Экономический и Социальный Совет

Distr.: General
27 July 2023
Russian
Original: English

Европейская экономическая комиссия

Комитет по устойчивой энергетике

Группа экспертов по системам экологически чистого производства электроэнергии
Девятнадцатая сессия
Женева, 3–4 октября 2023 года
Пункт 7 предварительной повестки дня
Надежность и киберустойчивость «умных» интегрированных энергетических систем

Группа экспертов по энергоэффективности
Десятая сессия
Женева, 5–6 октября 2023 года
Пункт 6 предварительной повестки дня
Цифровизация и устойчивость энергосистем

Ключевые соображения и решения для обеспечения киберустойчивости «умных» интегрированных энергетических систем

Записка секретариата

Резюме

Цифровизация в форме применения цифровых технологий и бизнес-моделей для существующих процессов привлекает все большее внимание как способ поддержки и дополнения энергетического перехода. Однако интеграция различных источников энергии и объединение различных компонентов энергосистем, составляющих «умные» интегрированные энергосистемы, предполагают обмен большими объемами данных, что повышает подверженность рискам кибербезопасности.

Настоящий документ был разработан на платформе Целевой группы по цифровизации в энергетике Группой экспертов по энергоэффективности и Группой экспертов по системам экологически чистого производства электроэнергии в соответствии с их соответствующими планами работы на 2022–2023 годы и с учетом растущих угроз информационной безопасности на фоне усиливающейся цифровизации энергетической системы. Целевая группа по цифровизации в энергетике также признает важность сотрудничества между всеми вспомогательными органами Комитета по устойчивой энергетике в рамках усилий по рассмотрению аспектов, характерных для различных элементов производственно-сбытовой цепочки в энергетике.

В документе содержится общий обзор по теме, описание и классификация типов кибератак на уязвимые компоненты энергосистемы и их возможные последствия; в заключение в нем приведен набор мер управленческого и технического характера, а также и рекомендации по вопросам политики, которые направлены на снижение рисков в области кибербезопасности.

I. Введение

1. С ростом интеграции возобновляемых источников энергии переменной мощности все чаще возникают ситуации избытка и дефицита энергии. В ответ на этот вызов надежности развивается концепция «умных» интегрированных энергетических систем», объединяющих разные источники и накопители энергии и открывающих возможности для проявления активной роли «просьюмера»[1].

2. Помимо интеграции разных источников энергии, эти «умные» системы содержат различные подключенные компоненты, позволяющие собирать детальные данные о производстве, передаче, распределении и потреблении энергии в режиме реального времени, а также анализировать эти данные с помощью таких инструментов, как искусственный интеллект (ИИ), что позволяет по-новому взглянуть на проблему и за счет этого получать более точные прогнозы и более эффективно поддержать принимаемые решения в области планирования, эксплуатации и технического обслуживания. Благодаря таким многосторонним взаимосвязям сложилась основанная на широкой цифровизации «умная» система, получившая название «"Умная" сеть». Такие системы могут быть как однонаправленными (когда сбор данных осуществляется без обратной связи), так и двунаправленными (когда собранные данные анализируются и используются для контроля, эксплуатации и/или управления конкретным оборудованием или устройствами). Кроме того, «умные» интегрированные энергетические системы могут координировать потребности и возможности всех генерирующих предприятий, операторов энергосистем, конечных потребителей и участников рынка электроэнергии. Таким образом, создаются благоприятные условия для работы системы с максимальной эффективностью, надежностью, отказоустойчивостью, гибкостью и стабильностью при минимизации затрат и воздействия на окружающую среду и максимальном увеличении возможностей системы.

3. На более высоком уровне цифровизации и интеллектуализации могут быть предложены различные решения, включая управление спросом на электроэнергию, снятие пиков нагрузки (приоритетное потребление энергии в периоды низкого спроса) и накопление избыточной энергии. Кроме того, цифровизация позволяет прогнозировать потоки энергии и дает возможность изменять поведение поставщиков, потребителей и покупателей энергии с помощью налогообложения, ценовых сигналов или мер политики.

4. Хотя использование «умной» интегрированной энергетической системы создает многочисленные преимущества, в этой связи также появляются и свои проблемы. Одной из таких проблем является повышенная подверженность риску кибератак. Такой риск является неотъемлемым следствием перехода от разрозненных физических устройств к «умным» устройствам и интегрированному через подключение к коммуникационным сетям оборудованию.

5. В общем случае целью кибератак является захват контроля над системой и/или данными, и/или повреждение физического оборудования, следствием чего являются репутационный ущерб либо снижение доверия к организации. Это означает, что в контексте «умных» интегрированных энергетических систем их цель состоит в том, чтобы взять под контроль энергетическую систему таким образом, чтобы помешать ее способности поставлять энергию.

6. Увеличение количества устройств только повышает вероятность кибератак. Это связано с тем, что датчики, реле, устройства управления машинами, контрольно-измерительные приборы и т.д. имеют разные поверхности атаки. Поверхностью атаки называют совокупность всех точек входа, которые хакеры могут использовать для установления контроля над системой, включая сеть, используемую для соединения ее компонентов. В случае «умной» интегрированной энергетической системы поверхность атаки включает в себя по меньшей мере те компоненты, которые

[1] GEEE-7/2020/INF.3 (https://unece.org/sites/default/files/2020-12/GEEE-7.2020.INF_.3.pdf).

связанны с генерацией, транспортировкой, сетями передачи и распределения энергии, накопителями энергии, энергопотребляющими устройствами и цифровой сетью связи.

A. Кибератаки на компоненты «умных» интегрированных энергетических систем и примеры их последствий

7. Поскольку энергетическая система отнесена к критической инфраструктуре, а энергетика является основой общества, последствия кибератак могут иметь далеко идущие последствия, в том числе последствия экономического, социального и экологического характера. Несколько недавних примеров кибератак, произведенных на критически важные инфраструктурные объекты с целью вымогательства, приведших к их временному выводу из эксплуатации и потере данных, свидетельствуют о тенденции к их росту: если в 2022 году количество атак с целью вымогательства увеличилось почти вдвое, то только за последние 6 месяцев этого года количество групп-вымогателей, оказавших воздействие на объекты промышленной инфраструктуры, выросло на 35 %, а количество вредоносных программ и программ вайперов — на 53 %[2].

8. Такая тенденция неудивительна, учитывая, что предотвращение кибератак и смягчение их последствий — задача не из простых; кроме того, кибербезопасности зачастую не уделяется должного внимания на всех этапах, начиная от проектирования до эксплуатации, в то время как «умная» интегрированная энергетическая система имеет огромную поверхность атаки. Подверженные кибератакам компоненты «умной» интегрированной энергетической системы, которые используют для генерации, передачи, распределения энергии, указаны в таблице 1.

Таблица 1
Некоторые компоненты «умной» интегрированной энергетической системы, используемые для генерирования, передачи, распределения и использования энергии

Генерирование	*Передача*	*Распределение, распределенные энергоресурсы и потребители*
Устройства контроля оборудования Системы технологического управления Устройства защиты (реле и т. д.) Устройства регистрации Интерфейсы для подключения к системе управления генерацией, системе диспетчерского контроля и сбора данных, пульту технического обслуживания и т. д.	Оптические трансформаторы Устройства контроля оборудования Устройства защиты (реле и т. д.) Аппаратура для измерения фазы Системы технологического управления Устройства регистрации Интерфейсы для подключения к системе управления энергопотреблением, системе диспетчерского контроля и сбора данных, к пульту технического обслуживания и т. д. Средства автоматизации подстанций Дистанционная оконечная аппаратура	Усовершенствованная инфраструктура учета («умные» счетчики) Средства автоматизации (средства для автоматического повторного включения, фидеры и т. д.) Устройства защиты Средства индивидуальной мобильности Средства контроля и управление для: ▪ солнечных панелей ▪ аккумуляторов (хранение) ▪ электромобилей и их зарядке ▪ «умных» зданий ▪ микросети Управление нагрузкой Средства для взаимодействия с клиентами

[2] Fortinet, *Global Threat Landscape Report. A Semiannual Report by FortiGuard Labs* (February 2023).

9. Эти подключенные и «умные» устройства, серверы, компьютеры и системы, используемые в «умной» интегрированной энергетической системе, содержат различные компоненты, которые могут быть потенциально атакованы описанными ниже способами:

a) серверы: посредством использования сервисов, которые не должны быть доступны внешнему миру, эксплуатации устаревшего программного обеспечения с известными уязвимостями, эксплуатации таких небезопасных параметров конфигурации, как пароли по умолчанию, а также посредством получения несанкционированного доступа к конфиденциальным данным;

b) сети: посредством обхода процедуры аутентификации, перегрузки сети, нарушающей ее нормальное функционирование, эксплуатации таких небезопасных параметров конфигурации, как слабое шифрование, а также посредством получения несанкционированного доступа к коммуникационным данным других пользователей;

c) веб-сайты: посредством использования функциональных возможностей, которые не должны быть доступны, эксплуатации известных уязвимостей, эксплуатации таких небезопасных параметров конфигурации, как пароли по умолчанию, получения несанкционированного доступа к конфиденциальным данным, например к основной базе данных или сеансу незашифрованной связи, получения несанкционированного доступа к базовому серверу, атаки на других пользователей и загрузки вредоносной программы;

d) приложения на мобильных устройствах: посредством использования функциональных возможностей, которые не должны быть доступны, эксплуатации известных уязвимостей, эксплуатации таких небезопасных параметров конфигурации, как пароли по умолчанию, получения несанкционированного доступа к конфиденциальным данным, например к основной базе данных или сеансу незашифрованной связи, а также посредством получения несанкционированного доступ к базовому мобильному устройству;

e) программное обеспечение и встроенные программы: посредством обхода процедуры аутентификации, эксплуатации известных уязвимостей, эксплуатации таких небезопасных параметров конфигурации, как неправильное управление правами, а также посредством получения несанкционированного доступа к конфиденциальным данным, например к исходному коду;

f) веб-сервисы: посредством эксплуатации известных уязвимостей, эксплуатации таких небезопасных параметров конфигурации, как аутентификация без пароля, получения несанкционированного доступа к конфиденциальным данным, например, к данным других пользователей, а также посредством несанкционированного доступа к базовому серверу;

g) облака: посредством получения несанкционированного доступа к данным других пользователей, например к файлам, эксплуатации несанкционированного доступа к базовому серверу, эксплуатации таких небезопасных параметров конфигурации, как аутентификация путем угадывания пароля, получения несанкционированного доступа к конфиденциальным данным, например к паролям или ключам доступа, а также посредством эксплуатации известных уязвимостей;

h) датчики, электромоторы, реле и т. д.: посредством эксплуатации известных уязвимостей программного обеспечения, эксплуатации небезопасных настроек конфигурации, вмешательства в данные, передаваемые датчиком/электромотором/реле/и т. д., манипулирования функциональностью датчика/электромотора/реле и т. д., отключения датчика, получения несанкционированного доступа к данным;

i) аппаратные средства: посредством манипуляции с аппаратными средствами, добавления вредоносного оборудования в сеть, атаки на интерфейсы, предоставляемые для поиска проблем, а также манипуляции с передаваемыми данными;

j) пользователи: посредством вредоносных писем, например фишинговых, предлагающих читателям предоставить конфиденциальные данные или прилагаемых файлов с вредоносным ПО, запугивания людей, с тем чтобы они непроизвольно совершили действие, наносящее им вред, дезинформации, провоцирующей на передачу конфиденциальной информации.

10. Потенциально возможны и многие другие виды атак. Их можно разделить на четыре типа:

a) физические атаки (на физические компоненты системы), в том числе:

i) причинение физического ущерба: атака на компонент, приводящая к его физическому повреждению, сбою в его работе или неработоспособности;

ii) социальная инженерия: обман и манипулирование людьми с целью заставить их поделиться конфиденциальной информацией, которая может быть использована для дальнейших атак;

iii) вскрытие узла или внедрение вредоносного узла: узел в «умной» интегрированной энергетической системе представляет собой элемент, соединяющий физическое устройство с Интернетом и отвечающий за сбор данных, их обработку и/или управление ими. Вмешательство в конфиденциальные данные означает не только их чтение, но и изменение. Это может быть достигнуто путем атаки на существующий узел, а также путем добавления нового узла.

b) Программные атаки (на компьютерные программы, выполняемые физическими устройствами «умной» интегрированной энергетической системы), в том числе:

i) вредоносные скрипты: добавление к существующему программному обеспечению дополнительных вредоносных функций, например для кражи регистрационных данных;

ii) вредоносное ПО: установка программного обеспечения, которое может поддерживать все виды вредоносных действий, например программы-шпиона для кражи данных, вирусов для повреждения или изменения файлов и/или данных, программ вайперов для стирания данных и программного обеспечения, а также вымогательского программного обеспечения для шифрования данных;

iii) отказ в обслуживании: атака типа «отказ в обслуживании» (DoS) делает программное обеспечение или устройство недоступным, например посредством его перегрузки или вывода из строя. Если такая атака осуществляется со многих компьютеров одновременно, она называется распределенной атакой типа «отказ в обслуживании» (DDoS).

c) Сетевые атаки (получение несанкционированного доступа и выполнение несанкционированных действий в сети), в том числе:

i) анализ трафика: получение информации на основе изучения характеристик потока данных, которые можно наблюдать, даже если содержание потока данных остается скрытым;

ii) маршрутизация информации: перехват, изменение и/или перенаправление данных, передаваемых по сети, в другой пункт назначения, например для мониторинга или кражи данных, или нарушения предоставляемых энергосистемой услуг;

iii) атаки типа «воронка»: вредоносный узел в сети посылает фальшивые сообщения другим узлам и обманным путем заставляет эти узлы передавать информацию вредоносному узлу;

iv) несанкционированный доступ: получение доступа к сети без разрешения.

d) Атаки с шифрованием (обход защиты путем шифрования, когда для превращения кода обратно в читаемую информацию или данные требуется ключ), в том числе:

i) криптоанализ: проводится для выяснения того, какая информация или данные зашифрованы без знания ключа;

ii) атака по стороннему каналу: использование информации, непреднамеренно предоставляемой компьютерной системой при выполнении криптографических операций, для получения доступа к зашифрованной информации;

iii) атака через посредника: расположение между двумя взаимодействующими компонентами, благодаря чему зашифрованные сообщения могут быть перехвачены и даже изменены.

11. Зачастую одновременно могут наблюдаться разные типы кибератак, вследствие которых в работе потенциальных жертв происходит наложение проблем и сбоев. Кроме того, кибератаки могут дополняться физическими атаками других видов.

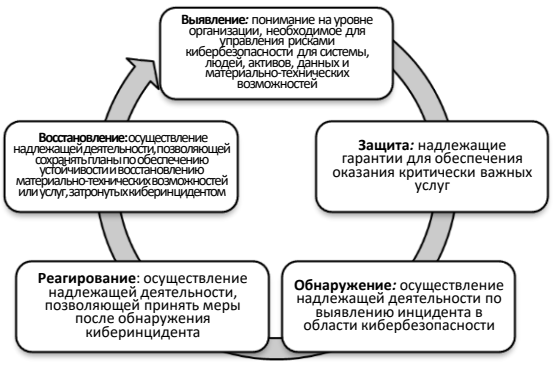
B. Меры по предотвращению кибератак на компоненты «умных» интегрированных энергетических систем

12. Поскольку «умная» интегрированная энергосистема является частью критической инфраструктуры, предотвращение кибератак имеет большое значение. А когда атаки все же происходят, их последствия должны быть смягчены. Для этого необходимо внедрить несколько решений, позволяющих сформировать общую, единую стратегию, которую иногда называют «защита в глубину».

13. Хорошими отправными точками для разработки и реализации эффективных программ в области кибербезопасности являются многие рамочные механизмы и стандарты; к их числу можно отнести, например, Framework for Improving Critical Infrastructure (Рамочный механизм по улучшению кибербезопасности критической инфраструктуры) Национального института стандартов и технологий (НИСТ) и серию стандартов 62443 Международной электротехнической комиссии (МЭК)[3].

14. Например, в Рамочном механизме НИСТ приводится детальный перечень видов деятельности, которые сгруппированы вокруг пяти основных функций, относящихся к разработке и внедрению (см. рис.). В нем также охвачены ресурсы (человеческие, материальные и финансовые), надзор (руководство), процессы и технологии.

Рисунок
Рамочный механизм НИСТ



Источник: подготовлено на основе материалов НИСТ, “NIST Releases Version 1.1 of its Popular Cybersecurity Framework” 16 April 2018.

15. Кроме того, предупреждение, смягчение последствий и восстановление должны осуществляться на управленческом и техническом уровнях (табл. 2).

[3] ISA/IEC 62443 series of standard, Automation and Control Systems Cybersecurity Standards.

Таблица 2

Некоторые виды деятельности по предотвращению, смягчению последствий и восстановлению для программ в области кибербезопасности

Уровень	*Предупреждение*	*Смягчение*	*Восстановление*
Управление (сверху вниз): меры политики и нормативное регулирование как информационная основа для персонала*	i) Управление рисками: включает выявление цифровых активов, к числу которых относится вся представляющая ценность цифровая информация, например, файлы с фотографиями, видео- и аудиофайлы и текстовые файлы. ii) Управление активами: пересмотр существующих мер безопасности и принятие дополнительных мер. iii) Управление обновлениями или патчами: поскольку устаревшее программное обеспечение увеличивает поверхность атак на него; при установке и развертывании обновлений администраторы должны руководствоваться регламентами управления обновлениями. iv) Системы кибербезопасности: межсетевые экраны могут использоваться для контроля входящего сетевого трафика на основе заранее заданных правил безопасности, обеспечивая тем самым только санкционированный доступ к сети или сегменту сети. Контроль доступа к сети (NAC) обеспечивает вход в сеть только аутентифицированных пользователей и устройств, которые прошли авторизацию и проверку на соответствие политикам безопасности. v) Разделение сетей: т. е. отделение сетей, особенно критически важной сети, от Интернета и других менее важных сетей, например административных, что снижает вероятность получения несанкционированного доступа к критически важной сети. vi) Управление доступом (включая аутентификацию и управление ключами): имена пользователей и пароли, а также другие средства аутентификации, например ключи, должны являться объектом для хранения и управления (предполагает создание, распространение, хранение и обновление). Чтобы обеспечить совместную работу различных элементов «умной» интегрированной энергетической системы, методы аутентификации в них должны совпадать. Выбор наиболее подходящего метода зависит от различных факторов, например от масштабируемости и безопасности. vii) Аттестация и анализ кода: аттестация кода означает проверку целостности программного обеспечения и уверенность в том, что оно не подвергалось вмешательству. Под	i) Система обнаружения вторжений: непрерывное наблюдение за системой и поиск аномалий. Аномалии могут принимать различные формы, например необычное количество попыток входа в учетную запись, необычный объем сетевого трафика с компьютера, наличие дополнительного устройства в сети и т. д. При обнаружении аномалии ее изолируют. Либо, когда с какого-либо компьютера отправляется необычно большой объем трафика, этот компьютер блокируется. Нередко об аномалии сообщают администратору сети для принятия в дальнейшем соответствующих мер. Поскольку возможны ложные срабатывания, для повышения эффективности обнаружения можно использовать машинное обучение и искусственный интеллект. ii) Методы предотвращения потери данных: они применяются в тех случаях, когда вирус пытается использовать или	В нормативные документы, основанные на этих стандартах, могут включаться пункты, посвященные планированию восстановления, предусматривающие процессы и процедуры, которые должны быть выполнены для обеспечения восстановления систем или активов, затронутых инцидентом кибербезопасности. Они должны использоваться в рамках управления непрерывностью бизнес-процессов для скорейшего возвращения к нормальной работе.

* Примечание: следует определить типы стратегий по предотвращению и смягчению последствий. Эти стратегии по предотвращению и смягчению последствий желательно закрепить в нормативных документах. Например, такое нормативное регулирование может быть реализовано в контексте стандартов серий IEC 62443 и ISO/IEC 27032:2012 «Information technology - Security techniques - Guidelines for cybersecurity standard (Информационная технология — Методы безопасности — Руководящие принципы для стандарта в области кибербезопасности) (https://www.iso.org/standard/44375.html). Первая из них посвящена кибербезопасности эксплуатируемых технологий в системах автоматизации и управления, а вторая — защите от взлома, саботажа или модификации конфиденциальных данных, систем, а также онлайновых операций и деятельности. При переходе к более высокому уровню безопасности — информационному — может быть применен стандарт ISO/IEC 27001:2022 «Системы менеджмента информационной безопасности» (https://www.iso.org/ru/standard/27001), который помогает организациям управлять информационной безопасностью путем решения вопросов, связанных с людьми, процессами и технологиями.

Уровень	*Предупреждение*	*Смягчение*	*Восстановление*
	анализом кода понимается проверка качества кода и гарантии отсутствия в нем проблем для безопасности, которые потенциально могут быть использованы злоумышленниками. Еще одним возможным решением для обеспечения безопасности системы является подход «нулевого доверия». viii) Защищенность устройств и программного обеспечения: защищенность компонентов «умной» интегрированной энергетической системы должна быть проверена, например, путем проведения теста на проникновение. ix) Криптография: обеспечение безопасного обмена данными и их сокрытия от несанкционированного доступа. Для преобразования данных в нераспознаваемые коды могут использоваться различные алгоритмы и методы в зависимости от критериев безопасности и контекста. Кроме того, в данном случае важна стойкость алгоритма. x) Информированность: использование, например, лайфхаков, для демонстрации того, как хакеры атакуют различные компоненты. Они могут использоваться не только для обучения технического персонала, но и нетехнического персонала тому, что они могут сделать для повышения уровня кибербезопасности. xi) Программа и культура кибербезопасности: обеспечение уверенности организаций в том, что все аспекты кибербезопасности учтены с учетом любых экономических, социальных и экологических рисков. xii) Использование стратегии «нулевого доверия», основанной на идее «никогда не доверяй, всегда проверяй», означает, что пользователи и устройства не должны быть доверенными по умолчанию, даже если они подключены к разрешенной сети.	переслать конфиденциальную информацию. Цель этих методов — предотвратить потерю информации и не допустить получения данных, пораженных вирусом. Этого можно добиться, изолировав зараженное устройство или заблокировав доступ с неавторизованных устройств.	
Технический (снизу вверх): выявленные проблемы доводятся до сведения руководства, обеспечивая обратную связь для совершенствования политики и нормативного регулирования	a) Анализ кода (по возможности, так как это возможно не для всех эксплуатируемых устройств): анализ кода означает анализ исходного кода приложения на предмет выявления уязвимостей. Этот анализ может быть статическим или динамическим. Статический анализ кода означает, что аналитик по вопросам безопасности имеет полный доступ к исходному коду и ищет уязвимости в строках кода. При динамическом анализе кода аналитик не имеет доступа к исходному коду, а выполняет компьютерную программу. Во время выполнения программа может быть просканирована на наличие уязвимостей. b) Сканирование уязвимостей: сканирование уязвимостей предполагает автоматическую оценку проблем безопасности систем и выполняемого на них программного обеспечения. Такое сканирование позволяет выявить возможные точки входа, через которые злоумышленники могут проникнуть в систему и использовать ее как ступень для дальнейших атак. c) Испытание на проникновение: тест на проникновение — это санкционированная кибератака на сеть, систему, устройство или программное обеспечение с целью проверки уровня безопасности тестируемого объекта. Цель этих тестов — выявить широкий спектр проблем безопасности. d) Атака «красной команды» имеет сходство с испытанием на проникновение, поскольку является санкционированной кибератакой. Основные отличия заключаются в том, что область	Операционный центр безопасности: группа специалистов по безопасности, осуществляющая мониторинг всей инфраструктуры информационных систем организации в целях обнаружения событий в области кибербезопасности в режиме реального времени и их максимально быстрого и эффективного устранения. Он выбирает, эксплуатирует и поддерживает технологии кибербезопасности организации, совершенствует возможности обнаружения угроз, обеспечения безопасности, реагирования и предотвращения, координирует все технологии и операции в	a) Цифровая криминалистика: предполагает сбор доказательств путем выявления, сбора и анализа данных и устройств, которые потенциально могут являться источником информации о кибератаке. Она также позволяет получать ценные сведения о том, как избежать кибератак в будущем. b) Устранение: устранение причины инцидента и

Уровень	*Предупреждение*	*Смягчение*	*Восстановление*
	применения испытания этого типа обычно шире, например оно проводится в масштабе компании, поскольку целью является поиск показательного примера далеко идущих последствий кибератаки в отличие от выявления широкого спектра проблем безопасности.	области кибербезопасности. Для выполнения своих функций она анализирует данные из различных источников, включая специальную информацию, полученную от компетентных органов и отраслевых организаций, в том числе информацию из системы управления информационной безопасности и событиями безопасности (SIEM), содержащую анализ поведенческих аномалий, проведенный с помощью искусственного интеллекта, для автоматического обнаружения кибератак и реагирования на них.	восстановление атакованной системы (систем) необходимо для того, чтобы вернуть их к нормальной работе (использование резервных копий, планов восстановления и планов обеспечения непрерывности бизнес-процессов).

III. Рекомендации по вопросам политики

16. С учетом вышесказанного о кибербезопасности «умных» интегрированных энергетических систем на рассмотрение предлагаются следующие выводы, меры и рекомендации по вопросам политики:

a) регулирование: обеспечение выполнения применимых стандартов и руководящих принципов, касающихся вопросов улучшения кибербезопасности эксплуатируемых технологий в области автоматизации, систем управления и кибербезопасности критической инфраструктуры;

b) финансы: предоставление налоговых льгот компаниям, внедрившим соответствующие стандарты кибербезопасности, а также выделение средств на реализацию таких инициатив в области кибербезопасности, как исследования, разработки и образование в области кибербезопасности;

c) структурные меры:

i) принятие национальных стратегий кибербезопасности, которые: описывают способы предотвращения кибератак на «умные» интегрированные энергетические системы и управление ими и; определяют роли и обязанности различных заинтересованных сторон, включая государственные учреждения, предприятия и частных лиц;

ii) сотрудничество с другими странами с целью сравнительного анализа их стандартов и обмена информацией о потенциальных субъектах угроз для более эффективного управления рисками кибербезопасности;

iii) реализация планов управления непрерывностью бизнес-процессов, описывающих порядок управления событиями, связанными с кибербезопасностью, в том числе, например, приводящими к отключению электроэнергии;

iv) обеспечение надлежащего распределения ответственности за кибербезопасность в энергетическом секторе (руководство кибербезопасностью) между заинтересованными сторонами на национальном и наднациональном уровнях;

d) отчетность: требование, касающееся представления официальным органам отчетности о защите данных и состоянии кибербезопасности для стимулирования осуществления стратегий «снизу вверх»;

e) повышение осведомленности: выявление лидеров отрасли, подающих пример, а также организация обучения и курсов подготовки для поддержки компаний и государственных органов в реализации мер в области кибербезопасности как на управленческом, так и на техническом уровнях.