Модельно-ориентированная киберфизическая защита энергетических объектов на основе платформы моделирования РАДУГА-ЭУ

В статье перечислены ограничения традиционных подходов к кибербезопасности при управлении технологическими процессами в реальном времени и предлагается дополнительный метод защиты, основанный на использовании расчетных моделей физических процессов. Рассмотрена возможность применения программной платформы моделирования РАДУГА-ЭУ, разработанной компанией «НПЦ Приоритет» и аттестованной Ростехнадзором, в качестве аналитического инструмента для выявления киберфизических аномалий в энергетических установках и объектах энергетической инфраструктуры. Предлагаемая архитектура позволяет выявлять аномальное поведение системы даже в тех случаях, когда управляющие команды являются корректными с точки зрения сетевого взаимодействия.

ООО «НПЦ Приоритет», г. Москва

Системы промышленного управления, применяемые на энергетических объектах, традиционно защищаются средствами классической кибербезопасности. К таким средствам относятся: сегментация сетей, системы обнаружения вторжений, контроль промышленных протоколов, механизмы аутентификации и контроля доступа. Эти меры существенно снижают вероятность несанкционированного доступа к системам управления. Однако они не обеспечивают полной защиты от сложных атак, которые могут осуществляться в рамках легитимных процедур управления технологическими процессами.

На энергетических объектах, включая электростанции и подстанции, управляющие команды напрямую связаны с физическими процессами, такими как регулирование температуры, давления, мощности, циркуляции теплоносителя и других параметров. Если злоумышленник изменяет параметры управления таким образом, что это не нарушает сетевые протоколы, традиционные системы кибербезопасности могут не обнаружить атаку.

Практика последних лет показывает, что вредоносные воздействия могут маскироваться под нормальные операции управления. Это требует разработки новых подходов, объединяющих методы кибербезопасности и анализа физических процессов.

Ограничения традиционных средств кибербезопасности для АСУ ТП

Большинство современных решений по кибербезопасности промышленных систем управления ориентированы прежде всего на защиту цифровой инфраструктуры: это мониторинг сетевого трафика, контроль корректности протоколов, обнаружение аномалий в сетевых взаимодействиях.

Однако системы управления технологическими объектами принципиально отличаются от традиционных информационных систем тем, что они управляют физическими процессами. Поведение таких систем определяется не только программной логикой, но и законами физики, включая термодинамику, гидродинамику, электромеханику, физику реакторов. Поэтому возможна ситуация, когда с точки зрения сетевой безопасности все выглядит корректно, но при этом физический процесс развивается аномально или опасно. Типичными примерами таких воздействий являются:

- постепенное изменение уставок управления;
- подмена показаний датчиков;
- согласованное изменение нескольких управляющих сигналов.

В таких случаях сетевые средства кибербезопасности могут оказаться неспособными обнаружить инцидент.

Концепция киберфизической безопасности

Для преодоления указанных ограничений в настоящее время развивается новое направление – киберфизическая безопасность. Основная идея этого подхода заключается в том, что необходимо контролировать не только сетевое взаимодействие, но и физическую согласованность технологического процесса. В рамках данного подхода система безопасности анализирует, соответствуют ли измеренные параметры технологического процесса значениям, которые долж-

ны наблюдаться согласно физической модели объекта. Если наблюдаемые параметры существенно отклоняются от расчетных значений, система может зафиксировать потенциальную аномалию или киберфизический инцидент.

Таким образом, формируется многоуровневая архитектура защиты, включающая:

- классические средства кибербезопасности;
- мониторинг поведения систем управления;
- анализ физической модели технологического процесса.

Роль моделей реального времени

Модели технологических процессов, работающие в режиме реального времени, могут стать важным инструментом киберфизической защиты. Такая модель описывает физическое поведение технологической системы и позволяет рассчитывать ожидаемые значения параметров при заданных условиях эксплуатации. Сравнение измеренных значений с расчетными значениями модели позволяет выявлять ситуации, при которых управляющие команды являются корректными, сетевой обмен выглядит нормальным, но физическое поведение системы становится несогласованным.

Такие отклонения могут свидетельствовать о неисправности оборудования, отказе датчиков, ошибках программного обеспечения или вредоносном вмешательстве в систему управления. Этот подход позволяет выявлять инциденты, которые не обнаруживаются традиционными средствами кибербезопасности.

Цифровые двойники ТЭС и АЭС как инструмент киберфизической безопасности

Для энергетических объектов, таких как тепловые и атомные электростанции, кибербезопасность не может рассматриваться исключительно как задача защиты сетевой инфраструктуры и информационных ресурсов. Управляющие воздействия в системах автоматизированного управления технологическими процессами напрямую влияют на физические процессы – теплогидравлику, электрические режимы, работу исполнительных механизмов, систем регулирования и защиты. Поэтому нарушение кибербезопасности в энергетических АСУ ТП фактически представляет собой кибер-физический инцидент, при котором воздействие на цифровую систему управления приводит к изменению физических параметров технологического процесса.

В последние годы в мировой научной литературе активно обсуждается использование цифровых двойников (Digital Twin) как инструмента повышения устойчивости таких систем. По удачно сформулированному определению из Wikipedia, цифровой двойник представляет собой динамическую цифровую модель физического объекта, синхронизированную с его состоянием в реальном времени и способную воспроизводить его поведение при различных режимах эксплуатации.

В контексте кибербезопасности цифровой двойник может использоваться для непрерывного сопоставления:

- фактически измеренных параметров объекта;
- расчетных параметров, получаемых из модели технологического процесса;
- прогнозных сценариев поведения системы при заданных управляющих воздействиях.

Такой подход позволяет выявлять ситуации, когда управляющие команды формально корректны, сетевой обмен не содержит признаков атаки, однако физическое состояние объекта начинает расходиться с допустимым режимом работы.

Особый интерес представляет использование цифровых двойников, работающих в режиме быстрее реального времени (faster-than-real-time). В этом режиме модель используется не только для диагностики текущего состояния системы, но и для прогнозного анализа. Модель может выполнять ускоренное моделирование развития технологического процесса и оценивать последствия подозрительных управляющих воздействий до того, как они приведут к опасным режимам.

Подобные подходы уже рассматриваются в исследованиях по безопасности систем SCADA и промышленных систем управления. Например, в ряде работ цифровые двойники используются для генерации сценариев атак и построения систем обнаружения вторжений, способных анализировать состояние технологического процесса и выявлять аномалии.

В других исследованиях (см. на сайте arxiv.org) предлагаются архитектуры безопасности, в которых цифровой двойник используется для моделирования технологического процесса и обнаружения атак типа FalseData-Injection, когда злоумышленник подменяет показания датчиков таким образом, что они остаются статистически правдоподобными.

Также предложены фреймворки, где цифровой двойник используется как часть системы обнаружения вторжений в ICS, позволяет моделировать различные сценарии атак и генерировать данные для обучения алгоритмов обнаружения аномалий (см. на сайте kth.diva-portal.org).

Особенно перспективным считается объединение цифровых двойников с алгоритмами машинного обучения и контекстно-ориентированными моделями технологических процессов. Такая комбинация позволяет:

- проводить непрерывный мониторинг состояния системы;
- прогнозировать возможные сценарии атак;
- автоматически формировать рекомендации по защитным действиям (см. link.springer.com).

Для энергетических объектов использование цифровых двойников имеет ряд дополнительных преимуществ. В отличие от многих промышленных систем, электростанции характеризуются высокой инерционностью процессов, сложной взаимосвязью параметров и строгими требованиями безопасности. Это делает модельно-ориентированный контроль особенно эффективным инструментом обнаружения отклонений. В связи с этим цифровой двойник может рассматриваться как отдельный уровень в архитектуре киберфизической защиты энергетического объекта:

- уровень традиционной кибербезопасности сети и вычислительной инфраструктуры;
- уровень контроля промышленных протоколов и команд управления;
- уровень анализа поведения технологического процесса на основе цифровой модели;
- уровень прогнозного анализа режимов работы системы.

Для платформ моделирования энергетических объектов, таких как РАДУГА-ЭУ, это открывает новое на-

правление применения. Платформа может использоваться не только для инженерных расчетов и анализа режимов работы ТЭС и АЭС, но и как компонент системы киберфизического мониторинга, обеспечивающей раннее выявление потенциально опасных отклонений технологического процесса.

Особенно перспективным является использование цифрового двойника в **режиме быстрее реального времени**, когда система моделирования способна выполнять ускоренные расчеты развития технологического процесса и заранее оценивать последствия управляющих воздействий. В этом случае цифровой двойник становится инструментом не только диагностики, но и прогнозной защиты технологических процессов энергетических объектов.

Применение платформы моделирования РАДУГА-ЭУ

Программная платформа РАДУГА-ЭУ может служить технологической основой для реализации описанного подхода. Она представляет собой систему моделирования сложных энергетических объектов, включая тепловые электростанции, атомные электростанции, энергетические инфраструктурные системы.

Платформа обеспечивает моделирование термодинамических процессов, моделирование систем управления и расчет параметров технологических процессов. Система разработана компанией «НПЦ Приоритет» и аттестована Ростехнадзором для выполнения инженерных расчетов энергетических установок.

Поскольку РАДУГА-ЭУ моделирует физическое поведение технологического объекта, ее можно использовать в качестве эталонной модели для выявления несоответствий между расчетным и фактическим поведением энергетической установки.

Предлагаемая архитектура системы включает три уровня.

Уровень 1 – система оперативного управления. Этот уровень включает стандартную инфраструктуру управления: программируемые логические контроллеры, SCADA-системы, рабочие станции операторов.

Уровень 2 – система кибербезопасности. На этом уровне работают традиционные средства защиты: мониторинг сетевого взаимодействия, обнаружение аномалий, контроль промышленных протоколов.

Уровень 3 – модель технологического процесса. На третьем уровне используется модель технологического объекта. Модель в режиме реального времени рассчитывает ожидаемые параметры технологического процесса. Измеренные значения сравниваются с расчетными значениями модели. Значительные отклонения могут свидетельствовать о возникновении кибер-физических аномалий.

Предлагаемый подход обладает рядом преимуществ. Во-первых, он позволяет выявлять аномалии даже в тех случаях, когда сетевой обмен выглядит полностью корректным. Во-вторых, данный метод не зависит исключительно от статистического анализа или методов машинного обучения, основанных на исторических данных. Вместо этого используется физическая модель объекта, основанная на фундаментальных законах. В-третьих, такой подход повышает вероятность раннего обнаружения опасных отклонений, что особенно важно для объектов критической инфраструктуры.

Сценарии киберфизических атак на энергетические объекты и их выявление с использованием цифрового двойника

Для оценки эффективности модельно-ориентированного подхода к обеспечению киберфизической безопасности рассмотрим два типовых сценария потенциальных атак на энергетические объекты. Такие сценарии отражают наиболее характерные особенности современных атак на промышленные системы управления: использование легитимных команд управления, постепенное изменение параметров технологического процесса и отсутствие явных аномалий в сетевом трафике.

Сценарий 1. Подмена данных датчиков (FalseDataInjection)

Одним из наиболее известных типов атак на системы промышленного управления является подмена данных датчиков. В этом случае злоумышленник получает доступ к сети системы управления и начинает изменять значения отдельных измерительных каналов.

Например, на тепловой или атомной электростанции могут быть подменены показания температуры теплоносителя, давления в контуре, расхода рабочей среды, электрической нагрузки генератора. При этом система управления продолжает работать в штатном режиме, поскольку управляющие алгоритмы получают формально корректные данные.

С точки зрения традиционных средств кибербезопасности ситуация может выглядеть нормальной:

- сетевые протоколы не нарушены;
- команды управления корректны;
- система авторизации не фиксирует несанкционированного доступа.

В результате оператор и система защиты могут долгое время не обнаруживать отклонение режима.

Однако цифровой двойник технологического объекта способен выявить такую атаку значительно быстрее. Модель технологического процесса вычисляет взаимосвязанные параметры системы на основе физических законов. Например, для теплогидравлического контура станции взаимосвязаны температура теплоносителя, давление, тепловая мощность и расход среды. Если один из параметров подменен, то остальные параметры перестают согласовываться с расчетной моделью. Даже небольшое расхождение между измеренными и расчетными значениями может свидетельствовать о некорректности данных.

Таким образом, цифровой двойник обнаруживает физическую несогласованность параметров, тогда как традиционные средства кибербезопасности видят только корректную сетевую активность.

Сценарий 2. Скрытое изменение уставок регулирования

Другой тип атаки связан не с подменой данных датчиков, а с изменением уставок систем автоматического регулирования. В этом случае злоумышленник постепенно изменяет параметры управления, например, уставку температуры, давление в контуре, скорость вращения турбины, нагрузку генератора. Такая атака может быть реализована через легитимные интерфейсы управления, поэтому она также не вызывает подозрений у традиционных систем кибербезопасности.

При постепенном изменении уставок система управления продолжает функционировать корректно, однако технологический режим может посте-

Таблица 1. Сравнение двух подходов к обнаружению атак

Критерий	Традиционная кибербезопасность	Цифровой двойник
Контроль сетевых протоколов	Да	Нет
Контроль физического состояния объекта	Нет	Да
Обнаружение подмены датчиков	Ограничено	Высокая вероятность
Выявление опасных режимов	Ограничено	Да
Прогноз развития инцидента	Нет	Да
Работа быстрее реального времени	Нет	Возможно

пенно приближаться к небезопасным условиям. Например:

- турбина начинает работать в нерасчетном режиме;
- возникает опасный тепловой градиент в оборудовании;
- возрастает вероятность вибрационных или кавитационных процессов.

Традиционные системы кибербезопасности в этом случае фиксируют лишь допустимые команды оператора или системы автоматического регулирования. Цифровой двойник, работающий в режиме быстрее реального времени, способен заранее оценить развитие такого режима. Используя текущие параметры системы, модель может выполнить ускоренное моделирование развития процесса и определить, приведет ли текущая тенденция изменения параметров к опасному состоянию.

Таким образом, цифровой двойник способен обнаружить потенциально опасный режим еще до того, как он проявится в реальной системе. Сравнение двух подходов к обнаружению атак представлено в табл. 1.

Значение подхода для энергетических систем

Использование высокоскоростных инженерных моделей энергоблоков

Следует отметить, что использование моделей, работающих быстрее реального времени, для анализа и проверки режимов энергетических установок не является новой идеей. В ряде проектов при создании энергетических блоков применялись комплексные системы моделирования, предназначенные для проверки технических решений и анализа режимов работы оборудования. В частности, программные комплексы РАДУГА и ТРР, разработанные компанией «НПЦ Приоритет», применялись при анализе режимов работы энергетических установок и при проверке инженерных решений на этапах проектирования и пусконаладочных работ.

Характерной особенностью этих систем является то, что их вычислительная производительность существенно превышает скорость протекания соответствующих физических процессов. В ряде случаев это приводило к необходимости искусственного замедления вычислений, чтобы синхронизировать расчеты модели с реальным временем технологического процесса.

Подобная особенность – следствие высокой эффективности используемых алгоритмов и структуры математических моделей. Однако именно эта характеристика открывает новые возможности применения таких систем в качестве инструментов прогнозного анализа и киберфизического мониторинга.

Комплексное моделирование энергетического объекта

Важная особенность платформ РАДУГА и ТРР – возможность моделировать не отдельные элементы оборудования, а комплексную систему энергетического объекта, включая:

- основные технологические контуры энергетического блока;
- системы автоматического регулирования;
- электрическую часть станции;
- взаимодействие с энергосистемой.

Такая интеграция различных подсистем в единой модели является редкой особенностью подобных программных комплексов. Во многих существующих системах моделирования рассматриваются отдельные аспекты функционирования энергетического объекта – например, теплогидравлические процессы, электрические режимы или системы управления. Комплексные модели, охватывающие одновременно все основные компоненты энергетического блока и его взаимодействие с энергосистемой, встречаются значительно реже.

Значение для киберфизической безопасности

Наличие интегрированной модели энергетического объекта создает принципиально новые возможности для анализа устойчивости системы управления. Если модель работает быстрее реального времени, она может использоваться для:

- ускоренного расчета развития технологического процесса;
- прогнозирования последствий управляющих воздействий;
- оценки устойчивости системы к потенциальным нарушениям режима.

В контексте кибербезопасности это означает возможность выявления ситуаций, когда система управления получает формально корректные команды, сетевой обмен выглядит нормальным, однако физическое поведение объекта начинает отклоняться от допустимого режима. Таким образом, модель может выполнять функции прогнозного наблюдателя технологического процесса, позволяя обнаруживать потенциально опасные режимы до их проявления в реальной системе.

Перспективы применения

Использование комплексных моделей энергетических установок, работающих быстрее реального времени, может стать важным элементом систем киберфизической защиты энергетической инфраструктуры. Особенно перспективным является применение таких моделей в качестве аналитического уровня системы мониторинга, дополняющего традиционные средства кибербезопасности. В этом случае цифровой двойник энергетического объекта выполняет функции:

- проверки физической согласованности технологических параметров;
- прогнозирования развития технологического режима;
- раннего обнаружения потенциальных киберфизических инцидентов.

Программные платформы класса РАДУГА-ЭУ могут служить основой для реализации подобного подхода на

энергетических объектах. Для энергетических объектов, включая ТЭС и АЭС, модельно-ориентированная киберфизическая защита особенно актуальна по следующим причинам:

- сложная взаимосвязь технологических параметров;
- высокая инерционность процессов;
- потенциально тяжелые последствия ошибок управления;
- высокая степень автоматизации систем управления.

В этих условиях цифровой двойник может выполнять роль дополнительного аналитического уровня защиты, обеспечивающего контроль физической состоятельности технологического процесса.

Использование платформ моделирования, таких как РАДУГА-ЭУ, позволяет реализовать данный подход на практике. Платформа обеспечивает моделирование сложных энергетических систем и может использоваться как основа для создания цифровых двойников электростанций. Таким образом, интеграция цифровых двойников в архитектуру киберфизической безопасности энергетических объектов может существенно повысить устойчивость критической энергетической инфраструктуры к современным угрозам.

Примеры использования

Моделирование было выполнено с использованием платформы РАДУГА-ЭУ с целью оценки ее применимости для моделирования энергетических систем в реальном времени и в режиме быстрее реального времени.

Были рассмотрены два характерных сценария: режим регулирования нагрузки в энергоблоках атомных электростанций и моделирование переходных процессов в тепловых энергоблоках. Для энергоблока АЭС был смоделирован режим маневрирования мощностью (100–20–100%). Результаты показали, что модель работает с ускорением приблизительно в 9 раз по сравнению с реальным временем, при этом сохраняются основные динамические характеристики системы.

Дополнительно были выполнены расчеты переходных процессов в тепловых энергоблоках. Результаты показали, что скорость моделирования превышает реальное время примерно в 4,36 раза. Это подтверждает способность платформы эффективно моделировать динамические процессы на тепловых электростанциях с существенным вычислительным ускорением.

Полученные результаты демонстрируют, что платформа РАДУГА-ЭУ обеспечивает возможность моделирования как атомных, так и тепловых энергетических систем в режиме быстрее реального времени. Важно отметить, что все расчеты выполнялись на стандартном планшетном компьютере, оснащенном процессором Intel Core i7, что подтверждает возможность реализации предложенного подхода без использования специализированных высокопроизводительных вычислительных ресурсов.

Указанные примеры проиллюстрированы схемами и графиками, которые можно посмотреть по ссылке https://isup.ru/articles/34/22747/ или перейдя по QR-коду:

Заключение

Основные результаты работы заключаются в следующем.

Предложен подход к киберфизической защите энергетических объектов на основе моделей, который расширяет традиционные механизмы кибербезопасности за счет включения анализа согласованности физических процессов в реальном времени.

Разработана многоуровневая архитектура для киберфизического мониторинга, интегрирующая традиционные инструменты кибербезопасности с цифровым двойником технологического процесса.

Продемонстрирована применимость платформы моделирования РАДУГА-ЭУ в качестве основного компонента системы киберфизического мониторинга, подчеркнута ее способность моделировать как физические процессы, так и поведение системы управления.

Экспериментально продемонстрирована возможность моделирования сложных энергетических систем в режиме, превышающем реальное время. В частности, достигнуты коэффициенты ускорения до 9× для моделей ядерных энергоблоков и приблизительно 4,36× для переходных процессов в тепловых энергоблоках.

Показано, что цифровые двойники, работающие быстрее реального времени, позволяют прогнозировать небезопасные условия эксплуатации и киберфизические аномалии до того, как они проявятся в физической системе.

Проанализированы типичные сценарии киберфизических атак, включая внедрение ложных данных и манипулирование заданными значениями параметров управления, и продемонстрировано, как модельные подходы могут обнаруживать такие атаки, даже если они остаются невидимыми для традиционных инструментов кибербезопасности.

В совокупности эти работы показывают, что интеграция высокоскоростных имитационных моделей в архитектуры кибербезопасности значительно повышает устойчивость энергетической инфраструктуры к сложным киберфизическим угрозам.

Оценка быстродействия модели проводилась на стандартном планшетном компьютере, оснащенном процессором Intel Core i7, что демонстрирует возможность реализации предложенного подхода без использования специализированных высокопроизводительных вычислительных систем.

Литература

1. *Кавун О. Ю.* Методика моделирования динамики энергоблока АЭС, реализованная в программном комплексе «РАДУГА-ЭУ» // ВАНТ. сер.: Физика ядерных реакторов. М.: 1999, вып. 2.
2. *Кавун О. Ю., Лифшиц А. М.* Использование отечественных программных комплексов для создания цифровых двойников электростанций на примере ПК «Радуга-ЭУ» // Автоматизация и IT в энергетике. 2023. № 11.

А. М. Лифшиц, председатель совета директоров,
В. Г. Айрапетян. к. ф-м. н., директор по научной работе,
ООО «НПЦ Приоритет», г. Москва,
тел.: +7 (495) 995-2733,
эл. почта: prioritet@priortelecom.ru,
сайт: www.priortelecom.ru

Иллюстрации предоставлены ООО «НПЦ Приоритет»