DOI: 10.25728/avtprom.2020.11.08

Практические подходы к созданию инфраструктуры индустриального киберполигона

О.Д. Архангельский, Д.В. Сютов, А.В. Кузнецов («Ростелеком-Солар»)

Обеспечение кибербезопасности АСУ и промышленной автоматики является одним из важнейших направлений в эпоху стремительного технологического развития киберфизических систем. Одним из направлений исследований в области обеспечения кибербезопасности промышленных объектов (в том числе, объектов критической информационной инфраструктуры), является проведение регулярных теоретических и практических тренировок для предупреждения, обнаружения и противодействия возможным компьютерным атакам – киберучений. Для проведения киберучений необходимо создание соответствующей инфраструктуры и методологии, позволяющих отрабатывать практические навыки обеспечения кибербезопасности без риска нанесения реального ущерба деятельности предприятия или останова технологического процесса. В статье рассматриваются основные подходы к созданию инфраструктуры для проведения киберучений, а также аспекты моделирования технологических процессов промышленных объектов в рамках формирования такой инфраструктуры.

Ключевые слова: кибербезопасность, автоматизированные системы управления, киберучения, киберполигон, информационная безопасность, киберфизические системы, полунатурное моделирование.

Введение

В настоящее время одним из основных дестабилизирующих факторов устойчивого функционирования объектов критической информационной инфраструктуры (КИИ) являются кибератаки. Кибератаки на информационные системы промышленных объектов способны приводить к нарушению технологического процесса, возникновению нештатных или аварийных ситуаций и даже к физическому разрушению промышленного оборудования [1, 2].

Риски нарушения технологического процесса в результате кибератак возрастают с увеличением уровня цифровизации объекта, появлением дополнительных сервисов, а также при использовании ПО и оборудования иностранных производителей. Современные реалии требуют от специалистов по информационной безопасности учитывать упомянутые риски и формировать новые подходы к обеспечению информационной безопасности. Актуальными вопросами в настоящее время являются координация действий специалистов по информационной безопасности (ИБ) и налаживание межведомственного взаимодействия в рамках реагирования на кибератаки, а также создание методической и технической базы для регулярной отработки специалистами ИБ практических навыков противодействия кибератакам. Основным подходом, позволяющим решить поставленные задачи, может стать проведение специализированных тренировок – киберучений.

Киберучения – новый вид отраслевых тренировок

Киберучения могут быть организованы и проведены как отдельно, так и в комплексе с существующими формами производственной деятельности, обеспечивающей поддержание необходимого профессионального уровня персонала для выполнения им производственных задач [3].

Подобный подход широко распространен в странах Европейского союза и США, где киберучения для различных отраслей промышленности проводятся на регулярной основе по аналогии с тренировками оперативного-диспетчерского персонала объектов энергетики, противопожарными тренировками и т.д. В настоящее время в России также начал формироваться запрос на проведение киберучений и создание соответствующей инфраструктуры[1]. Вопросы отработки основных аспектов обеспечения кибербезопасности объектов КИИ рассматриваются на уровне профильных министерств (Минкомсвязи и Минэнерго России), крупнейших предприятий отраслей КИИ (АО «СО ЕЭС», ПАО «Россети», ПАО «РусГидро» и др.), а также регуляторов в области обеспечения ИБ (ФСТЭК и ФСБ).

Актуальность данной тематики в нашей стране связана с несколькими основными аспектами.

Усложнение и взаимная интеграция информационных и автоматизированных систем, переход к киберфизическим системам, предполагающим интеграцию вычислительных ресурсов и физического оборудова-

[1] Постановление Правительства РФ от 12 октября 2019 г. № 1320 "Об утверждении Правил предоставления субсидий из федерального бюджета на создание киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности".

ния, не позволяют проанализировать все возможные последствия кибератак аналитическими методами ввиду очень высокой сложности и многосвязности таких систем, а также наличия недекларированных возможностей и уязвимостей ПО. Для определения векторов и возможных последствий кибератак необходимо проводить практические исследования и испытания на специализированной инфраструктуре.

Не менее важными являются кадровые проблемы и нехватка специалистов в области обеспечения информационной безопасности информационных и автоматизированных систем. Недостаточный уровень практических знаний и навыков в части ИБ, отсутствие практики отработки действий оперативного персонала и специалистов ИБ промышленных объектов при кибератаках не позволяют оперативно реагировать на инциденты информационной безопасности на объектах КИИ. Следствием становится недостаточная осведомленность сотрудников служб ИБ и персонала промышленных объектов о возможностях злоумышленников по взлому АСУТП и IIoT-систем.

Указанные проблемы могут быть решены благодаря проведению регулярных киберучений и тренировок. Однако проведение киберучений на собственной инфраструктуре промышленного предприятия сопряжено со значительными рисками нарушения технологического процесса и является дорогостоящим и сложным в реализации (как с технической, так и с организационной стороны) мероприятием. В качестве альтернативы такому решению киберучения могут быть проведены на специализированной инфраструктуре – киберполигоне. Инфраструктура киберполигона позволяет проводить киберучения и отрабатывать практические навыки обеспечения кибербезопасности без риска нанесения реального ущерба деятельности предприятия или останова технологического процесса.

Национальный киберполигон

Инфраструктура для проведения киберучений в настоящее время реализуется компанией «Ростелеком-Солар» (дочерней компанией «Ростелеком») в рамках проекта «Национальный киберполигон» — одного из проектов по информационной безопасности из Национальной программы «Цифровая экономика России» в 2020 г. [4]. «Национальный киберполигон» является сложным комплексным проектом, включающим три составляющие, которые необходимы для успешного функционирования:

– технологическая инфраструктура киберполигона, то есть то оборудование и ПО, на базе которого функционирует киберполигон;

– комплекс методических и методологических материалов, описывающих реализацию основной функциональности киберполигона (например, комплекс методик для проведения киберучений, регламенты поиска уязвимостей и НДВ в оборудовании и ПО);

– команда экспертов и технических специалистов, обеспечивающих функционирование киберполигона.

Рассмотрим подробнее вопросы формирования технологической инфраструктуры киберполигона. Отметим, что в рамках проекта «Национальный киберполигон» технологическая инфраструктура разделена на два блока: информационные технологии и индустриальная (промышленная) часть. Далее речь пойдет об индустриальной части киберполигона.

Для определения концептуального облика инфраструктуры индустриальной части киберполигона основополагающим является вопрос выбора подхода к моделированию киберфизической системы промышленного предприятия. В большинстве отечественных и зарубежных научных исследований принята стандартная классификация типов моделирования, включающая натурное, программное и полунатурное моделирование [4]:

- натурное моделирование: натурный стенд, реальный тестовый объект *(Full-scale system)*;
- математическое моделирование;
- полунатурное моделирование: с вторичным оборудованием в контуре *(Controller HIL)* и с включением силового оборудования в контур *(Power HIL)*.

Для проведения сравнения указанных типов моделирования воспользуемся следующими основными характеристиками [5]:

1) полнота модели, то есть возможность вычисления всех характеристик системы с требуемой точностью и достоверностью;

2) гибкость модели, которая позволяет воспроизводить различные ситуации и процессы, изменять структуру, алгоритмы и параметры изучаемой системы;

3) длительность разработки и реализации, характеризующая временные затраты на создание модели;

4) блочность структуры, допускающая добавление, исключение и замену некоторых частей (блоков) модели.

Было проведено детальное сравнение указанных методов моделирования (рис. 1).

Как видно из представленной схемы, каждый из перечисленных типов моделирования в рамках рассматриваемых характеристик обладает своими преимуществами и недостатками. В тоже время наиболее сбалансированным подходом можно считать метод полунатурного моделирования сложной киберфизической системы. Данный метод обладает преимуществами как математического, так и натурного моделирования.

Полунатурное моделирование предполагает разбиение сложной системы на две части: одна часть моделируется численным способом, а другая представляется реальным физическим оборудованием. Особенностью таких моделей является наличие обратной связи между физическим оборудованием и математической моделью: изменение состояния устройств автоматики вызывает срабатывание управляемого элемента (например, силового выключателя подстанции) в математической модели и, наоборот: изменение параметров в математической модели

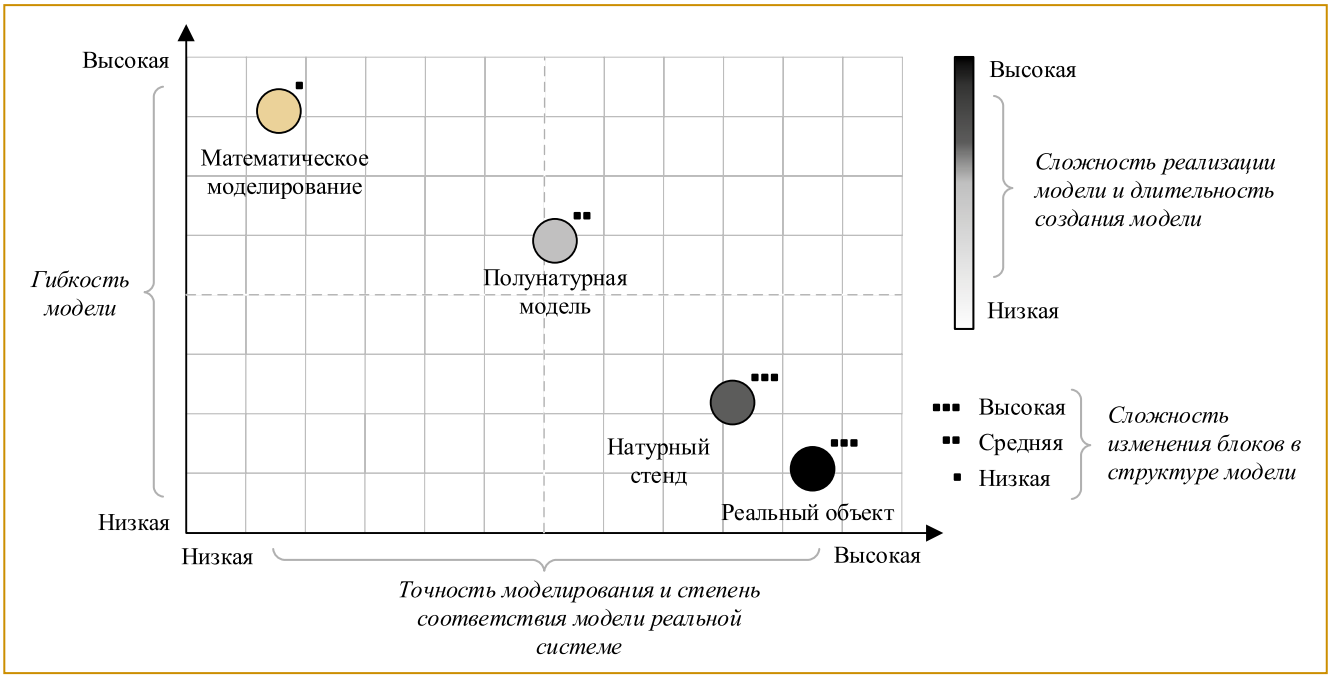

Рис. 1. Сравнение различных типов моделирования киберфизических систем

(например, вследствие моделируемого короткого замыкания на шинах подстанции) приводит к срабатыванию соответствующей защиты и автоматики, реализованных в физических терминалах и контроллерах. При этом обратная связь может осуществляться как в замкнутом, так и в разомкнутом контуре моделирования. В связи с этим в настоящее время существует два основных подхода к созданию лабораторных стендов в рамках концепции полунатурного моделирования:

1) применение набора специализированных испытательных установок и специализированного ПО для проведения экспериментов и обработки результатов (разомкнутый контур моделирования);

2) применение программно-аппаратных комплексов моделирования в реальном времени с подключением реального (физического) оборудования (замкнутый контур моделирования).

В случае использования первого подхода математические модели строятся, как правило, без привязки к реальному времени. Одним из основных преимуществ таких систем моделирования является фактическое отсутствие ограничений на размеры моделируемой энергосистемы: время расчета определяется только производительностью аппаратных средств, на которых установлено ПО моделирования. Однако для применения данного типа моделирования существуют определенные ограничения. Слабая связность входящих в контур моделирования элементов и отсутствие автоматизации взаимодействия между физическими элементами и математической моделью (вследствие разомкнутого контура моделирования) не подходит для создания моделей сложных киберфизических систем, где требуется постоянная обратная связь между оборудованием и математической моделью. Кроме того, процесс интерпретации полученных при моделировании результатов также усложняется из-за необходимости сопоставления результатов работы различного ПО и утилит, а также сопоставления полученных данных по меткам времени для воссоздания единой картины аварийного события или процесса.

Указанных проблем можно избежать при использовании единых аппаратно-программных комплексов моделирования в реальном времени вместо набора отдельных испытательных установок и утилит. Это решение является более дорогим, однако для масштабных исследований, затрагивающих одновременно несколько технологических подсистем объекта (или нескольких промышленных объектов) такое решение наиболее эффективно. Использование программно-аппаратных комплексов моделирования позволяет создавать масштабные модели с непрерывной обратной связью между физической и математической частями модели, а также проводить испытания с учетом динамических изменений в системе. Основным отличием программно-аппаратных комплексов является проведение расчетов в реальном времени (то есть время вычисления соответствует временному шагу в моделируемом процессе), а также возможность объединения в «замкнутый контур» физического оборудования и математической модели.

Практическая реализация

Для наиболее корректного отображения всех взаимосвязей сложной киберфизической системы архитектура разрабатываемого индустриального полигона должна максимально точно повторять архитектуру исходной системы. В рамках реализации первой очереди киберполигона в качестве исходной была выбра-

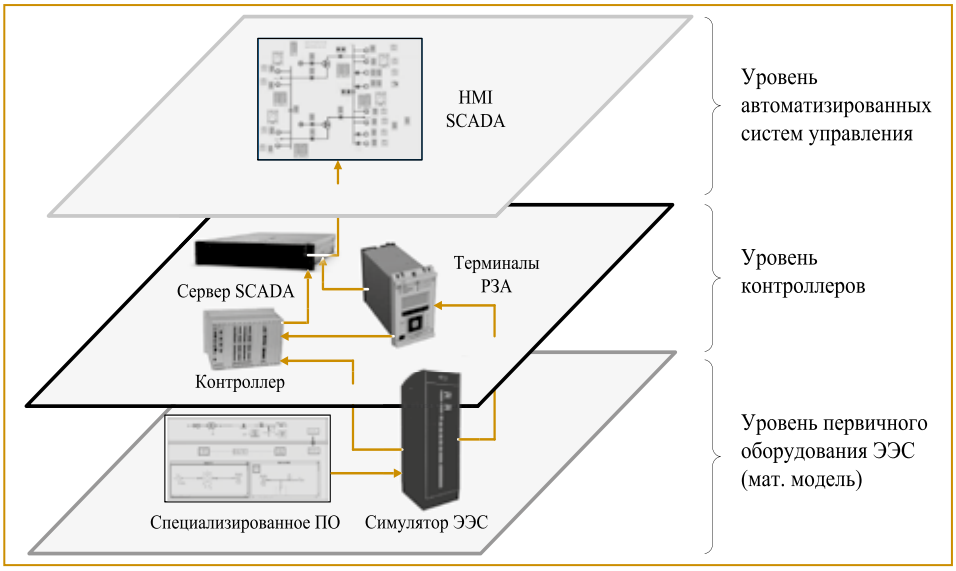

Рис. 2. Архитектура индустриального полигона

на электроэнергетическая система (на данном этапе рассматриваются объекты передачи и распределения электроэнергии — магистральные и распределительные сети и электрические подстанции).

Инфраструктуру индустриального киберполигона целесообразно представить в виде нескольких взаимодействующих между собой уровней (рис. 2):

– первичного оборудования (математическая модель);

– контроллеров (физические и виртуальные интеллектуальные устройства);

– АСУ (программные комплексы АСУТП и оперативно-информационные комплексы или SCADA и EMS/DMS).

Оборудование, которое не может быть смоделировано натурно по экономическим или техническим причинам, заменяется специализированным ПО для моделирования. При этом предусматриваются специализированные программные интерфейсы (коннекторы), позволяющие данному ПО взаимодействовать с реальным физическим оборудованием и математической моделью.

Рассмотрим более детально практическую реализацию различных уровней архитектуры индустриального киберполигона.

Уровень первичного оборудования

Первичное оборудование уровня технологического процесса воспроизводится в математической модели с цифровыми и аналоговыми интерфейсами. В настоящее время для создания моделей, работающих в реальном времени, применяются два программно-аппаратных комплекса: OPAL-RT и RTDS (Real Time Digital Simulator). Создание и изменение параметров цифровой модели, управление процессом моделирования осуществляются с использованием специализированного ПО. При использовании комплекса OPAL-RT применяется ПО MatLab/Simulink, для работы с симулятором RTDS используется программный комплекс RSCAD. Данные программно-аппаратные симуляторы способны производить расчеты с шагом до нескольких микросекунд, что является достаточным для корректного описания электромагнитных и электромеханических переходных процессов, необходимых к рассмотрению при моделировании электроэнергетической системы и происходящих в ней процессов.

При создании киберполигона для проведения моделирования сложной электроэнергетической системы был выбран программно-аппаратный комплекс RTDS: используемый крупнейшими производителями оборудования (в том числе Siemens, ABB, Alstom, General Electric, Toshiba, SEL, Schneider Electric) более чем в 30 странах, а также применяются ведущими научными лабораториями и институтами (SCADA National Lab, Technical University of Denmark, DTU, University of South Wales, Durban University of Technology, Florida State University). Благодаря высокой надежности, релевантности получаемых в ходе расчета данных и удобства разработки математических моделей электроэнергетических систем цифро-

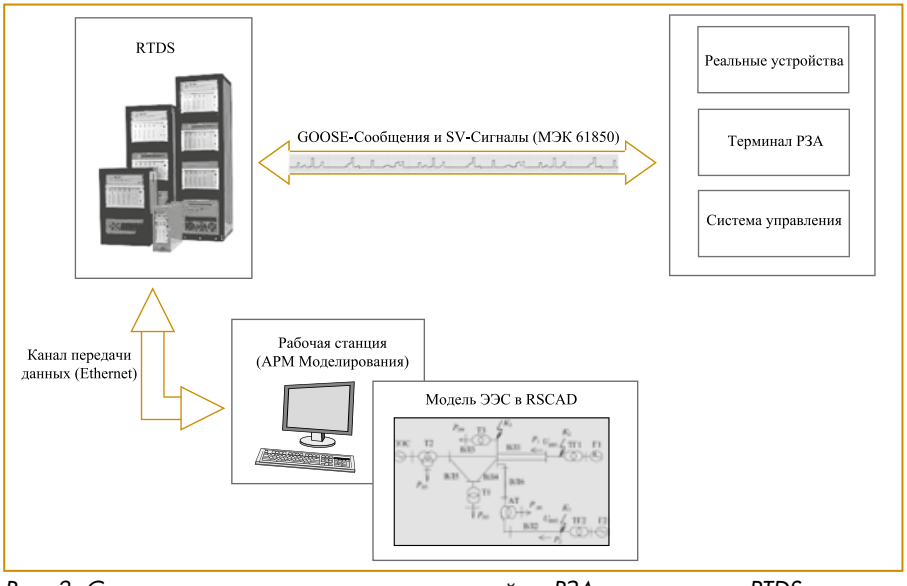

Рис. 3. Структурная схема подключения устройств РЗА к симулятору RTDS

вые симуляторы RTDS де-факто являются стандартом в электроэнергетической отрасли.

Уровень контроллеров

Поскольку в настоящее время в электрических сетях России происходит постепенный переход к целевой схеме цифровой подстанции (ЦПС), в рамках моделирования объектов электроэнергетики рассматривались два типа энергообъектов: современные ЦПС и модернизируемые объекты, характеризующиеся частичным внедрением технологий цифровой подстанции.

Для моделирования ЦПС в рамках полунатурной модели электро-энергетической системы была сформирована шина процесса на базе специализированных управляемых коммутаторов. Терминалы РЗА и контроллеры присоединения на моделируемых подстанциях получают информацию об измеренных параметрах электрического режима (токах и напряжениях), а также о положении коммутационной аппаратуры. Информация передается по шине процесса от симулятора RTDS по протоколам SV и GOOSE (рис. 2). Для формирования шины процесса используются специализированные коммутаторы с поддержкой протокола PTP (IEEE1588v.2) производителей: Phoenix Contact, MOXA, Kyland и Hirschman.

Для моделирования объектов с частичным внедрением технологий цифровой подстанции требуется обеспечить формирование цифрового потока данных об измерениях тока и напряжения с линейных трансформаторов тока и напряжения (SV-поток) и данных о положении коммутационных аппаратов (GOOSE-сообщения). Для этого применяется устройство сопряжения с объектом (УСО, Merging Unit, MU). Аналоговые сигналы токов и напряжения, подаваемые на вход УСО, формируются из низкоуровневых сигналов с платы цифро-аналогового преобразователя (ЦАП) RTDS с последующим усилением сигнала при помощи специализированных усилительной системы. Таким образом, входные сигналы усиливаются до уровня, требуемого для нормальной работы терминалов РЗА (рис. 4).

С целью обеспечения корректной работы основных подсистем управления и релейной защиты, на моделируемых подстанциях необходимо сформировать систему точного времени. Для этого предусматривается установка серверов точного времени.

Для мониторинга параметров режима и переходных процессов в узлах моделируемой электросети предлагается установка устройств синхронизированных векторных измерений (УСВИ, PMU). Измеренная информация от этих устройств в соответствии с IEEE C37.118v2 по сети передается в диспетчерский центр, где принимается программным устройством PDC (Phasor Data Concentrator) и передается в систему мониторинга для использования в алгоритмах оценки устойчивости сети, создания архива и в качестве дополнительной информации для верификации измерений, полученных по протоколу IEC60870-5-104 с моделируемых подстанций.

Отметим, что в целях обеспечения большей гибкости и масштабируемости инфраструктуры некоторые устройства РЗА, АСУТП и телемеханики выполнены в виде виртуальных интеллектуальных электронных устройств — специализированных программ, запускаемых в среде виртуализации. Виртуальные устройства выполняют те же функции, что и их физические аналоги и обладают всеми необходимыми цифровыми интерфейсами для взаимодействия с физическими контроллерами и математической моделью. Такой подход позволяет формировать модели крупных энергообъектов с большим количеством устройств автоматизации.

Уровень АСУ

Автоматизированные системы управления являются одними из наиболее критичных элементов, поскольку нарушение функционирования оперативных информационных комплексов или АСУТП может вызвать несанкционированное отключение первич-

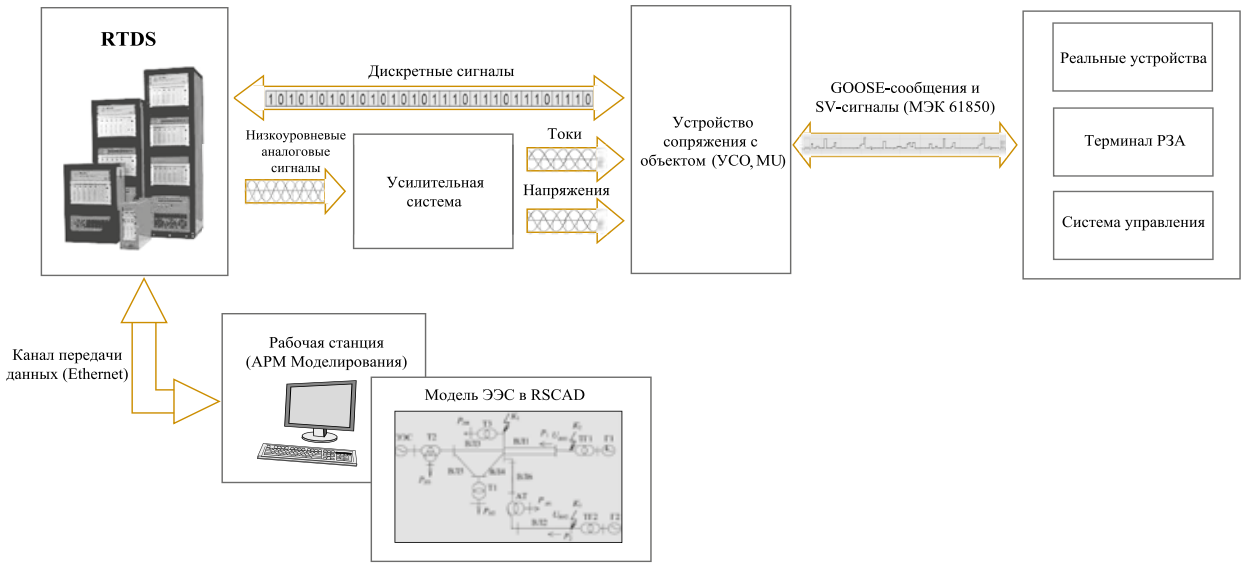

Рис. 4. Структурная схема подключения устройств РЗА к симулятору RTDS через УСО

ного оборудования энергообъекта. Это, в свою очередь, может послужить триггером развития аварийной ситуации и привести к прекращению подачи электроэнергии потребителям, а в некоторых случаях к повреждению первичного оборудования. Соответственно, для анализа возможных сценариев атак на данные системы, их также необходимо смоделировать в рамках киберфизической модели.

Для моделирования диспетчерского центра верхнего уровня применяется система «ОИК Диспетчер НТ», обладающая функциональностью телеуправления. Для моделирования автоматизированных систем уровня подстанции в рамках индустриального киберполигона используются программные и программно-аппаратные комплексы Siemens, General Electric, АО «ЧЭАЗ», ООО «ИнСАТ». Развернутые в рамках киберполигона АСУТП и ОИК обладают полной функциональностью в части управления первичным оборудованием объекта, то есть управление может осуществляться как из системы ОИК (с уровня диспетчерского центра), так и из SCADA-системы подстанции. Наличие уровня АСУ позволяет не только расширить моделируемые сценарии, но и рассмотреть последствия возможных отказов терминалов РЗА, систем связи, средств отображения и т.д., а также оценить результаты возможных кибератак, связанных с подменой информации в SCADA.

Заключение

Предложенные подходы были апробированы в ходе киберучений по анализу нарушений работоспособности объектов электроэнергетического комплекса в результате кибератак на системы управления и защиты цифровых подстанций, проведенных под эгидой Минкомсвязи России при поддержке Министерства энергетики РФ [6].

В результате проделанной работы в рамках описанного проекта «Национальный киберполигон» удалось создать гибкую инфраструктуру для проведения киберучений и исследований в области ИБ промышленных объектов. Инфраструктура позволяет детально смоделировать технологические процессы и, в силу своей гибкости, может быть изменена в соответствии с запросом конкретного предприятия. Все это позволяет добиться высокой точности воспроизведения технологических процессов заказчика и в рамках исследований сформировать актуальный перечень угроз, а также оценить возможные последствия реализации угроз ИБ.

Список литературы

1. *Simon Parker.* Understanding the Physical Damage Of Cyber Attacks, URL: https://www.infosecurity-magazine.com/opinions/physical-damage-cyber-attacks
2. *Kaixing Huang, Chunjie Zhou, Yu-Chu Tian, Shuang-Hua H Yang, Yuanqing Qin.* Assessing the Physical Impact of Cyber-Attacks on Industrial Cyber-Physical Systems // IEEE Transactions on Industrial Electronics PP(99):1-1, 2018.
3. *Карантаев В.Г., Кузнецов А.В., Архангельский О.Д., Сютов Д.В.* Опыт проведения киберучений по анализу нарушений работоспособности объектов электроэнергетического комплекса в результате кибератак // Релейщик. 2020. №1 (36).
4. *Khaitan Siddhartha Kumar, McCalley James D., Liu Chen Ching (Eds.).* Cyber Physical Systems Approach to Smart Electric Power Grid. Springer. 2015.
5. *Советов Б.Я., Яковлев С.А.* Моделирование систем. М.: Высш. Шк., 2001. – 343 с.
6. *Карантаев В.Г., Кузнецов А.В., Архангельский О.Д., Сютов Д.В.* Опыт проведения киберучений по анализу нарушений работоспособности объектов электроэнергетического комплекса в результате кибератак // Релейщик. 2020. №1 (36).

Архангельский Олег Денисович *– ведущий аналитик-методолог проекта «Индустриальный киберполигон»,*
Сютов Дмитрий Владимирович *– главный инженер проекта «Индустриальный киберполигон»,*
Кузнецов Андрей Владимирович *– руководитель проекта «Индустриальный киберполигон», заместитель руководителя Лаборатории Кибербезопасности АСУТП по производству компании «Ростелеком-Солар».*
E-mail: o.arkhangelskii@rt-solar.ru; d.syutov@rt-solar.ru; a.kuznetsov@rt-solar.ru

Новые IoT-датчики Cisco упрощают получение данных и повышают безопасность и эффективность

Cisco представила два новых сенсорных решения с облачным управлением для упрощения масштабного мониторинга производственных объектов и оборудования от расположенных внутри здания ИТ-шкафов до внешних объектов и пространств, относящихся к операционным технологиям (Operation Technology, OT).

• Датчики Meraki MT для мониторинга помещений и ИТ-инфраструктуры. Три модели устройств с облачным управлением — MT10, MT12 и MT20 — передают в реальном времени данные о температуре, влажности, протечках и проникновении в помещение.

• Датчики Industrial Asset Vision для мониторинга OT-объектов и оборудования внутри и вне производственных помещений. Новая облачная панель управления позволяет немедленно реагировать в соответствии с поступающей информацией. Датчики, соответствующие степеням защиты IP65 и IP67, интегрированы с шлюзом Cisco LoRaWAN IoT Gateway и предоставляют данные о температуре, влажности, уровнях вибрации и освещенности по помещениям и оборудованию.

Эти решения уже функционируют в энергетике, нефтегазовой отрасли, образовании и здравоохранении, обрабатывающей промышленности и розничной торговле, повышая эффективность операционной деятельности и предотвращая аварии и дорогостоящие простои.

http://www.cisco.com