфиденциальности данных. Рассмотрена их применимость в странах с экономикой переходного типа, например, в странах Черноморского региона.

[25] Более подробное описание зон безопасности дано в Приложении 2: Сводка основных результатов проекта ESSENCE. Раздел 2.

3.6.1 Расчетные затраты в проекте ESSENCE

Оценка затрат на примере конкретных ситуаций и их экстраполяция на все рассматриваемые страны дана в Таблица 7.[26]

В обоих случаях рассматриваются две ситуации: затраты при гипотетическом сценарии, когда стандарты безопасности вообще не применяются (затраты начинаются с нулевого уровня), и затраты, начиная с текущей ситуации, в целях принятия дополнительных мер безопасности (приращение затрат). В первом столбце дана справочная информация, показывающая долю сделанных ранее капиталовложений, поскольку ни одна энергосистема не эксплуатируется без защиты. Эта информация интересна тем, что дает основу для оценки масштабируемости в других ситуациях.

Принятая методика позволяет рассчитать денежные потоки, связанные с внедрением и поддержкой стандартов безопасности. Одна часть указанных затрат, особенно, затраты, связанные с разработкой, приобретением и внедрением мер кибербезопасности, является инвестиционными, то есть разовыми затратами ($З_{Кап}$), которые производятся при первоначальном внедрении. Другая часть, особенно, затраты, связанные с поддержанием мер безопасности, — это ежегодные текущие затраты ($З_{Тек}$).

Таблица 7. Совокупные затраты на внедрение и обеспечение мер противодействия киберугрозам на примере конкретных ситуаций в рамках проекта ESSENCE (тыс. евро)

	ЗАТРАТЫ С НУЛЕВОГО УРОВНЯ		ПРИРАЩЕНИЕ ЗАТРАТ	
	$З_{Кап}$	$З_{Тек}$	$З_{Кап}$	$З_{Тек}$
Передача электроэнергии, Польша	26 016	5 016	7 486	2 457
Производство электроэнергии, Италия	27 730 – 52 480	6 480 – 11 980	20 000 – 40 000	3 480 – 5 980

Источник: (Calabrese, Finardi, and Ragazzi 2014)

Так как по Италии рассматривалось только производство электроэнергии, то согласно пункту 3.1, для оценки числа электростанций (принадлежащих нескольким операторам), подлежащих защите, было необходимо принять ряд допущений. Напротив, при изучении

[26] Более подробная информация (при детализации с учетом сохранения конфиденциальности особо важных данных) о сценариях атак, выбранных мерах противодействия и расчетах затрат дана в отчетах по разбору конкретных ситуаций.
Пример Италии: (Angeletti et al. 2014). Пример Польши: (Bartosewicz-Burczy et al. 2014).

примера Польши (только национального оператора магистральных сетей), в оценку включалась защита всей национальной магистральной сети. Из этого ясно, почему в Таблица 7 для Польши дана точная оценка: все магистральные сети находятся в ведении одного оператора. И наоборот, для Италии приведен диапазон оценочных значений, так как система энергогенерирующих мощностей находится в ведении нескольких генераторных компаний.[27]

3.6.2 Как применить результаты проекта ESSENCE в иных условиях?

Понять, какие трудозатраты требуются для обеспечения необходимого уровня защиты энергосистемы нелегко, т.к. это зависит от множества факторов, определяемых местными условиями. Вот почему невозможно рассчитать затраты по формуле с фиксированными параметрами. Тем не менее, расчеты, использованные для получения совокупных значений (см. «Таблица 7»), позволяют определить ряд показателей, представляющих общий интерес. Что касается затрат на осуществление руководства, в Таблица 8 перечислены ресурсы, необходимые для реализации комплексного плана.

[27] Для понимания масштаба исследований, проведенных на примере этих стран, напомним, что население Италии 60 млн., а Польши 38 млн. человек.

Таблица 8. Ресурсы, необходимые для реализации плана по руководству системой кибербезопасности (евро или численность персонала)

Область	Описание	Трудозатраты (внедрение)	Трудозатраты (выполнение)
Программа по безопасности	• Группа руководителей высшего звена разрабатывает принципы организации и проведения программы обеспечения безопасности.	• 4 человека	• 1 человек
Обеспечение программы безопасности	• Группа технических специалистов, отвечающих за **внутреннюю** систему обеспечения безопасности.	• 6 человек	• 1 человек
	• Группа технических специалистов, отвечающих за **внешние контакты** со сторонними организациями.	• 6 человек	• 1 человек
Концепция безопасности	• Группа специалистов в области АСУ ТП и ИТ, разрабатывающие концепцию, стандарты и регламенты обеспечения безопасности.	• 3 человека	• 2 человека
Управление рисками	• Консультант по вопросам безопасности, работающий на контрактной основе. • Группа экспертов.	• 4 человека на полставки	• 90 000 евро/год • 2 человека на полставки
Управление активами	• Консультант по вопросам безопасности, работающий на контрактной основе. • Автоматизированный технический комплекс управления активами (по желанию).	• 500 000 евро (крупный или средний оператор)	• 90 000 евро/год • 2 человека

Источник: (Angeletti et al. 2014)

Данные по трудозатратам относятся к численности необходимого персонала (штатные сотрудники) и (или) затратам в евро на приобретение товаров и услуг (в ценах 2014 г. на примере Италии). В таблице приведены как первоначальные затраты для реализации плана, так и ежегодные, необходимые для его дальнейшего выполнения. Стоит напомнить, что затраты на руководство отличаются низкой масштабируемостью, поэтому малым предприятиям рекомендуется обращаться в объединенный центр обеспечения безопасности.

Исследование на примере Италии позволяет также получить некоторую информацию по затратам, необходимым для защиты стандартного энергоблока 380 МВт (Таблица 9). Эту информацию можно использовать для оценки затрат на защиту генерирующих объектов, но только после оценки масштабируемости (прежде всего, применительно к операторам генерирующих мощностей, в ведении которых находится несколько энергоблоков).

Таблица 9. Затраты на оборудование и программное обеспечение для защиты объекта и сети стандартного энергоблока 380 МВт (евро)

	$З_{Кап}$ (затраты на оборудование и программное обеспечение)	**$З_{Тек}$**
Требования к сети	370 000	20 000
Требования к объекту	125 000	90 000
Всего	495 000	110 000

Источник: (Angeletti et al. 2014)

Что касается магистральных сетей, исследование на примере Польши показало, что затраты на защиту подстанции составляли 151 180 евро на первоначальное внедрение и 27 830 евро в год на техническое обслуживание. Следует отметить, что увеличение затрат носит нелинейный характер вследствие экономии, обусловленной ростом масштабов производства. Необходимо применять нелинейную шкалу, которая позволяет учитывать как масштабируемые, так и не масштабируемые затраты. Таблица 10 содержит более детальные данные по оператору магистральных сетей «Польские электроэнергетические сети», эквивалентные стране, имеющей 100 подстанций. Кроме того, в качестве метода обобщения результатов, дана количественная оценка общих трудозатрат (при отсутствии

защиты на начальном этапе), необходимых для более мелких (30 подстанций) и более крупных (200 подстанций) у сетевого оператора, на базе масштабируемых затрат.[28]

Таблица 10. Совокупные затраты на внедрение и обеспечение мер противодействия киберугрозам оператором магистральных сетей (евро)

		30 подстанций	100 подстанций	200 подстанций
Затраты на внедрение	Подстанции	6 047 200	15 118 000	27 212 400
	АСУ ТП	1 453 280	3 633 200	6 539 760
	Офисные системы	2 905 920	7 264 800	13 076 640
	ИТОГО $З_{Кап}$	10 406 400	26 016 000	46 828 800
Затраты на обслуживание и программное обеспечение	Подстанции	834 900	2 087 250	3 757 050
	АСУ ТП	155 216	388 040	698 472
	Офисные системы	510 496	1 276 240	2 297 232
	Итого обслуживание/ПО	1 500 612	3 751 530	6 752 754
Затраты на обслуживание/ оплата труда	Подстанции	208 800	696 000	1 392 000
	АСУ ТП	54 000	180 000	360 000
	Офисные системы	116 700	389 000	778 000
	Итого обслуживание/оплата труда	379 500	1 265 000	2 530 000
	ИТОГО $З_{Тек}$	1 880 112	5 016 530	9 282 754

Источник: (Calabrese, Finardi, and Ragazzi 2014)

[28] При анализе приведенных значений следует учитывать, что в изученном примере средняя почасовая оплата квалифицированного персонала составляет 20 евро (в ценах 2014 г.) и АСУ ТП ПЭС включают 100 серверов плюс резервный узел из 40 серверов с подключением через Интернет. Штат ПСЭ насчитывает 2000 человек.

4 Оценка эффективности

В настоящем разделе представлены подходы к оценке эффективности затрат на кибербезопасность. Такая оценка необходима, чтобы определить, насколько эффективны капиталовложения в повышение безопасности энергосистемы. Задача в том, чтобы предоставить регулирующим органам (и энергокомпаниям) средства оценки и мониторинга эффективности инвестиций.

Регулирующие органы смогут оценить эффективность мер кибербезопасности, сравнить их с контрольными показателями и затем оценить их эффективность с точки зрения затрат на их обеспечение.

ЦЕЛЬ ДАННОГО РАЗДЕЛА...

...описать и сравнить существующие средства оценки эффективности капиталовложений в кибербезопасность.

В разделе также вводятся некоторые базовые принципы оценки эффективности и рассматривается вопрос о том, как применять преложенную систему показателей, чтобы получить достоверные результаты.

Термин *оценка* (англ. *metric*) здесь относится либо к методу измерения, либо к единице измерения, которая используется в оценке контроле, ранжировании и выборе объектов (явлений, процессов или людей). В данном разделе рассматриваются оба варианта, дающие ответы на вопросы «*что?*» (переменные, т.е. показатели) и «*как?*» (методика расчета показателей и сбора данных). Таким образом вводится комплекс средств измерения и даются указания по их применению.

Как указано в пункте 2.1, роль (порядок применения и назначение) оценки зависит от методики, применяемой регулирующими органами. Метод, представленный в данном разделе, может применяться, например, для определения ключевых показателей эффективности (КПЭ),[29] необходимых для того, чтобы понять, обеспечивает ли установленный комплекс кибербезопасности желаемый уровень защиты. Регулирующие органы могут применить этот метод для сравнительной оценки эффективности капиталовложений в альтернативные средства кибербезопасности. В условиях непрерывного повышения сложности кибератак, сравнительный анализ призван обеспечить базу для обоснования стратегического плана капиталовложений в кибербезопасность. Либо, в случае регулирования по показателям эффективности, этот метод может служить для выработки мер стимулирования в целях обеспечения адекватного уровня киберзащиты. В следующем разделе подробно рассмотрен вопрос о том, как применять предложенные методы оценки при разработке регуляторного подхода.

Разработка метода оценки эффективности капиталовложений в кибербезопасность представляет собой сложную задачу, потому что требует глубокого понимания контекста, в котором будет функционировать система, и тщательного ситуационного анализа. Следует отметить, что исследования и эксперименты в этой области продолжаются и сегодня, так что предложений имеется много, но общепринятая практика пока не выработана.

[29] КПЭ являются критически важным подмножеством показателей эффективности. Они описывают настолько значимые возможности и свойства системы, что в случае их выхода за установленные, предельно допустимые значения на каком-либо предприятии, регулирующий орган будет вправе пересмотреть обоснование затрат данного предприятия на кибербезопасность.

4.1 Определение оптимальных показателей эффективности

Оценка результативности не ограничивается капиталовложениями в кибербезопасность, но затрагивает государственную политику, инновационные объекты, подходы, а также инвестиции. Исследователи и практики выработали общую позицию, позволяющую ответить на вопрос «как?», то есть правильно подойти к выбору показателей. Качество и адекватность показателей тесно связаны с выбранной методикой оценки и в совокупности определяют ее успех. Выбор неправильных показателей может свести на нет хороший план оценки. Аналогично, самый продуманный показатель может привести к неправильным выводам, если он не поддается измерению или используется неправильно. Поэтому важно понять общие требования и специфику показателей эффективности. Показатель должен иметь определенные свойства, чтобы его можно было использовать в качестве характеристики эффективности. К таким свойствам относятся:

- *Явно выраженная причинно-следственная связь*. Причинно-следственная связь между капиталовложением и переменной, которая характеризует ожидаемый результат, должна быть четко видна, а показатель должен отображать суть желаемого результата. Причинно-следственная связь должна быть столь же явно выражена в отношении других переменных, возможно, влияющих на результат (отсутствие дополнительных побочных факторов).
- *Измеримость*. Переменная, характеризующая результат, должна быть представлена показателями, которые можно наблюдать и зарегистрировать. Сбор данных для расчета показателя должен быть простым и не слишком затратным. Материальные затраты и трудозатраты, связанные с измерениями, должны быть соразмерны с важностью оцениваемого явления.
- *Специфичность*. Необходимо четкое представление о том, что является объектом измерений. Уровень детализации должен быть таким, чтобы результат и его изменения во времени и пространстве можно было наблюдать (чувствительность).

Выходная величина, результат и воздействие: пример

Группа сотрудников проходит учебный курс по процедурам безопасности при общении со сторонними организациями.

- **ВЫХОДНАЯ ВЕЛИЧИНА:** Количество слушателей, сдавших заключительный экзамен по теоретической части → Отражает интенсивность и качество работы, но мерилом результативности не является
- **РЕЗУЛЬТАТ 1:** Количество нарушений процедур безопасности (например, использование несанкционированных USB-накопителей) в течение года по прохождении курса → характеристика результативности
- РЕЗУЛЬТАТ 2: Количество вторжений в ИТ комплекс в течение года по прохождении курса → характеристика результативности, не обладающая чувствительностью
- ВОЗДЕЙСТВИЕ: Разница в количестве нарушений процедур безопасности в течение года по прохождении курса между группой сотрудников, прошедших обучение, и другой группой аналогичных сотрудников, обучение не проходивших.

4.2 Что такое эффективность? Понятия продукта, результата и воздействия

Эффективность характеризует результаты действий, но следует понимать, о каких результатах идет речь. **Продукт** — прямое следствие предпринятого действия (например, капиталовложения, программы обучения, новой процедуры, новой директивы, политики, стимула). **Результат** — изменение в объективных переменных, которое наблюдается в результате осуществления действия. Это изменение не прямое, но опосредованное, т.к. зависит от субъективных обстоятельств и переменных. Оно может запаздывать по времени.

Чтобы оценить эффективность действия (капиталовложения, программы обучения, новой процедуры, новой директивы, политики или стимула), необходимо проверить, что:

1) действие произошло и дало ожидаемые результаты; например, политика не даст результата при плохом управлении;
2) произошло изменение желаемого результата.
3) изменение было вызвано данным действием.

Все три момента важны, но последний анализировать сложнее всего. Сложность в том, что изменение — не значит следствие. После того, как выбран набор показателей, оценка эффективности состоит в сравнении одного или нескольких показателей до и после действия. Чтобы убедиться, что наблюдаемое изменение является следствием заданного действия, а не каких-либо внутренних причин, которые привели бы к этому результату в любом случае, необходимо убедиться в том, что именно произведенное действие **повлияло** на выбранную переменную. Для этого, наблюдаемое изменение сравнивается с изменением, зарегистрированным в сходных ситуациях, в которых действие не проводилось. Данный **метод сравнительного анализа** применяется тогда, когда есть основания подозревать «эффект балласта», который заключается в том, что улучшение наблюдаемого показателя могло произойти и в отсутствие действия.[30] Испытывая те или иные экспериментальные меры противодействия киберугрозам, важно провести подобный сравнительный анализ прежде, чем эти меры будут введены повсеместно, поскольку данный анализ – это единственный способ собрать надежные доказательства результативности новой политики.

4.3 Организационные аспекты сбора данных

Этот раздел можно было бы назвать «Как избежать самообмана». Оценка эффективности — задача, сложность которой зачастую недооценивают. Дело в том, что ее рассматривают как нейтральное использование информации, собранной и проанализированной с целью демонстрации эффективности по некоторому числу критериев. В действительности же, в

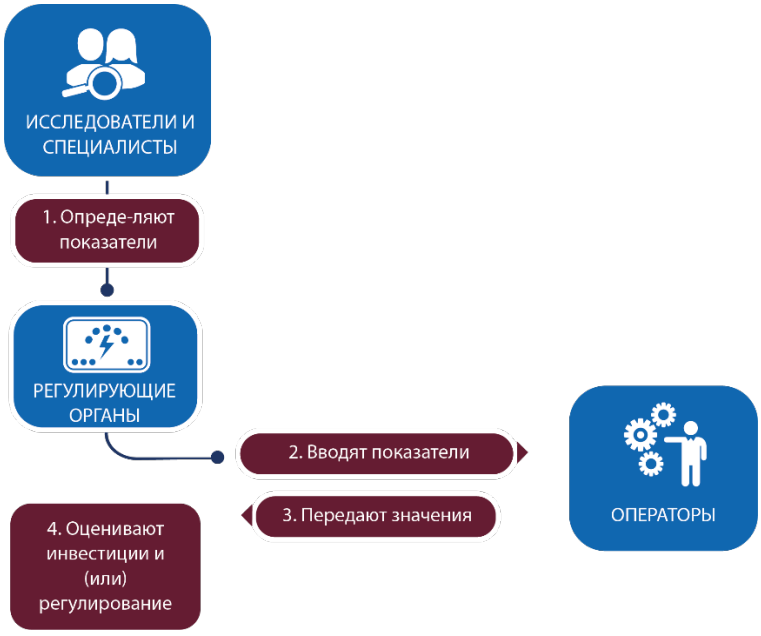
[30] Например, в кибербезопасности улучшение наблюдаемых показателей может происходить без каких бы то ни было активных действий, благодаря тому, что сотрудники следят за обсуждением вопросов кибербезопасности в СМИ и тем самым повышают осведомленность о рисках киберугроз.

этом будто бы рациональном, техническом подходе скрывается множество проблем, т.к. оценка сопряжена не только с объективными измерениями, но и с субъективным суждением. Если оценка затрагивает межведомственные отношения (две заинтересованные организации или даже просто два разных отдела у оператора), измерение эффективности приобретает субъективный оттенок, влияющий на решения о том, что следует измерять, как, зачем и кто это должен делать (Lewis 2015). Создать систему сбора данных не менее важно (и не менее сложно), чем выбрать правильные данные.

Когда регулирующие органы в своей деятельности начинают использовать показатели эффективности, они, как правило руководствуются логикой, показанной на Рис. 5.

1. Выбор, определение и обоснование применения показателей эффективности берется из соответствующей литературы.
2. Регулирующий орган выбирает определенных подход и обязывает подведомственные компании рассчитывать установленные показатели.
3. Компании периодически предоставляют собранные данные (показатели) регулирующему органу.
4. Регулирующий орган анализирует представленные данные, делает соответствующие выводы и на их основе дает оценку планам будущих капиталовложений, предложенным подведомственными компаниями.

Рис. 5. Определение показателей для целей регулирования



Опыт показывает, что основными этапами оценки являются этапы, в которых принимают участие как регулирующий орган, так и подведомственные компании (этапы 2 и 3). Обратите на это внимание.

- Этап 2. Регулирующий орган может потребовать расчета определенного показателя, но это не означает, что соответствующую формулу можно начать применять автоматически. Конечный метод — результат процесса, а не одномоментного принятия установленной формулы. «Тонкая настройка» достигается множественными экспериментами и выводами на основе полученных результатов. При этом учитываются данные как регулирующих органов, так и операторов.

  Этап 3: Сбор данных — сложный и трудоемкий процесс, требующий соответствующей квалификации, иными словами, затратный. Более того, предоставляя информацию о своей «внутренней кухне», компания тем самым провоцирует суждение о себе со стороны внешних лиц. Оператор (или предприятие более низкого уровня) может опасаться, что за декларируемой целью оценки эффективности (с целью ее повышения) могут скрываться попытки негласного контроля. Таким образом, органы регулирования, запросившие у оцениваемой организации необходимые данные, могут столкнуться с явным или молчаливым сопротивлением. Иными словами, нельзя недооценивать подобные организационные аспекты сбора данных и следует изучить его различные сценарии (например, введение санкций за неподчинение или создание независимого органа для сбора такой информации и управления ею).

4.4 Характеристики кибербезопасности

Характеристики кибербезопасности подразделяются на две категории:

- показатели уровня развития, говорящие, главным образом, об уровне готовности организации к кибератакам, и

- показатели эффективности кибербезопасности общего характера, указывающие на общую эффективность внедренных мер противодействия киберугрозам.

Как будет показано ниже в разделе 4.4.1, эти две категории содержат ряд точек соприкосновения, а в чём-то и пересекаются. Тем не менее, они принципиально различны. Исследования показателей эффективности кибербезопасности сегодня еще не закончены, общепринятая практика почти отсутствует. Характеристики, предложенные Исследовательским институтом электроэнергетики (EPRI), представляют собой результат исследований в этой сфере, продвинувшихся далее всего. Другие подходы находятся на предварительных этапах. Характеристики развития находятся на гораздо более высоком уровне, хотя до повсеместного их применения еще очень далеко.

4.4.1 Показатели уровня развития организации

Поскольку анализ уровня развития организаций — относительно разработанная область, можно сравнить несколько существующих в этой области методик. С точки зрения организационного управления и регулирования, наиболее интересны именно характеристики развития, вероятно потому, что они уравновешивают вклад специалистов

с одной стороны, организационной политики и процедур с другой, и технических средств управления с третьей. Однако показатели развития – это, по сути, качественные характеристики оператора, и, как любые качественные показатели, оставляют широкое поле для интерпретации.

Показатель уровня развития может применяться в разных сферах, не только в энергетике, и является одним из элементов кибербезопасности. В нашем контексте этот показатель можно определить следующим образом: это готовность реагировать на возможные нарушения безопасности. Для измерения этого показателя применяются различные шкалы, градуированные по уровням. Например, четырехуровневая шкала предусматривает уровни «неподготовленный», «реагирующий», «активно действующий» и «действующий на упреждение».

Следует учитывать, что этот показатель, хотя и связан с другими аспектами кибербезопасности, но отличается от них. В частности,

- Уровень развития — одно из условий эффективности (например, одни и те же капиталовложения могут дать разный результат в зависимости от исходного уровня развития).

- Повышение уровня развития — один из желаемых результатов программы укрепления кибербезопасности (важнейшими элементами кибербезопасности являются готовность и осведомленность).

Указанные выше связи убедительно свидетельствуют о важности инвестирования в людей и процессы (организационное управление), прежде всего в условиях, где начальный уровень развития компании низок. Эти прямые и обратные причинно-следственные связи также объясняют, почему целесообразно разрабатывать и внедрять конкретные показатели уровня развития, не ограничивая оценку техническими показателями.

В последующих разделах изложены современные подходы, отобранные среди многих подходов, разработанных консалтинговыми компаниями, и различающиеся лишь в деталях.

«Индекс развития» Университета Карнеги-Меллона

Модель оценки уровня развития, разработанная Университетом Карнеги-Меллона, и известная первоначально как «Модель оценки уровня возможностей» (CMM), позднее была дополнена другими моделями и преобразована в «Интегрированную модель оценки уровня возможностей» (CMMI). Эта модель первоначально задумывалась как средство оценки способности организации разработать то или иное программное обеспечение. Это самая известная модель оценки уровня развития организации, ее применяют в очень многих сферах, не только в сфере кибербезопасности (CMMI Institute 2019). Модель предлагает довольно сложный с точки зрения использования на практике комплексный подход. Термин «уровень развития» относится к степени формализации и оптимизации процессов и оценивается по пятиуровневой шкале: *начальный уровень* (хаос, отсутствие системы, личный героизм), *повторяемость, определенность, последовательное организационное обеспечение* (система готова к действиям) и *оптимизация* (система эффективна и экономична).

Уровни определяются в континууме зрелости, высший уровень является идеальным состоянием, в котором процессами управляют целенаправленно и систематически, их оптимизируют и непрерывно совершенствуют. Вышеперечисленные уровни соотносятся с кибербезопасностью следующим образом:

- *Начальный уровень*. Нет ни структуры, ни организации системы безопасности. Защита осуществляется усилиями отдельных людей, повторяемость и масштабируемость отсутствуют.

- *Повторяемость*. Система позволяет повторно использовать определенные меры противодействия. Основные процедуры разработаны, определены и задокументированы.

- *Определенность*. В этой системе больше внимания уделяется документации, стандартизации и обеспечению мер.

- *Последовательное организационное обеспечение*. Организация контролирует процессы безопасности и управляет ими посредством сбора и анализа данных.

- *Оптимизация*. Текущий контроль обратной связи в процессе работы создает возможности систематического совершенствования процедур безопасности и внедрения новых.

В настоящее время разработчики стандарта IEC 62443 исследуют упрощенную версию модели, основанную на сочетании системы показателей развития и уровней безопасности, приведенных в указанном стандарте. Данное сочетание именуется «уровнем защищенности». Работа пока не вышла за экспериментальную стадию, и шагов по внедрению результатов в стандарт IEC 2009 еще не предпринято.

Комплекс оценки уровня развития системы кибербезопасности (C2M2)

Комплекс оценки уровня развития кибербезопасности (C2M2) создан в рамках государственно-частного партнерства, основанного в целях расширения возможностей систем кибербезопасности в электроэнергетике и оценки состояния кибербезопасности электрических сетей (Christopher et al. 2014). Комплекс ориентирован на внедрение и управление средствами кибербезопасности, связанными с эксплуатацией ресурсов ИТ и ЭТ, а также условий, в которых они применяются.

Комплекс C2M2 состоит из трех моделей оценки уровня развития кибербезопасности: базовой модели (C2M2) общего назначения и двух дополнительных моделей для подотраслей: электроэнергетики (EC-C2M2) и нефтегаза (ONG-C2M2). Имеются также справочный материал и методические указания по внедрению данных моделей для операторов соответствующих подотраслей. Модель представляет собой перечень практик кибербезопасности, сгруппированных в 10 категорий и упорядоченных по уровням развития. Компании и организации могут сравнить собственную практику и средства кибербезопасности с практикой и средствами, предложенными в модели C2M2. На основании этого сравнения компания (организация) получает оценку в баллах по каждой категории. Результаты сопоставляются с контрольными баллами, отражающими устойчивость компании (организации) к риску по данной категории. Все модели находятся

в открытом доступе. Хотя изначально модели предназначались для самостоятельного использования, их применение оказалось непростым. Поэтому организации приглашают принять участие в однодневных семинарах по использованию моделей, где им оказывают содействие опытные специалисты.

Модель оценки уровня развития Nemertes

Иной подход заложен в модель оценки уровня развития Nemertes Research (Nemertes 2017). Ее проще понять и применить, чем CMMI и C2M2. Простоту подхода (к тому же, согласованного с триадой персонал-процесс-техника IEC 62443) иллюстрирует Таблица 12. Для оценки способности персонала противостоять постоянно развивающимся киберугрозам используется простой коэффициент от 0 до 3. Политика, процедуры и инструкции, принятые в организации, оцениваются по «индексу процессов». При этом, квалификация персонала и текущие процессы должны быть согласованы с имеющейся в организации техникой. С этой целью используется «технологический индекс».

Таблица 11. Модель оценки уровня развития Nemertes

	Неподготовленность Уровень 0	Реагирование Уровень 1	Активные действия Уровень 2	Действия на опережение Уровень 3
ПЕРСОНАЛ (уровень квалификации)	0	1	2	3
ПРОЦЕССЫ	Несистематичность	Базовые	«Нулевая тяга»	Новые угрозы
ТЕХНИКА	Защита периметра	Традиционный	Передовой	Сложные прототипы

Уровень развития организации определяется сочетанием этих показателей. Например, самый низкий уровень (неподготовленность) говорит о том, что квалификация персонала в зачаточном состоянии, процессы по большей части не систематичны, кибербезопасность сводится к защите периметра межсетевыми экранами и отсутствием соединений между административными и эксплуатационными подсетями.

4.4.2 Характеристики EPRI: комплексный и зрелый подход к оценке эффективности системы кибербезопасности

Как указано в документе EPRI «Характеристики кибербезопасности в электроэнергетике» (том 3) (Suh-Lee 2017),[31] EPRI вводит три показателя стратегического

[31] Полностью подход EPRI представлен в следующих отчетах: Suh-Lee 2017; Lee and Suh-Lee 2016.

уровня, 11 — тактического уровня и 45 — эксплуатационного уровня, всего 59. Иерархия показателей EPRI и их краткое обоснование представлены в на Рис. 6, заимствованном из вышеупомянутой публикации.

Рис. 6. Иерархия характеристик кибербезопасности EPRI

Источник: (Suh-Lee 2017)

Примечание. CVSS —шкала комплексной оценки уязвимости.

Рис. 7. Применение показателей EPRI

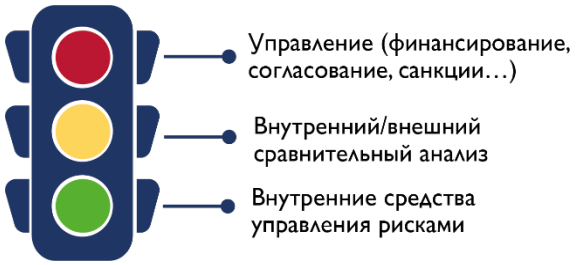
Для получения количественных характеристик используют 120 единиц информации (полный список необходимых единиц информации и показателей приведен в Приложении 3). Некоторые представляют собой результаты статистической обработки рабочих показателей энергокомпании. Так, эксплуатационные показатели – это замеры рабочих показателей в компании, которые берутся из журналов регистрации и других официальных документов. Тактические характеристики дают общее представление о текущем состоянии и ходе выполнения мероприятий по кибербезопасности в организации. Стратегические характеристики предназначены для измерения корпоративного риска. Они увязываются с направлениями основной деятельности. Единицы информации, на основе которых рассчитывают количественные характеристики, представляют собой значения измеримых

величин. Характеристики допускаются к применению после внешней оценки методики, предложенной в отчете.[32]

Очевидно, что некоторые из вышеперечисленных требований трудно выполнить, не накопив практический опыт. В этом и состоит основная цель опытного применения методики EPRI в пяти энергокомпаниях США (членах EPRI), в настоящее время экспериментирующих с предложенными показателями (характеристиками). Сам EPRI сейчас пропагандирует внедрение этих показателей в качестве стандарта в Европейском Союзе, где, возможно, будет запущено опытное применение по аналогии с США.

Хотя набор из 120–150 единиц информации может показаться громоздким, EPRI на основании опытного применения в США утверждает, что им можно пользоваться уже на минимальном уровне развития (начиная с уровня 1). Модель непригодна только для организаций с самым низким уровнем подготовки (нулевым). Кроме того, EPRI объявил о скором выпуске программного обеспечения с открытым исходным кодом, чтобы компании могли менять его под свои условия. Данное средство, в котором используются средства ИТ и связи, будет иметь вид электронной панели управления и позволит ускорить сбор нужной информации. Тем не менее, очевидно, что для внедрения и полного освоения системы может понадобиться немало времени (по мнению специалистов EPRI, для крупных организаций не менее полугода), а также квалифицированный персонал.

Рис. 8. Использование системы EPRI для собственных нужд и сторонними организациями



Неудивительно, что для количественной оценки уровня готовности столь сложного и многогранного объекта, как система кибербезопасности оператора, требуется оценить так много различных показателей. Есть основания полагать, что 120–150 единиц информации — это верхний предел, причем столько их требуется только для крупных компаний. Следует изучить вопрос о том, нельзя ли сократить их число при оценке уровня развития небольших компаний и компаний с менее сложной структурой. Наконец, стоит отметить, что EPRI прямо указывает: вначале должна быть принята сама модель оценки уровня развития организации и только потом в ней могут применяться предложенные характеристики системы кибербезопасности.

В аннотации EPRI указывает, что комплекс характеристик кибербезопасности EPRI расширит возможности энергокомпаний в следующем:

[32] Окончательное решение может быть принято только по результатам опытного применения утвержденной методики. Настоятельно рекомендуется не пренебрегать этим этапом, т.к. на нем могут быть выявлены недочеты и намечены пути их устранения.

- сбор количественных данных о системе кибербезопасности, на основе которой будут приниматься решения по управлению рисками;
- контроль над выполнением поставленных целей с помощью воспроизводимого метода;
- повышение подотчетности посредством выявления недочетов или неэффективных мер безопасности; и наконец,
- создание объективной картины существующих в компании условий для последующего сравнительного анализа методов и средств кибербезопасности, принятых в компании, с контрольными величинами.

Сказанное позволяет заключить, что данная система представляет собой серьезное средство управления рисками. При этом EPRI весьма осторожно высказалась по поводу возможности применения своего комплекса сторонними организациями для сравнительной самооценки и регулирующими органами для сравнительного анализа в целях контроля (Рис. 7 и Рис. 8). Более того, на этом предварительном, экспериментальном этапе данная методика потребует полного взаимодействия со стороны оцениваемой компании.

4.4.3 Важный аспект системы EPRI: агрегирование данных

При разработке системы EPRI применялись различные методы агрегирования данных, особенно для расчетов показателей более высокого уровня на основе показателей более низкого (например, тактическую характеристику из ряда эксплуатационных). Наиболее распространенный прием агрегирования представляет собой сочетание балльной оценки и взвешенного среднего.[33]

Таблица 12 иллюстрирует пример тактического показателя: балльная оценка реагирования на нештатную ситуацию.

Имеется пять исходных величин, каждая из которых является эксплуатационной характеристикой. У каждой характеристики есть заданные минимальное и максимальное значения. С помощью функции отрицательной балльной оценки[34] для каждой входной характеристики определяют свой балл. На заключительном этапе рассчитывается совокупный балл, характеризующий реагирование на нештатную ситуацию (T-IRS). Это число представляет собой взвешенное среднее исходных баллов, нормализованное по диапазону от 0 до 10.

[33] Агрегирование — процесс, в котором несколько взаимосвязанных величин группируют, чтобы получить одну величину, которая более содержательна или удобна для сравнительного анализа.

[34] Функция отрицательной балльной оценки представляет собой отношение расстояния от фактического значения до максимального к максимальному расстоянию. Таким образом, чем больше значение, тем меньше балльная оценка. Формула выглядит так: Балльная оценка = (Макс-Факт)/(Макс-Мин).

Таблица 12. Балльная оценка реагирования на нештатную ситуацию с весовымикоэффициентами

Балльная оценка реакции на нештатную ситуацию с весовыми коэффициентами	Факт. Знач.	Мин.	Макс.	Оценка (-)	Весовой коэф.	Оценка х вес.коэф.
O-I-MTTC Среднее время до сдерживания	8,4	0	30	0,7200	3	2,1600
O-I- MTTR Среднее время до восстановления	21,4	0	60	0,6433	3	1,9300
O-I- MTTA Среднее время до действия	3,8	0	7	0,4571	3	1,3714
O-I- MCRM Средние затраты на реагирование (чел.-час)	11,1	0	480	0,9769	0,5	0,4884
O-I- MCRX Средние затраты на реагирование (долл.)	400	0	48 000	0,9917	0,5	0,4958
O-PHC	Балльная оценка реагирования на нештатную ситуацию			6,4457		

Источник: (Suh-Lee 2017)

Разработчики показателей отмечают: «Как правило, в системе EPRI, показатели безопасности определяются с помощью серии весовых коэффициентов, которые имеют стандартные значения и применяются к каждому из исходных показателей при агрегировании в показатель более высокого уровня... При этом значения весовых коэффициентов выбираются почти произвольно. Предполагается, что пользователи проанализируют «стандартные» значения коэффициентов и скорректируют их в соответствии со спецификой своих условий». Следует учитывать, что, с одной стороны, корректировка, обусловленная индивидуальными условиями компании, не допускает возможности объективного сравнительного анализа. Кроме того, могут потребоваться длительные и сложные взаимные консультации, прежде чем все участники процесса согласятся с заданными баллами и весовыми коэффициентами для применения при агрегировании базовых показателей (эксплуатационных характеристик) в тактическую характеристику, как в приведенном выше примере. С другой стороны, это необходимо сделать в любом случае, иначе показатель не будет общепринятым и сопоставимым для всего множества участников. Поскольку аналогичный процесс потребуется для формирования единого мнения по большому числу показателей (45 эксплуатационных и 11 тактических), становится ясно, что прежде чем эти показатели станут общепринятыми и

прежде, чем их можно будет применять на практике в электроэнергетике, предстоит большая работа.

4.5 Сравнительная оценка и заключение

Анализ показателей кибербезопасности, приведенный выше, позволяет заключить, что в настоящее время только показатели уровня развития организации (компании) и показатели системы EPRI пригодны для практического применения. Другие показатели эффективности в кибербезопасности, например, заданные стандартом IEC 62443, пока не вышли за стадию изучения. Пока такого рода проекты не достигнут зрелости, возможности применять соответствующие подходы для обоснования затрат или в иных целях регулирования не будет. Существует несколько моделей оценки уровня развития организации, по каким-то уже накоплен некоторый опыт применения. Некоторые разработаны частными консалтинговыми фирмами и продаются, в то время как C2M2 остается бесплатным. Тем не менее, ограничиваться моделями оценки уровня развития компании при оценке эффективности капиталовложений не следует, поскольку они не охватывают все аспекты кибербезопасности и основаны главным образом на самооценке, а не на объективных данных.

Система показателей, разработанная EPRI, имеет комплексный (но, соответственно, и сложный) характер и, по-видимому, хорошо продумана и реализована с точки зрения важнейших аспектов, рассмотренных в разделе 4.4.3. Если текущие и будущие эксперименты подтвердят реализуемость и практическую применимость эти показателей, они смогут сыграть передовую роль не только в электроэнергетике, но и в любом критически-важном начинании, а также на уровне отрасли или частного сектора в целом. Действительно, хотя комплекс показателей изначально разрабатывался EPRI для электроэнергетики, характеристик, отражающих специфику этой отрасли, среди них нет. При этом, однако, нужно учитывать следующие соображения:

- комплекс показателей EPRI все еще остается прототипом, который требует испытаний и усовершенствования; может потребоваться несколько лет и гораздо больше экспериментов и оценок, прежде чем он будет принят во всем мире;
- В настоящее время эти показатели применяются, главным образом, как средство сравнительного самоанализа в компаниях, уверенных в обоснованности своего подхода к кибербезопасности. Они не изучены в той степени, которая необходима для принятия в качестве стандарта или передового опыта оценки состояния кибербезопасности оператора и обмена соответствующими данными.
- Модель оценки развития, например C2M2, предлагается в качестве модели для предварительной оценки. Она позволит дать оценку мерам по улучшению системы кибербезопасности, то есть, может быть использована для оценки уровня развития компании и мер по совершенствованию системы после того, как в компании проведена оценка риска. Особенно полезна C2M2 в подотраслях, в настоящее время не охваченных государственным регулированием. Модели уровня развития и модели EPRI дополняют друг друга и в совокупности средствами оценки эффективности общей стратегии кибербезопасности.

Исходя из вышеизложенного, рекомендуется принять модель оценки уровня развития и внимательно следить за совершенствованием методики EPRI. Хотя последняя все еще

не вышла за стадию прототипирования, весьма вероятно, что в краткосрочной или среднесрочной перспективе она найдет широкое применение в электроэнергетике.

Выбор подхода для регулирующих органов в энергетике сводится к следующему: внедрить методику EPRI целиком или ограничиться несколькими показателями, выбрав их из 11 тактических и 45 эксплуатационных характеристик, предусмотренных в методике EPRI. Идея упрощенного подхода привлекательна, а ее внедрение — более практично. Проблема в том, что даже самые современные системы расчета показателей кибербезопасности в настоящее время не составляют общепринятого стандарта. Требуются дальнейшие исследования, чтобы понять, даст ли упрощенная стратегия корректное, пусть и не столь глубокое, представление о состоянии системы кибербезопасности в компании,[35] или исказит картину вследствие своей ограниченности. Именно поэтому, пока регулирующие органы ожидают более определенных результатов исследований, возможно, предпочтительней принять простую модель оценки уровня развития. В этом случае, с точки зрения регулирующего органа, обоснованием затрат может считаться улучшение состояния кибербезопасности в компании-заявителе. Уровень кибербезопасности подведомственной компании при этом оценивается с помощью таких средств, как система EPRI или ES-C2M2, а также параллельные методики, выработанные на основе стандартов IEC 62443 и IEC 62351.

[35] Опытное применение методики EPRI дает возможность получить анонимизированные данные, которые затем статистически обрабатываются в целях дополнительного обоснования приемлемости такого подхода.

5 Подход к капиталовложениям в кибербезопасность

ЦЕЛЬ ДАННОГО РАЗДЕЛА...

...показать, как можно организовать процесс принятия решений от теории до реализации.

В разделе рассматривается ряд принципов и средств регулирования и их практического применения на примере нескольких сценариев в целях повышения уровня кибербезопасности стран Европы и Евразии.

Цель данного раздела — помочь регулирующим органам разработать общий подход к оценке обоснованности капиталовложений в кибербезопасность и расчета тарифов (включая практические предложения по процессам, процедурам, нормотворчеству и правилам регулирования). Для этого необходимо дать оценку существующим средствам и механизмам и далее планировать переход к новым методам, не отходя при этом от национальных нормативов регулирования энергосистем. Существующие средства и механизмы, в свою очередь, связаны с общей нормативно-правовой базой и могут включать регламенты лицензирования и закупок, требования конфиденциальности, контроль над доступом к данным и процессам, а также нормативы качества обслуживания и доказательства того, что деятельность подведомственных предприятий направлена на общественные интересы (подотчетность).

В странах, где энергетика пока находится на этапе перехода к полноценным рыночным отношениям, нормативно-правовая база и производственные регламенты не сформированы окончательно; но как раз это и может оказаться преимуществом. В западных странах законы, нормативные акты и директивы — это долговременные многослойные напластования, которые очень трудно объединить и соблюдать. Страны с переходной экономикой могут создать эффективную и простую нормативную базу, извлекая уроки из опыта США и ЕС, но не подражая им, хотя такой подход и требует сильной политической воли и стратегического видения.

Начинать следует с формирования стратегии кибербезопасности, основанной на концепции стратегического планирования. Такая стратегия охватывает три направления: квалификация персонала (обучение и понимание круга проблем); согласованные процессы, воплощенные в действующей политике, процедурах и регламентах; внедрение технических решений в соответствии с горизонтом планирования (от 10 до 20 лет).

Каждое направление требует существенных капиталовложений, а выбор определяется на основе прогнозируемой результативности. В данном разделе рассмотрены средства и принципы регулирования и показан порядок их применения в типовых ситуациях (сценариях) регулирования. Цель раздела – описать процесс принятия решений от теории до реализации и проиллюстрировать его такими сценариями. Полученные сведения могут применяться в качестве ориентира при решении других задач или разработке политики.

5.1 Справочная информация

В данном разделе представлены цели, стоящие перед регулирующими органами в период радикальных преобразований в энергетике. Именно цели задают направление всех решений регулирующих органов, в том числе, в сфере кибербезопасности.

Развитие электроэнергетики в быстро меняющихся современных условиях заставляет уделять пристальное внимание регулированию сетей. В энергосистемах

постоянно внедряются технические решения, приводящие к изменениям в производстве и потреблении электроэнергии. Еще более радикальный характер изменениям придает то, что до недавнего времени объектом регулирования были системы, в которых инновации были крайне редки, а четко очерченных услуг предлагалось мало.

Сегодня цели регулирования услуг электроэнергетики сосредоточены в трех направлениях:

- удовлетворение потребностей и обеспечение качества обслуживания потребителей;
- обеспечение безопасности сети и ее устойчивости к нештатным ситуациям;
- создание сети, которая позволяет использовать технологии с пониженными выбросами углекислого газа.

В данном разделе:

- Дана сводка основных целей регулирования и принципов, определяющих сценарии регулирующих органов.
- Сделан обзор типов мер и средств регулирующих органов.
- Рассмотрен вопрос разработки действенных нормативов в разрезе кибербезопасности.
- Приведены примеры и альтернативные сценарии, основанные на описанных средства, которые могут оказаться перспективными для регулирующих органов в энергетике.

Сегодня регулирование направлено на то, чтобы поставить потребителей всех уровней (от бытовых до крупнейших промышленных) на ведущие роли, что на практике означает:

- у потребителей должно быть право участвовать в принятии решений и давать оценку обслуживанию и бизнес-практике компаний;
- стоимость услуг должна быть адекватной;
- потребители должны иметь право непосредственного участия в развитии энергосистемы посредством своих действий и инвестиций.

Первый пункт в основном касается регулирующих органов: именно они определяют порядок сбора и обнародования отзывов потребителей. Эта деятельность соответствует их роли народного представителя и может осуществляться на основе разного рода консультаций. Этот пункт еще важнее в стремительно развивающихся сферах, в числе которых и кибербезопасность. Современная система открывает немало возможностей, но и создает множество потенциальных рисков – фактор, которые подчеркивает важность участия заинтересованных сторон в принятии решений. Соответственно, одной из важнейших современных задач является организация каналов обмена информацией среди всех заинтересованных сторон, например назначив ответственного по связям с отраслевыми и потребительскими ассоциациями, средним и крупным бизнесом и т.д.[36]

[36] Подробнее см. издание НАРУК «*Вводный курс по коммуникациям для органов государственного регулирования энергокомпаний*» (Choueiki 2019).

5.2 Типы мер и действий

Ниже приводится перечень, а также развернутые определения, основных мер и действий, которые помогут регулирующим органам в достижении рассмотренных выше целей. В большинстве случаев для достижения конкретной цели или нескольких целей в рамках одной стратегии можно применять сочетание нескольких мер и действий.

Минимальные нормативы. Регулирующий орган определяет минимальные нормативы (список мер, которые необходимо соблюдать) и санкции за их несоблюдение. Санкции могут включать штрафы или принуждение к действию.

Основные показатели эффективности. Их цель аналогична цели минимальных нормативов –обеспечить соблюдение компаниями минимальных нормативных требований, -- но реализуется этот тип мер иначе. Регулирующий орган определяет ряд важнейших параметров и их минимальных значений, которые характеризуют настолько важные функции и свойства системы, что выход этих параметров за предельные значения вынуждает регулирующий орган применить санкции (как и выше, в виде штрафов или принуждения к действию).

Предварительно оговоренные показатели. Регулирующий орган устанавливает условия для определенных показателей, связанных с планами компании. Например, в контексте РППЭ эта мера используется в тех случаях, когда цели регулирования не достигаются, если предоставить энергокомпании право самой решать, как добиться необходимых результатов. Регулирующий орган определяет целевые показатели или капиталовложения компании и требует от компании их выполнения. В таких случаях используется и КПЭ: если целевые показатели не достигнуты, регулирующий орган вправе пересмотреть обоснование затрат оператором.

Стимулирование. В случае РППЭ поощрения или санкции применяются в зависимости от тех или иных показателей. Значения показателей отражают повышение или снижение качества обслуживания потребителей. Механизмы стимулирования во многом зависят от специфики деятельности и от отрасли, поэтому их следует выбирать тщательно во избежание отрицательных побочных эффектов. Например, излишне строгая проверка на соответствие установленным стандартам может побудить компании скрывать необходимую информацию.

Кроме описанных мер, упомянем другие факторы, которые следует учитывать в процессе регулирования.

Механизмы неопределенности. Позволяют пересматривать принятые меры при изменении внешних условий. Крайне важно заранее определить, какие риски могут возникнуть у компаний и какие действия предпринять, чтобы заново определить цели.

Консультации с общественностью или заинтересованными сторонами. Регулирующий орган вправе полагаться не только на мнение собственных или привлеченных специалистов. Многие компоненты вышеописанных мер (минимальные нормативы, КПЭ и их предельные значения, требования к проектам, возможные риски)

можно определять в консультациях с общественностью или внешними заинтересованными сторонами.

Соглашения. При регулировании объемов производства, некоторые компоненты вышеуказанных мер, например КПЭ, а также их предельные значения или целевые показатели, могут быть определены посредством соглашения между регулирующим органом и оператором энергосистемы. Регулирующий орган и оператор согласуют нормы, которые затем служат критериями экономического стимулирования. Тем самым усиливается заинтересованность оператора в выборе желаемой стратегии.

5.3 Построение сценариев кибербезопасности, начиная с определения целей

Задача данного раздела — дать рекомендации относительно выработки мер обеспечения кибербезопасности в энергосистеме с точки зрения регулирующего органа. Несмотря на то, что в этих рекомендациях невозможно описать меры, которые бы идеально соответствовали специфике всех стран, процесс принятия решений, как правило, следует определенному порядку, который в свою очередь состоит из этапов: решений, определений и мероприятий. Изменять порядок этапов не следует, так как он обеспечивает последовательный переход от принципов к реализации, где каждое решение задает спектр возможных вариантов следующего этапа. На Рис. 9 данный процесс показан применительно к методике регулирования «затраты-плюс», а на Рис. 10 — для методики РППЭ.

Обе методики начинаются с определения стратегии кибербезопасности, в частности, с постановки цели. Прежде чем перейти к конкретным этапам реализации, регулирующему органу следует определить общую стратегию кибербезопасности в энергетике как едином комплексе.[37] Без понимания того, куда двигаться, согласованные действия невозможны. Чтобы регулирование соответствовало тому, ради чего оно было задумано, требуются четко определенные цели, а также стратегия и средства их достижения. Для стратегии необходимо, чтобы директивный орган видел перспективу («Какие ценности побудили меня разработать данный подзаконный акт?», «Какие цели я преследую?») и мог формулировать свои ожидания (Как должен измениться рынок электроэнергии благодаря реализации стратегии?).[38]

[37] В соответствии с общей стратегией кибербезопасности в стране, сформированной действующими законами и нормами. Регулирующие органы, начиная с уровня центрального правительства, должны разработать конкретные задачи для электроэнергетики, согласованные с общегосударственной стратегией, учитывая при этом финансовые последствия планируемых изменений и приоритеты политики.

[38] ПРИМЕЧАНИЯ К РИСУНКАМ

Затраты-плюс, Этап 4. Определить затраты, связанные с кибербезопасностью, сложно, если в планах компаний, требующих согласования, они не выделены в отдельную статью. Например, средства кибербезопасности часто входят в комплект новых аппаратных средств и программного обеспечения. Если функции кибербезопасности не выделить отдельно, покупка такого оборудования будет выглядеть как необоснованный выбор более дорого из возможных вариантов. Затраты на организационное управление и процедуры безопасности также зачастую включаются в другие категории затрат, если оператор не приводит отдельного обоснования соответствующих ресурсов. Порядок определения затрат на кибербезопасность должен быть установлен заранее. Этот этап будет сопряжен с меньшими сложностями, если предшествующий ему этап 2 отработан тщательно и во всех деталях.

Затраты-плюс и РППЭ, Этап 6. Если кибербезопасность обеспечивается с помощью комплекса мер противодействия киберугрозам, крайне важно своевременная обновлять стратегию. Подход к кибербезопасности, который сводится лишь к соблюдению нормативов, плохо справляется с изменениями в обстановке и может создать ложное ощущение безопасности. Далее, в РППЭ, очень важно учитывать приобретаемый опыт и соответственно регулярно вносить изменения в стратегию. Наконец, проблемы «философии стимулирования» связаны с тем, что систему стимулов также необходимо постоянно обновлять в соответствии с изменением обстановки.

РППЭ, Этап 2. *Четкая задача* означает, что выбранная формулировка позволяет во всех случаях понять, соответствует ли этой задачи конкретная ситуация. Если на этот вопрос отвечают «частично» или «по обстоятельствам», это означает, что задача поставлена нечетко. *Измеримая задача* означает, что заданная цель (например, снижение уровня безработицы) выражается измеримой переменной (например, процент безработных, а не трудоустраиваемость). *Рациональность задачи* означает, что целевой показатель задан на уровне, который может быть достигнут усилиями, соразмерными с предлагаемым стимулом.

РППЭ, этап 3. Данный этап должен быть организован как процесс (последовательность семинаров и консультаций), а не как единовременное решение.

Рис. 9. Сценарий регулирования по методике «затраты-плюс»

Рис. 10. Сценарий регулирования по показателям эффективности (РППЭ)

5.4 Сценарии кибербезопасности

В этом разделе даны примеры сценариев государственного регулирования,[39] имеющих одну и ту же цель – укрепление кибербезопасности. Задача в том, чтобы показать, как один и тот же принцип по-разному реализуется на практике в зависимости от методики, принятой регулирующим органами. Некоторые средства, применяемые регулирующими органами, включая те, которые еще предстоит принять, определяются нормативно-правовой базой страны.

Этап 1. Определить стратегию кибербезопасности для энергосистемы

Проблема. Директивный орган (при содействии регулирующего органа) обнаружил, что энергокомпании вкладывают средства в кибербезопасность, не имея для этого достаточного обоснования, поскольку у них нет ни стратегии, ни квалификации для успешной реализации мер противодействия киберугрозам.

Стратегия. Регулирующий орган вмешивается в эту ситуацию, предлагая энергокомпаниям разработать стратегию и внутреннюю документацию, включающую подготовку, меры по повышению готовности и осведомленности персонала, а также надлежащие процедуры.

Ниже описаны пять сценариев, соответствующих этапам, перечисленным в разделе 5.3, в котором определен план регулирования. В сценариях описаны категории мероприятий (по одному на этап) в том порядке, в котором их следует выполнять. Результат должен обеспечить единство подхода и обосновать выбор того или иного варианта.

Все сценарии направлены на решение одной и той же проблемы, поэтому Этап 1 в них совпадает. Выбранная цель отражает организационно-управленческий аспект кибер-безопасности, поскольку именно эта часть представляется наиболее важной. Именно от нее зависит эффективность остальных инвестиций в кибербезопасность. Более того, это сфера, в которой показатели (конкретно, показатели уровня развития) наиболее близки к широкому использованию, поэтому имеет смысл попробовать применить РППЭ.

[39] Как сказано выше, в сценариях определены действия, которые должны быть выполнены в определенном порядке. Действия одного типа могут входить в разные сценарии, при этом их результаты могут различаться в зависимости от специфики. Мы предлагаем регулирующим органам делать акцент на мероприятиях по доведению информации и больше консультироваться с компаниями, чтобы уяснить степень их осведомленности в вопросах кибербезопасности и спрогнозировать осложнения, обусловленные принятыми решениями.

5.4.1 Сценарий 1. Соблюдение нормативов по методике «затраты-плюс»

В сценарии показано, как достичь цели, поставленной на Этапе 1, используя методику «затраты-плюс».

- **Этап 2** *Определить меры противодействия киберугрозам*, соответствующие стратегии. Регулирующий орган определяет перечень мер в сферах кибербезопасности, перечисленных в Таблице 5. Компании обязаны ввести их у себя на производстве.

- **Этап 3** *Разработать нормативы по затратам*, соответствующие стратегии. Покрываются все издержки, понесенные компаниями с целью реализации мер противодействия киберугрозам.

- **Этап 4** *Определить порядок* отчетности Регулирующий орган определяет порядок отчетности о приемлемых затратах. Детально определяются категории затрат (зарплата новых сотрудников, расходы на консультантов, затраты на обучение). Компаниям предлагается выделить затраты на кибербезопасность из общей массы затрат и инвестиций.

- **Этап 5** *Проверить фактически понесенные издержки* и соответствие реализованных мер нормативам. Регулирующий орган проверяет, что издержки соответствуют приемлемым категориям. С этой целью можно провести аудиты, в ходе которых проверяется, были ли приняты меры и как именно. Регулирующий орган может привлечь к работе сторонних специалистов, чтобы оценить выполнение требуемых мероприятий. Компании и регулирующий орган вправе нанимать сторонних специалистов для содействия в процессе аудита.

- **Этап 6** *Актуализация плана-графика* Этапа 2. По завершении процесса регулирующий орган проводит серию консультаций и открытых обсуждений с компаниями и специалистами, чтобы понять, актуальны ли запланированные ранее меры или необходимо их заменить. То же относится к методикам отчетности и аудита.

5.4.2 Сценарий 2. Частичное участие компаний в рамках методики «затраты-плюс»

Сценарий является альтернативой Сценарию 1 в рамках той же методики «затраты-плюс».

- **Этап 2** *Определить меры противодействия киберугрозам.* Регулирующий орган совместно с компаниями организует процесс открытых консультаций, где обсуждается перечень мер противодействия киберугрозам в областях, перечисленных в Таблице 5. По результатам консультаций регулирующий орган вырабатывает минимальный комплекс требований; все не вошедшие в него меры считаются факультативными. Регулирующий орган собирает и анализирует мнения компаний, но несет единоличную ответственность за окончательные решения.

- **Этап 3** *Определить нормативы по расходам.* Регулирующий орган компенсирует затраты только на заранее оговоренные дополнительные (факультативные) меры. Затраты на выполнение минимальных требований принимает на себя оператор. В исключительных обстоятельствах предусматривается возможность компенсации затрат (отсутствующих в перечне Этапа 2) на технические новинки или на удовлетворение новых нужд.

- **Этап 4** *Определить порядок отчетности*. Регулирующий орган определяет порядок отчетности по дополнительным издержкам, а также порядок подачи заявки на компенсацию исключительных расходов. Подавать заявки на компенсацию дополнительных издержек компаниям разрешается раз в год.

- **Этап 5** *Проверить фактически понесенные расходы.* Регулирующий орган проверяет, соблюдены ли минимальные требования и соответствуют ли показанные в отчетах расходы по мерам, выходящим за рамки минимальных требований. Для этого проводятся проверки с целью установить, реализованы ли эти меры и как именно. Кроме того, регулирующий орган проверяет, соответствуют ли заявки нормам на расходы.

- **Этап 6** *Актуализация плана-графика*. Чтобы получить информацию об эффективности политики, компании обязаны применять модель C2M2. Регулирующий орган оказывает поддержку и дает методические указания компаниям, которые проводят самооценку уровня развития своей системы кибербезопасности. Общие результаты самооценки подвергаются анализу и обсуждаются с целью оценки политики, внесения изменений в минимальные нормативы и определения приемлемых дополнительных издержек. Также сравниваются компании, получившие финансирование на дополнительные меры кибербезопасности – и компании, выполняющие минимальные требования, чтобы понять, помогло ли дополнительное финансирование повышению уровню развития компаний («анализ влияния»). Далее, устанавливается, воспользовались ли компании возможностью (и если да, то как) подать заявку на компенсацию дополнительных издержек и анализируется, как регулирующий орган организовал управление этой возможностью. На основе полученных результатов регулирующий и директивный органы вносят изменения и дополнения в стратегию на последующие годы.

5.4.3 Сценарий 3. Участие оператора в рамках методики «затраты-плюс»

Этот сценарий базируется на Сценарии 2, но допускает особый подход и особые условия для одного из операторов, чей уровень осведомленности в сфере кибербезопасности выше, чем у других операторов.

- **Этап 2** *Определить меры противодействия киберугрозам.* Регулирующий орган и выбранная компания согласовывают и принимают минимальные требования на основе перечня мер противодействия киберугрозам, составленного в Сценарии 2, а также решают, какие дополнительные меры могут получить финансирование. В заключительном соглашении предусмотрено следующее:

- на данного оператора распространяются те же минимальные требования, что и на другие компании;
- возможно финансирование более широкого спектра факультативных мер;
- оператор организует семинары-практикумы для других компаний.

- **Этап 3** *Определить нормативы по расходам.* Регулирующий орган компенсирует затраты только на заранее определенные дополнительные (факультативные) меры. Затраты на выполнение минимальных требований берет на себя оператор. Поскольку этот оператор получает больший объем финансирования, чем другие операторы, хотя он уже и так достаточно развит и организован, он за свой счет проводит курсы обучения для других компаний

- **Этап 4** *Определить порядок отчетности*. То же, что в Сценарии 2. Компания предоставляет учебный план тренингов на согласование.

- **Этап 5** *Проверить фактически понесенные расходы.* То же, что в Сценарии 2.

- **Этап 6** *Актуализация плана-графика*. Поскольку данный оператор уже имеет опыт применения показателей уровня развития в своей практике, от него потребуются консультации и данные для сравнительного анализа. Например, в компании уже применяли C2M2 до введения регулирования, поэтому она соглашается организовать для других компаний тренинг по внедрению и использованию C2M2. Также, компания соглашается предоставить перечень характеристик (статистику и анонимизированные данные) регулирующему органу для сравнительного анализа.

5.4.4 Сценарий 4. Экспериментальное использование стимулов для повышения показателей развития

Сценарий отражает возможный вариант достижения цели, поставленной на Этапе 1 в рамках методики РППЭ.

- **Этап 2** *Определить* четкие, измеримые и рациональные *цели*, согласно стратегии. Компании должны достичь минимального уровня развития. Для определения показателей развития регулирующий орган использует модель C2M2.

- **Этап 3** *Определить совокупность показателей, контрольные значения и стимулы*. Компании обязаны применять модель C2M2 (или подгруппу из области значений модели). Регулирующий орган устанавливает контрольное значение или минимальный уровень показателей развития, которого следует достичь (например, уровень 1); если компания не смогла достичь установленных значений, налагается штраф, если компания превысила установленные значения, она получает поощрение.

- **Этап 4** *Определить методику расчета показателей*. В рамках помощи компаниям в ознакомлении с новыми нормами, регулирующий орган проводит семинары, в ходе которых компании знакомят с логической схемой и функциональными

характеристиками модели C2M2. Затем компании проводят самооценку, используя инструментарий C2M2, который находится в свободном доступе. Компаниям могут предложить участие в однодневных семинарах (организованных регулирующим органом) по самооценке и провести итоговый анализ с участием опытных методистов.

- **Этап 5** *Провести проверку* методики расчета показателей. На данном этапе регулирующий орган проводит аудит, в ходе которого специалисты (приглашенные за счет регулирующего органа) проверяют, соответствуют ли представленные оператором значения (полученные в ходе самооценки) реальной ситуации. В случае обнаружения значительных расхождений на операторов налагаются санкции.

- **Этап 6** *Обновить план-график*. Регулирующий орган анализирует результаты Этапов 3 и 4, исходя из оценки специалистов, отзывов компаний и собственного опыта. Регулирующий орган проводит общий анализ по отрасли для уточнения оценки достигнутого компаниями уровня развития. Анализ проводится на базе консультаций, в ходе которых компании и представителей заказчика просят прокомментировать результаты, полученные регулирующим органом, и дать свои рекомендации по совершенствованию работ в рамках поставленных целей. Обсуждение должно охватывать техническое содержание стратегии и его практическую реализацию, в частности:

  - **Выбор показателей**. Является ли C2M2 надежной моделью? Легко ли ее применять? Достаточно ли она чувствительна, чтобы использовать ее качестве стимула?

  - **Уровень контрольных значений**. Каков средний уровень показателей развития после введения контрольных значений? Следует ли повысить минимальные требования?

  Коллективное обсуждение можно провести в режиме очного или виртуального совещания. Регулирующему органу следует собрать отзывы и рассмотреть их в процессе принятия решения, которое может привести к пересмотру ранее одобренных мер. Хотя окончательное решение принимает регулирующий (или директивный) орган, все отзывы компаний должны быть задокументированы, а регулирующий орган должен объяснить, как они были (или почему не были) приняты во внимание.

5.4.5 Сценарий 5: принять за основу собственные стратегии компаний, не опираясь на систему показателей эффективности кибербезопасности

Этот сценарий также имеет отношение к РППЭ (регулирование по показателям эффективности), но в этом случае регулирующий орган принимает, что система РППЭ недостаточна развита для ее применения в целях регулирования. Более того, поскольку эта система базируется на самооценке, полученные с ее помощью результаты недостаточно надежны для решения вопросов о стимулировании, поэтому, регулирующий орган опирается на перспективные проекты (поэтому этапы те же, что и в методике

«затраты-плюс»). Это позволяет придерживаться основных принципов РППЭ, исходя из того, что операторы имеют достаточно знаний и информации для принятия более правильных решений, чем регулирующий орган.

- **Этап 2** *Определить меры противодействия киберугрозам.* Задача этого этапа — дать компаниям возможность принимать собственные стратегии кибербезопасности, вкладывать средства на совершенствование собственной организационной структуры и повышение информированности персонала, приобретать профессиональные знания и опыт. Регулирующий орган определяет четыре направления, по которым компании могут подавать свои предложения:

  - разработка и внедрение модели организации системы кибербезопасности;
  - определение и принятие комплекса правил и регламента повседневного управления системой кибербезопасности;
  - повышение квалификации персонала, отвечающего за кибербезопасность; а также
  - проведение внутренних информационных кампаний по повышению уровня осведомленности персонала о киберугрозах.

- **Этап 3** *Разработать нормативы, регулирующие затраты на контрмеры.* Регулирующий орган допускает следующие затраты: (1) техническая подготовка персонала, (2) программы повышения уровня общей осведомленности о киберугрозах, (3) создание специализированного подразделения по кибербезопасности, (4) аппаратные и программные средства, связанные с кибербезопасностью. Заявки принимаются на финансирование в объеме до 65 %, так как эти суммы считаются частью плановых расходов на основную деятельность, а верхний фиксированный лимит на совокупную сумму расходов определяется в соответствии с характеристиками и размерами предприятия-оператора. Регулирующий орган определяет бюджет. Компании подают заявки в соответствии с установленным порядком в режиме онлайн. По всем заявкам, соответствующим требованиям, финансирование выделяется в хронологическом порядке до исчерпания бюджетных средств. Регулирующий орган определяет правила мониторинга, оценки и рассылки результатов проектов внутри энергетического сектора, чтобы все операторы энергосистемы могли ознакомиться с инновационными подходами своих коллег.

- **Этап 4** *Определить порядок отчетности*. Все затраты должны быть документально подтверждены и обоснованы. Помимо обычной отчетности по затратам, компании обязаны показать, что проектные работы проведены в дополнение к основной деятельности.

- **Этап 5** *Проверить расходы и соблюдение нормативов*. Регулирующий орган проводит аудит для проверки по факту соответствия выполненных работ нормативам, а расходов – заявленным планам.

- **Этап 6** *Обновить план-график*. Регулирующий орган приглашает компании принять участие в однодневных семинарах по самооценке и проанализировать достигнутый ими уровень развития с помощью опытных методистов. Результаты семинаров используются компаниями для актуализации собственной стратегии

кибербезопасности, а регулирующим органом — для получения отзывов, которые помогут скорректировать будущую политику.

6 Заключение

Настоящие Методические указания содержат ряд предложений и рекомендаций по решению проблем кибербезопасности, подготовленных для регулирующих органов стран Европы и Евразии, а именно:

- Принципы определения затрат и некоторых контрольных значений для сравнительного анализа; в обсуждении используются, главным образом, результаты оценки затрат на кибербезопасность, полученные в рамках проекта ESSENCE.
- Краткое описание анализа экономических результатов (роста затрат и экономии) вследствие введения стандарта либо обязательных контрмер; на примере показано, как применять данный анализ для теоретического расчета затрат и полезного эффекта от соблюдения стандарта (контрмер).
- Оценка эффективности инвестиций, выделенных операторами на борьбу с киберугрозами в целях повышения уровня кибербезопасности энергосистемы. Анализ текущей системы показателей кибербезопасности, в заключение которого дана рекомендация дополнить показатели развития экспериментальными метриками производительности, недавно предложенными Научно-исследовательским институтом электроэнергетики (EPRI), несмотря на то, что этот метод недостаточно отработан.
- Схема выработки подхода регулирующего органа к кибербезопасности по методикам «затраты плюс» и РППЭ. Основная идея – проследить весь процесс от разработки принципов до их практического применения на базе фактических данных о состоянии энергосистемы. Все сценарии начинаются с одного и того же этапа: формирования стратегии кибербезопасности. Стратегия в свою очередь базируется на представлении регулирующего органа о том, каким должна быть система кибербезопасности в отрасли, то есть, ценности, которыми руководствуется регулирующий орган: его цели и то, каких изменений на рынке электроэнергии он ожидает в ответ на реализации своей стратегии.
- Пять возможных сценариев, в которых показано, как применяется вышеописанный процесс принятия решений. Подчеркнем, что эти сценарии показывают лишь пять из сотен возможных вариантов. Преимущество этих сценариев в том, что они позволяют продемонстрировать применение предложенной схемы на практике, показать, что выбор зависит от исходной ситуации и от принципов, лежащих в основе регулирования. Сценарии также показывают, что в одной и той же стране могут одновременно применяться разные подходы, например, когда общее регулирование осуществляется по методике «затраты-плюс», а для решения узкоспециальных задач в виде эксперимента применяется метод РППЭ.

Наконец, «Методические указания» содержат описания средств и методик, причем регулярно предлагается несколько вариантов их применения. Достаточно подробно освещаются основные принципы применения средств и методик, однако универсальных решений «под ключ» не приводится. Итак, каким образом регулирующие органы могут определить необходимые шаги, в особенности, те из них, кто только приступает к работе по организации госрегулирования в сфере кибербезопасности? Что выбрать из множества имеющихся вариантов? Мы полагаем, что регулирующим органам следует вначале проанализировать ситуацию, сложившуюся на сегодня в системе госрегулирования

энергетики, и ответить на ряд вопросов, которые могут серьезно повлиять на их выбор. Ниже дан список вопросов, с которых следует начинать оценку:

- *Каковы наши цели? С чего нам начать?* Определение стратегии и приоритетов помогает сосредоточиться на начальных этапах этого очень трудоемкого процесса. Начинайте с плана, но не тратьте время на его совершенствование; это также заставит операторов обдумать свою стратегию. Опыт регулирующих органов в США показывает, что, приступив к работе, даже если это и кажется каплей в море, вы накопите опыт, получите отзывы и начнете взаимодействие с компаниями, что сыграет важную роль в формировании и дальнейшем совершенствовании стратегии.

- Какие *сильные и слабые стороны, возможности и угрозы* в сфере кибербезопасности присутствуют у основных операторов энергосистем и других коммунальных служб нашей страны? Анализ фактической ситуации в отрасли поможет найти наилучшее решение. Если ситуация неясна, важно начать задавать вопросы операторам, причем несущественно, будут ли эти вопросы изначально правильными. В свою очередь, операторы начнут задумываться о собственной кибербезопасности, что уже немало.

- *Имеются ли регулирующее законодательство или административно-правовые нормы,* расширяющие или сдерживающие действия регулирующих органов в этой сфере? Переход на новые методы регулирования осуществить проще, если действовать с учетом нормативно-правовой базы и действующих правовых инструментов.

- *Какие соглашения о взаимопомощи* имеются (если имеются) на сегодня? Начальные этапы процесса весьма затратные, им препятствует инерционность. Но кибербезопасность касается не отдельно взятой страны, это общая проблема взаимосвязей в регионе, поэтому включение проблем кибербезопасности в соглашения о взаимопомощи по широкому кругу вопросов вполне естественно.

- Достаточно ли у нас *штатных квалифицированных специалистов,* которые могли бы выделить затраты на кибербезопасность и сравнить их с контрольными показателями (методика «затраты-плюс»)? Есть ли у операторов и наших штатных сотрудников опыт применения показателей *эффективности* (в информационных сетях или другой сфере) (методика РППЭ)? Эти вопросы помогают оценить плюсы и минусы различных подходов.

В странах ЕС (и отдельных штатах США) действуют разные стратегии регулирования, некоторые из них пока не вышли за рамки предварительного изучения вопроса. Это показывает, что до выработки эталонного подхода пока далеко.[40] Вероятно, он и вовсе не

[40] Показателен в этом плане пример Управления рынков газа и электроэнергии (OFGEM) (Великобритания), описанного в Приложении 4, поскольку в этой организации уже сформирован высокотехнологичный комплексный подход к регулированию в сфере кибербезопасности.

появится, потому что регулирование не сводится к техническим вопросам. Оно осуществляется на основе системы ценностей, общей концепции развития и законодательной базы в каждой отдельной стране. Однако бессмысленно ожидать, ничего не предпринимая, пока сформируется ясная, полная и отвечающая специфике отдельной страны картина. Регулирующим органам следует немедленно приступить к работе и начать извлекать уроки из собственных действий, потому что опыт поможет лучше ответить на вопросы, чем фолианты в тысячу страниц, морально устаревающие через полгода после выхода в свет. «Методические указания» призваны помочь регулирующим органам освоиться в новой парадигме и научиться проявлять гибкость в условиях постоянных перемен, чтобы помочь операторам поднять свой уровень готовности и способность успешно реагировать на киберугрозы.

7 Литература

Angeletti, Valentino, Luca Guidi, Daniela Pestonesi, Marco Biancardi, Marco Alessi, Graziano Abrate, Clementina Bruno, Fabrizio Erbetta, Giovanni Fraquelli, Azahara Lorite-Espejo. 2014. *Italian Case Study: Socio-Economic Impact Analysis of a Cyberattack to a Power Plant in an Italian Scenario. Cost and Benefit Estimation of CIPS Standard Adoptions. A Reduced Version*. Ceris Technical Reports - Special ESSENCE series on Security Standards for Critical Infrastructures, no. 55. National Research Council of Italy, Research Institute on Business and Development (CNR-CERIS).

http://essence.ceris.cnr.it/images/documenti/RT_55.pdf

(Пример реализации в Италии. Анализ общественно-экономического воздействия кибератаки на электростанцию в итальянском сценарии. Оценка затрат и полезного эффекта принятия стандартов CIPS. Сокращенная редакция)

Bartosewicz-Burczy, H., C. Bruno, F. Garcia, T. Wlodarczyk. 2014. *Polish Case Study (Пример реализации в Польше). Scenario Based Assessment of Costs and Benefits of Adoption of Comprehensive CIP Standards.* Ceris Technical Reports - Special ESSENCE series on Security Standards for Critical Infrastructures, no. 56. National Research Council of Italy, Research Institute on Business and Development (CNR-CERIS).

http://essence.ceris.cnr.it/images/documenti/RT_56.pdf

(Оценка затрат и полезного эффекта принятия комплекса стандартов CIP на основе сценариев)

Bruno C., A. Lorite-Espejo, H. Bartoszewicz-Burczy, A. Cortes, E. Doheijo, A. Diu, U. Finardi, E. Ragazzi, G. Falavigna, V. Moiso, L. Guidi, D. Pestonesi, T. Wlodarczyk, G. Abrate, F. Erbetta, G. Fraquelli. 2014. *Benefit Analysis. Assessing the Cost of Blackouts in Case of Attack. Evaluation Based on Italian and Polish Case Studies*. Ceris Technical Reports - Special ESSENCE series on Security Standards for Critical Infrastructures, no. 52. National Research Council of Italy, Research Institute on Business and Development (CNR-CERIS).

http://www.ceris.cnr.it/ceris/rt/RT_52.pdf

(Анализ полезного эффекта. Оценка издержек отключений в случае атаки. По материалам примеров реализации в Польше и Италии)

Cadmus Group. 2018. *Cybersecurity Strategy Development Guide*. NARUC Center for Partnerships and Innovation.

https://pubs.naruc.org/pub/8C1D5CDD-A2C8-DA11-6DF8-FCC89B5A3204

(Пособие по разработке стратегии кибербезопасности)

Cadmus Group. 2019. *Cybersecurity Preparedness Evaluation Tool*. NARUC Center for Partnerships and Innovation.

https://pubs.naruc.org/pub/3B93F1D2-BF62-E6BB-5107-E1A030CF09A0

(Средство оценки готовности в кибербезопасности)

Calabrese G., U. Finardi, E. Ragazzi. 2014. *Cost Analysis of Standard Implementation in the SCADA Systems of Electric Critical Infrastructures*. Ceris Technical Reports - Special ESSENCE series on Security Standards for Critical Infrastructures, no. 53. National Research Council of Italy, Research Institute on Business and Development (CNR-CERIS).

http://essence.ceris.cnr.it/images/documenti/RT_53.pdf

(Анализ затрат на внедрение стандартов в системах АСУ ТП объектов критической инфраструктуры в электроэнергетике)

Choueiki, Hisham. 2019. *Promoting Transparency and Public Participation in Energy Regulation: A Communications Primer for Utility Regulators*. NARUC.

https://www.naruc.org/international/news/promoting-transparency-and-public-participation-in-energy-regulation-a-communications-primer-for-utility-regulators/

(Повышение уровня гласности и участия общественности в регулировании в энергетике. Вводный курс по коммуникациям для органов государственного регулирования энергокомпаний)

Christopher, Jason D., Fowad Muneer, John Fry, Paul Skare. 2014. *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) - Version 1.1*. Washington DC: U.S. Department of Energy.

https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0

(Модель зрелости возможностей кибербезопасности в электроэнергетике. Версия 1.1.)

CISA (U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency (CISA). n.d. “Critical Infrastructure Sectors.”

https://www.cisa.gov/critical-infrastructure-sectors

(Отрасли, относящиеся к критической инфраструктуре). Доступ 17.01.2020.

CMMI Institute, 2019. “What is CMMI?”

https://cmmiinstitute.com/cmmi/intro

(Что такое CMMI)

CNR-IRCrES (The National Research Council of Italy, Research Institute on Sustainable Economic Growth). n.d. Emerging Security Standards to the EU power Network controls and other Critical Equipment (ESSENCE)

http://essence.ceris.cnr.it/

(Новые стандарты безопасности на средства управления электрическими сетями и другим критически важным оборудованием в ЕС (ESSENCE). Веб-сайт. Доступ 17.01.2020.

Costantini, Lynn P., Matthew Acho. 2019. *Understanding Cybersecurity Preparedness: Questions for Utilities*. NARUC Center for Partnerships and Innovation.

https://pubs.naruc.org/pub/3BACB84B-AA8A-0191-61FB-E9546E77F220

(Как оценить готовность в сфере кибербезопасности. Вопросы к энергокомпаниям)

DHS (U.S. Department of Homeland Security). n.d. “Critical Infrastructure Security.”

https://www.dhs.gov/topic/critical-infrastructure-security

(Безопасность критической инфраструктуры). Доступ 17.01.2020.

EPRI (Electric Power Research Institute), 2017, “Cyber Security Metrics for the Electric Sector.”

https://www.epri.com/#/pages/product/000000003002010426/?lang=en-US

(Характеристики кибербезопасности в электроэнергетике). Доступ 06.02.2020

EU (EC) (European Union). 2008. “Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance).” *Official Journal of the European Union* L no. 345 (2008): 75–82.

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

(Директива Совета Европы 2008/114/ЕС от 8 декабря 2008 г. Об определении и назначении объектов критической инфраструктуры в Европе и об оценке необходимости совершенствования их защиты. Распространяется на Европейскую экономическую зону)

Huang L., Q. Zhu. 2019. “Adaptive Strategic Cyber Defense for Advanced Persistent Threats in Critical Infrastructure Networks.” In: *Performance Evaluation Review* 46, no. 2: 52-56,

https://doi.org/10.1145/3305218.3305239

(Киберзащита на основе адаптивной стратегии от развитых устойчивых угроз сетям на объектах критической инфраструктуры)

Huang L., Q. Zhu. 2020. “A Dynamic Games Approach to Proactive Defense Strategies against Advanced Persistent Threats in Cyber-Physical Systems.” In: *Computers and Security* 89 (2020).

https://doi.org/10.1016/j.cose.2019.101660

(Подход на основе динамических игр к стратегиям упреждающей защиты от развитых устойчивых угроз к кибернетико-физических системах)

IEC (International Electrotechnical Commission). 2009. *IEC TS 62443-1-1:2009*. IEC.

https://webstore.iec.ch/publication/7029#additionalinfo

Keogh M., Thomas S. 2017. *Cybersecurity. A Primer for State Utility Regulators. Version 3.0*. NARUC Center for Partnerships and Innovation.

https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F

(Кибербезопасность. Вводный курс для органов государственного регулирования в энергетике)

Lee, A. C. Suh-Lee. 2016. *Creating Security Metrics for the Electric Sector, Version 2.0*. Palo Alto, CA: Electric Power Research Institute.

https://www.epri.com/#/pages/product/3002007886/?lang=en-US

(Разработка характеристик кибербезопасности для электроэнергетики)

Lewis, J. M. 2015. “The Politics and Consequences of Performance Measurement.” In: *Policy and Society* 34 no. 1: 1–12.

https://doi.org/10.1016/j.polsoc.2015.03.001

(Политика и последствия измерений эффективности)

NARUC (National Association of Regulatory Utility Commissioners). 2017a. *Black Sea Cybersecurity Strategy Development Guide* NARUC

https://pubs.naruc.org/pub.cfm?id=E20048B4-155D-0A36-3117-F2F0A7A692F4

(Пособие по разработке стратегии кибербезопасности для Черноморского региона)

NARUC 2017b. *Cybersecurity Evaluative Framework for Black Sea Regulators.* NARUC

https://pubs.naruc.org/pub.cfm?id=E3CE75B5-155D-0A36-31FD-1B268F7BD125

(Общие принципы оценки кибербезопасности для регулирующих органов Черноморского региона)

Nemertes 2017. *The Nemertes Security Maturity Model.* Nemertes Research.
https://nemertes.com/research/nemertes-security-maturity-model/
(Модель зрелости возможностей Nemertes)

NERC (North American Electric Reliability Corporation). 2016. *Security Management in the Electricity Sub-Sector Version 1.1*. NERC.
https://www.mro.net/MRODocuments/Security%20Management%20in%20the%20Electricity%20Sub-Sector%20Version%201.1%20September%202016.pdf
(Управление безопасностью в электроэнергетической подотрасли)

NERC. n.d. “CIP Standards.” Standards. NERC.
https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
(Стандарты CIP)

NIST (National Institute of Standards and Technology). 2018. *Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1*. NIST.
https://www.nist.gov/cyberframework/framework
(Основные принципы повышения уровня кибербезопасности объектов критической инфраструктуры)

NIST. n.d.a. “Advanced Persistent Threat.” Computer Security Resource Center Glossary.
https://csrc.nist.gov/glossary/term/advanced-persistent-threat
(Глоссарий Центра ресурсов компьютерной безопасности. Развитая устойчивая угроза). Доступ 17.01.2020.

NIST. n.d.b. “Cyber Security.” Computer Security Resource Center Glossary.
https://csrc.nist.gov/glossary/term/Cyber-Security
(Глоссарий Центра ресурсов компьютерной безопасности. Кибербезопасность). Доступ 17.01.2020.

Suh-Lee, C. 2017. *Creating Security Metrics for the Electric Sector, Version 2.0. Volume 3*. Palo Alto, CA: Electric Power Research Institute.
https://www.epri.com/#/pages/product/3002010426/?lang=en-US
(Характеристики кибербезопасности для электроэнергетики. Том 3)

С вопросами по настоящей публикации просим обращаться:
Colleen Borovsky (Коллин Боровски) (cborovsky@naruc.org)
Erin Hammel (Эрик Хэммел) (ehammel@naruc.org).

NARUC (National Association of Regulatory Utility Commissioners)

1101 Vermont Ave, NW, Suite 200
Washington, DC 20005 USA — США
Тел.: +1-202-898-2210
www.naruc.org