DOI: 10.25728/avtprom.2021.11.06

Опыт проведения киберучений на национальном киберполигоне

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

Рассмотрена программно-аппаратная структура Национального киберполигона, созданного ПАО «Ростелеком» при содействии Министерства цифрового развития, связи и массовых коммуникаций РФ. Показано исследование объектов электроэнергетики и опыт проведения киберучений на Национальном киберполигоне. Описаны проводимые и планируемые работы по расширению, модернизации существующей функциональности полигона.

Ключевые слова: киберполигон, цифровой двойник, объекты электроэнергетики, киберучения, критическая информационная инфраструктура.

Интеллектуализация и цифровизация электроэнергетической отрасли в соответствии с ведомственным проектом Минэнерго «Цифровая энергетика» на сегодняшний день является одной из приоритетных задач в отрасли (minenergo.gov.ru/node/14559). Степень готовности электроэнергетического комплекса к цифровизации можно оценить по числу объектов, на которых уже используются цифровые решения. Так, например, согласно отчету ПАО ФСК ЕЭС, в настоящее время реализовано 198 подстанций с поддержкой международного стандарта МЭК 61850 (из них 16 подстанций – в 2020 г., на дистанционное управление переведено 12 подстанций), что составляет 28 % от общего числа всех подстанций ПАО ФСК ЕЭС [1]. Все большее число подстанций переводится на телеуправление; так, до конца 2021 г. ПАО «ФСК ЕЭС» реализует дистанционное управление еще на 93 подстанциях по всей стране. К 2025 г. все подстанции ПАО «ФСК ЕЭС» будут обеспечены цифровой связью с возможностью удаленного управления из единых центров и будут реализованы 33 проекта «Цифровых подстанций» с более глубокой степенью цифровизации [1].

Проводимая в настоящее время цифровизация электроэнергетического комплекса, с одной стороны, позволит значительно повысить управляемость и наблюдаемость сети, снизить капитальные затраты на строительство новых и операционные затраты на обслуживание действующих объектов (CAPEX и OPEX), а также уменьшить время ликвидации технологических нарушений. [2]. С другой стороны, внедрение новых интеллектуальных технологий, сложного технического, информационного и коммуникационного оборудования на объектах электроэнергетики ведет к значительному росту рисков нарушения устойчивого функционирования объектов электроэнергетики из-за некорректной работы цифровых систем управления вследствие внешних информационных воздействий – компьютерных атак. Скоординированные компьютерные атаки на инфраструктурные объекты могут привести к нарушению или полному прекращению технологических и бизнес-процессов, возникновению аварийных ситуаций и физическому разрушению оборудования объектов критической информационной инфраструктуры (КИИ) Следствием таких атак могут являться нарушения в работе первичного (физического) оборудования, что может привести к массовым отключениям потребителей, а при атаке на несколько крупных

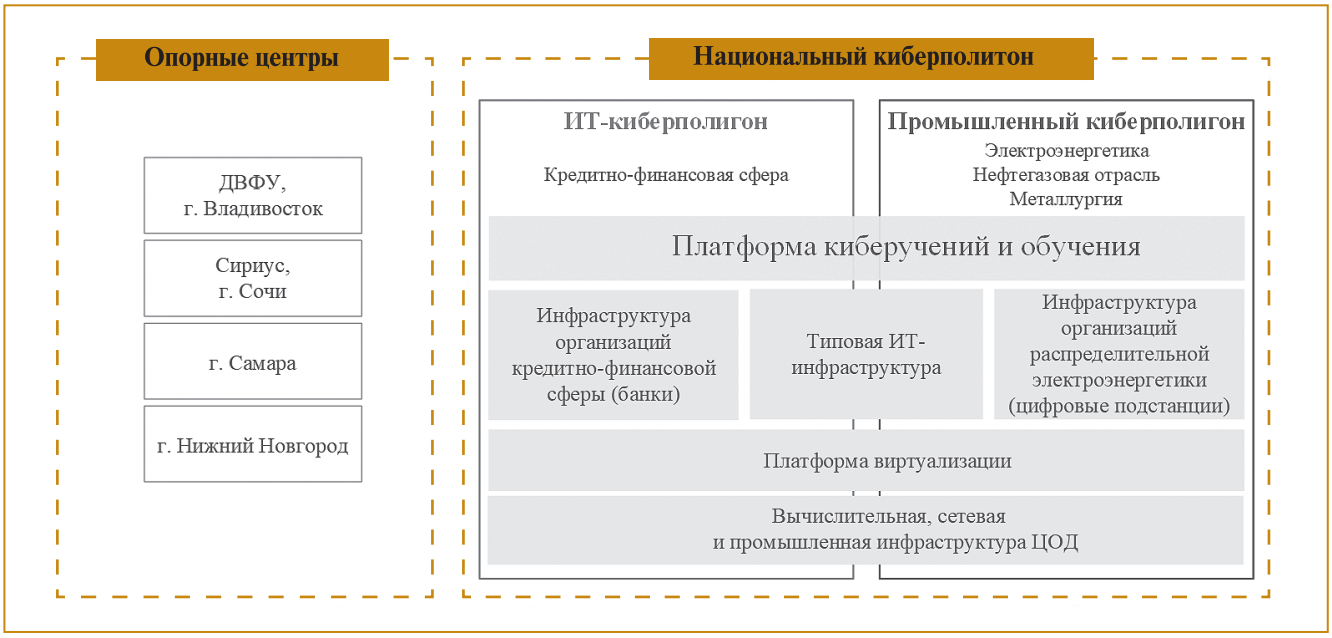

Рис. 1. Общая структура Национального киберполигона

подстанций – к выводу из строя целых областных энергосистем [3]. Кроме того, на государственном уровне кибератаки могут привести к значительным экономическим убыткам, снижению обороноспособности страны, дестабилизации социальной обстановки, а также возникновению угроз окружающей среде, жизни и здоровью граждан [4]. В связи с перечисленными выше аспектами именно компьютерные атаки необходимо рассматривать как один из важнейших современных видов угроз безопасности государства [5].

В данных условиях особое значение приобретают вопросы обеспечения безопасности объектов КИИ. Современные реалии требуют от специалистов по информационной безопасности учитывать упомянутые риски и формировать новые подходы к обеспечению информационной безопасности значимых объектов. Актуальными вопросами в настоящее время являются координация действий специалистов по информационной безопасности как внутри отдельных компаний отрасли, так и между несколькими субъектами отрасли, налаживание межведомственного взаимодействия в рамках реагирования на целенаправленные компьютерные атаки, а также создание методической и технической базы для регулярной отработки специалистами ИБ практических навыков противодействия таким атакам.

Киберучения

Основным подходом, позволяющим специалистам получить практический опыт противодействия компьютерным атакам и решить поставленные задачи, является проведение специализированных тренировок – киберучений. Киберучения проводятся с целью повышения уровня подготовки участников и направлены на решение следующих задач:

– отработка навыков по мониторингу и реагированию на компьютерные атаки, подходов к раннему обнаружению и формированию превентивных мер выявления компьютерных атак, действий по ликвидации последствий компьютерных атак и восстановлению штатного режима функционирования объекта КИИ;

– отработка процессов управления и координации работ по противодействию компьютерным атакам, а также отработка процессов взаимодействия участников киберучений и анализ полноты и достаточности существующей модели взаимодействия;

– определение текущего уровня навыков и степени готовности участников киберучений к отражению компьютерных атак;

– оценка последствий компьютерных атак, а также анализ эффективности и достаточности имеющихся планов минимизации последствий компьютерных атак и резервных схем функционирования объектов КИИ при нарушении их функционирования.

На основании проведенного анализа документов международных организаций NIST, MITRE и ENISA, посвященных киберучениям, была проведена классификация различных форм проведения учений и выделены три основных типа киберучений: штабные, практические и гибридные. [6]

Штабные киберучения (также носят название командно-штабной тренировки) предполагают теоретический разбор участниками различных сценариев и направлены на отработку взаимодействия, выявления существующих проблем и апробацию различных организационных решений по обеспечению безопасности и реагированию на компьютерные атаки. Данный тип учений применяется, как правило, на начальном этапе, когда требуется отработать основные организационные подходы к обеспечению информационной безопасности организации. Целевой аудиторией данного типа киберучений являются руководители подразделений организации-участника (технические руководители, руководители ИБ-отделов) и топ-менеджмент организации.

В ходе практических киберучений отрабатываются практические сценарии на реальной или тестовой инфраструктуре, моделирующей предприятие организации-участника учений либо типовой промышленный объект. В отличие от штабных киберучений, где отрабатываются организационные аспекты противодействия компьютерным атакам, в ходе данного типа киберучений отрабатываются в первую очередь практические навыки по обнаружению, противодействию, реагированию и расследованию компьютерных атак. Такой формат определяет и соответствующую целевую аудиторию киберучений практического типа: это технические специалисты, аналитики и администраторы средств защиты информации из различных подразделений организации-участника киберучений (либо нескольких смежных организаций отрасли).

При высоком уровне зрелости процессов, политик и процедур обеспечения информационной безопасности в организации, возможно проведение масштабных комплексных учений, предполагающих сочетание двух упомянутых выше типов киберучений. Гибридные киберучения (также носят название командно-штабные учения) предполагают выполнение командами участников теоретических и практических заданий, что позволяет одновременно в рамках единого сценария отработать как организационные, так и практические аспекты противодействия компьютерным атакам. Принять участие в таких киберучениях могут одновременно как административный персонал объекта КИИ (руководители отделов и департаментов), так и технический персонал: инженеры служб релейной защиты и автоматики (РЗА), АСУТП, администраторы ИБ и т.д.

Для проведения киберучений различных типов необходимо создание специализированной инфраструктуры – киберполигона. Киберполигон включает в себя техническую инфраструктуру, методологические подходы к проведению киберучений и построению математических моделей и процессов, на которых производится отработка сценариев, а также

команду экспертов, обладающих компетенциями в исследуемых отраслях.

Для проведения киберучений и отработки практических навыков реагирования на компьютерные атаки, ПАО «Ростелеком» при содействии Министерства цифрового развития, связи и массовых коммуникаций РФ в настоящее время реализует проект по созданию Национального киберполигона. Инфраструктура Нацио-нального киберполигона позволяет с высокой точностью моделировать актуальные угрозы и потенциально опасные ситуации, исследовать последствия атак на КИИ, а также отрабатывать меры по реагированию на выявленные угрозы и способы противодействия компьютерным атакам на инфраструктуру РФ. В настоящей статье будет детально рассмотрена техническая инфраструктура Национального киберполигона, показано применение данной инфраструктуры при проведении киберучений, а также описаны проводимые и планируемые работы по расширению, модернизации существующей функциональности полигона.

Существующая инфраструктура Национального киберполигона

Инфраструктура национального киберполигона представляет собой программно-аппаратный комплекс, позволяющий с заданной точностью моделировать типовые инфраструктуры объектов КИИ и являющийся площадкой для проведения исследований, тренировок и киберучений, а также практического обучения сотрудников. Общая структура киберполигона приведена на рис. 1.

Для реализации типовой инфраструктуры объектов КИИ в рамках киберполигона используется концепция цифровых двойников, то есть применение виртуальной интерактивной копии реального физического объекта или процесса. Для каждой из отраслей КИИ, исследуемых на Национальном киберполигоне (на данный момент — это электроэнергетика, металлургия, нефтегазовая и кредитно-финансовая отрасли) при участии отраслевых экспертов и центров компетенций (высшие учебные заведения, исследовательские лаборатории и т.д.) создается отдельная математическая модель, отражающая основные технологические процессы. Применение данного решения позволяет детально рассматривать влияние кибератак на технологический процесс за счет создания копии не только самого объекта, но и самих технологических и бизнес-процессов на данном объекте.

В рамках предлагаемого подхода детально моделируются только те процессы, на которые может быть оказано внешнее информационное воздействие. Так, для моделирования инфраструктуры типового энергообъекта в рамках киберполигона специалистами ПАО «Ростелеком» были проведены внутренние исследования по анализу первичных и вторичных систем объектов электроэнергетики с целью выявления тех из них, которые потенциально могут быть подвергнуты компьютерным атакам. На основании полученных данных были определены возможные функциональные нарушения в работе оборудования, входящего в состав первичных и вторичных систем цифровых подстанций, в результате компьютерных атак, а также был проведен анализ возможных последствий в рассматриваемой электрической сети. В рамках проведенного исследования были детально рассмотрены следующие технологические процессы:

– технологический процесс распределения электрической энергии, воздействие на который может быть произведено путем несанкционированного включения или отключения коммутационных аппаратов подстанции. Возможными последствиями компьютерной атаки, направленной на несанкционированное управление коммутационными аппаратами, могут стать частичная потеря передаваемой мощности либо полное прекращение подачи электроэнергии одному или нескольким потребителям;

– технологический процесс оперативной блокировки коммутационных аппаратов подстанции. В случае вывода из строя оперативной блокировки коммутационных аппаратов возможно возникновение короткого замыкания при включении заземляющего ножа (ЗН) распределительного устройства (РУ) 500 кВ на элемент под рабочим напряжением;

– процессы, возникающие при протекании коротких замыканий. Данные процессы рассматривались в рамках проведения оценки возможных повреждений силового оборудования подстанции в случае отказа или несрабатывания устройств РЗА вследствие компьютерной атаки;

– процессы, протекающие в высоковольтных линиях электропередачи (ЛЭП). Данные процессы рассматриваются в рамках оценки последствий возможного информационного воздействия на автоматику регулирования шунтирующего реактора. Излишнее или недостаточное регулирование может приводить к нежелательным перетокам реактивной мощности, следствием чего будет являться отклонение напряжения от номинального значения;

– процессы в силовых трансформаторах. В данном случае точкой воздействия может быть внешняя автоматика управления устройством регулирования под нагрузкой (РПН) трансформатора. Например, в случае управления устройством РПН при высоких токах нагрузки с отключенной блокировкой, возможно возникновение процессов ускоренного старения изоляции трансформатора и выхода оборудования из строя.

Техническая реализация инфраструктуры промышленного сегмента Национального киберполигона

Инфраструктура промышленного сегмента Национального киберполигона выполняется в соответ-

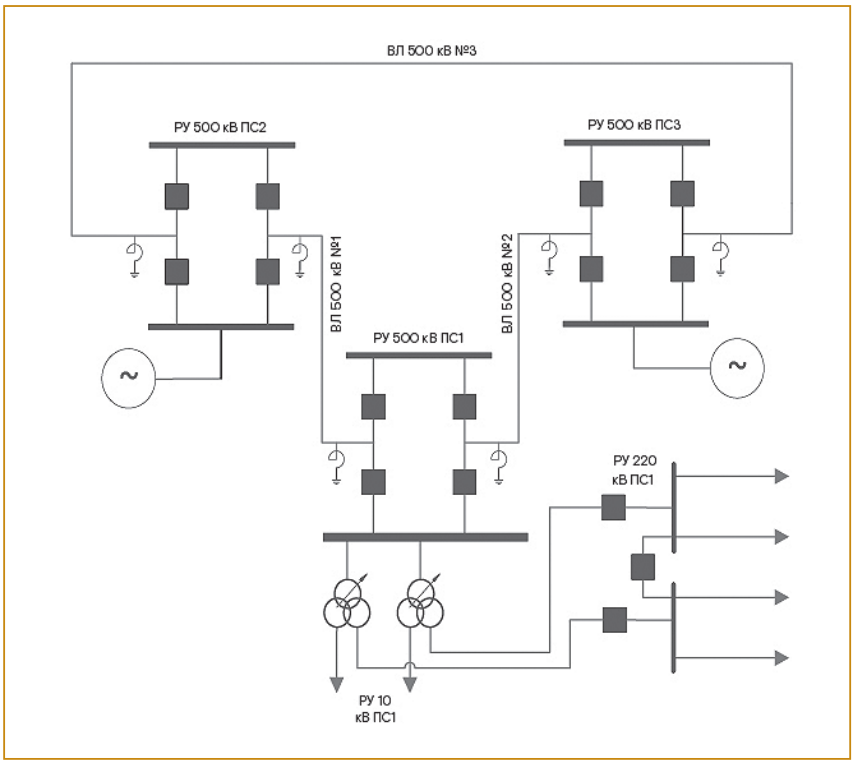

Рис. 2. Структурная схема модели магистральных электрических сетей в RTDS

ствии с трехуровневой архитектурой, при этом для организации среднего и верхнего уровней применяются реальные компоненты систем промышленной автоматизации в рамках концепции полунатурного моделирования. Нижний уровень (уровень объекта) представлен программно-аппаратным комплексом RTDS, в котором реализована математическая модель электроэнергетической системы, участка электрической сети или энергообъекта. Средний уровень представлен основными системами автоматизации, которые применяются на промышленных объектах: на данном уровне установлены система релейной защиты и автоматики (РЗА), система мониторинга переходных режимов (СМПР), система коммерческого учета электроэнергии (АИИС КУЭ). Верхний уровень создаваемой модели представлен АСУТП и системами диспетчерского управления.

Расположенный на нижнем уровне трехуровневой архитектуры программно-аппаратный комплекс RTDS позволяет детально моделировать процессы, происходящие на объектах электроэнергетики. В рамках реализации проекта в программном комплексе RSCAD была смоделирована типовая инфраструктура магистральных электрических сетей (схема представлена на рис.2).

Схема состоит из трех подстанций 500 кВ, соединенных между собой линиями электропередачи по кольцевой схеме, питание осуществляется от двух эквивалентных энергосистем. Одна из подстанций смоделирована более детально: представлены силовые трехобмоточные трансформаторы 500/220/10 кВ с устройством регулирования напряжения (РПН), РУ 220 кВ шунтирующие реакторы (ШР) на ЛЭП 500 кВ для компенсации реактивной мощности на линии. В модели реализована вся необходимая коммутационная аппаратура: выключатели, разъединители и заземляющие ножи с оперативной блокировкой.

Для системы мониторинга выводятся основные измерения в контрольных точках (напряжения и токи в узлах сети, передаваемые активные и реактивные мощности). Поскольку программно-аппаратный комплекс RTDS может взаимодействовать со вторичным оборудованием (системой РЗА, АСУТП) как посредством аналоговых и дискретных физических сигналов, так и при помощи цифровых протоколов связи IEC 61850 9.2 LE (Sampled Values), IEC 61850 8–1 (GOOSE), в рамках создания инфраструктуры Национального киберполигона был выбран второй вариант, так как целевым моделируемым объектом электрических сетей является «цифровая подстанция».

Система релейной защиты и автоматики, расположенная на среднем уровне, представлена оборудованием нескольких отечественных и зарубежных производителей и выполняет основные функции релейной защиты и автоматики, регламентированные НТД ПАО ФСК ЕЭС:

– терминалы основной и резервной защит линии 500 кВ (выполнены на оборудовании производства компаний Siemens, Релематика, ЧЭАЗ, General Electric);

– терминалы основной и резервной защит трансформатора (выполнены на оборудовании производства компаний Siemens, ЭКРА, Релематика, ЧЭАЗ);

– комплекты ступенчатых защит (КСЗ) линий 220 кВ (реализованы на базе терминалов ЭКРА, Siemens, Релематика, General Electric);

– инженерные АРМ для конфигурирования устройств РЗА.

Оборудование системы мониторинга переходных режимов (СМПР) уровня присоединения, а также концентратор данных СМПР представлены устройствами производства «Энергосервис».

Оборудование системы АИИСКУЭ уровня присоединения представлено устройствами производства Энергосервис, «Прософт-Системы». В качестве устройства сбора и передачи данных (УСПД) использован виртуальный контроллер КМ ЭНТЕК.

В состав АСУТП, расположенной на верхнем уровне, входят контроллеры АСУТП, а также программное обеспечение систем промышленной автоматизации (SCADA):

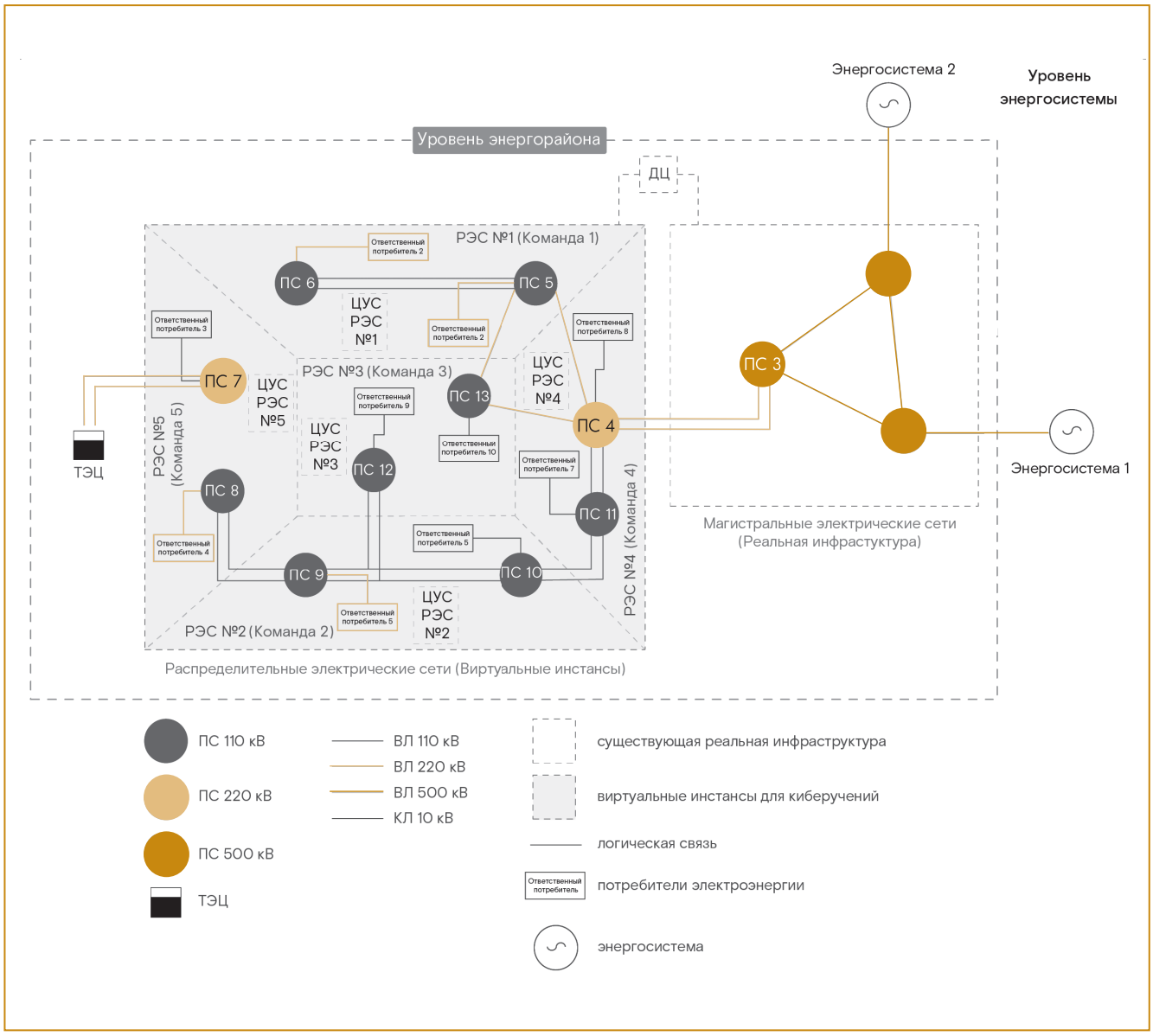

Рис. 3. Схема электроснабжения, используемая в рамках учений

– контроллеры присоединения, выполняющие функцию управления коммутационными аппаратами, производства компании «Прософт-Системы»;

– контроллеры, выполняющие функцию шлюза телемеханики (передачи данных в диспетчерский центр) производства компаний «Прософт-Системы», General Electric, PLC Technologies;

– программное обеспечение платформ промышленной автоматизации SCADA производства General Electric, Siemens, ЧЭАЗ, ИнСАТ;

– инженерные АРМ для конфигурирования устройств АСУТП

Программное обеспечение диспетчерского центра включает в себя сервер системы диспетчерского управления с установленным программным обеспечением «ОИК Диспетчер НТ» и сервер системы АИИСКУЭ с установленным программным обеспечением «Энергосфера». Также на уровне диспетчерского центра расположены автоматизированные рабочие места диспетчерского персонала.

Практика применения

Технологическая инфраструктура Национального киберполигона и сформированная методологическая база по подготовке и проведению киберучений позволяет проводить на площадке Национального киберполигона киберучения для отработки вопросов взаимодействия как внутри одной организации, так и нескольких организации в области электроэнергетики в условиях скоординированных компьютерных атак. В настоящий момент на базе Национального киберполигона выстроены процессы подготовки и проведения киберучений различного уровня, что позволяет проводить данные мероприятия на регулярной основе.

На базе Национального киберполигона в период 2020–2021 гг. был проведен ряд киберучений

в формате командно-штабных тренировок с целью изучения основных аспектов обеспечения информационной безопасности инфраструктурных объектов РФ и отработки действий субъектов КИИ в условиях целенаправленных компьютерных атак.

В конце 2019 г. на площадке ПАО «Ростелеком» были организованы штабные киберучения по анализу нарушений работоспособности объектов электроэнергетического комплекса в результате компьютерных атак на системы управления и защиты цифровых подстанций. Киберучения были проведены совместно с Минэнерго России и другими федеральными органами исполнительной власти, а также с участием представителей отрасли электроэнергетики. Целью учений являлось повышение уровня осведомленности сотрудников и руководителей профильных организаций РФ о способах повышения защищенности программного и аппаратного обеспечения промышленной автоматизированной инфраструктуры организаций РФ, в том числе объектов КИИ и, как следствие, повышение уровня обеспечения информационной безопасности КИИ [7].

В августе 2020 г. на площадке ПАО «Ростелеком» в рамках штабных киберучений состоялся деловой обмен мнениями по вопросам информационной безопасности предприятий электроэнергетики, участвующих в обеспечении г. Москвы и Московской области. Участие в мероприятии приняли отраслевые специалисты разных уровней и профилей: руководителей, специалистов по ИБ, технологов и регуляторов. В ходе учений была отмечена необходимость совершенствования отраслевой нормативной базы в части информационной безопасности (стратегия, политика, регламенты).

В декабре 2020 г. на базе Национального киберполигона были проведены первые киберучения, включающие практическую составляющую. Киберучения были проведены с целью повышения готовности участников к нештатным ситуациям, связанных с целенаправленными компьютерными атаками на электроэнергетический комплекс, а также отработки практических сценариев взаимодействия, реагирования и противодействия атакам, а их участниками стали представители субъектов КИИ электроэнергетики, а также представители отраслевого регулятора и регулятора в сфере информационной безопасности.

Согласно замыслу киберучений, защищаемая инфраструктура (электрические сети вымышленного города-миллионника) была разделена на несколько районов электрических сетей (РЭС); в качестве отдельного сегмента была выделена инфраструктура магистральных электрических сетей (МЭС). В каждом районе находилось несколько подстанций высокого класса напряжения и некоторое число ответственных потребителей, не обладающих резервными источниками электроснабжения (рис. 3).

В ходе киберучений организаторами проводились тренировочные компьютерные атаки, направленные на компрометацию технологического сегмента, целью которых было полное прекращение электроснабжения потребителей города. Каждая команда участников киберучений играла роль сотрудников одного из регионов электрических сетей (РЭС) или магистральных электрических сетей (МЭС) и была ответственна за непрерывное функционирование и безопасность соответствующего района электрических сетей. Участники проводили оценку защищенности инфраструктуры РЭС и МЭС, а также выявляли компьютерные атаки и осуществляли реагирование на них.

Для координации действий команд по выявлению и противодействию компьютерным атакам было сформировано специальное техническое подразделение – центр по реагированию на компьютерные инциденты (Computer Emergency Response Team - CERT), в которое вошли представители регулятора в области информационной безопасности и организаторы киберучений, обладающие навыками реагирования на компьютерные атаки в технологическом сегменте с учетом отраслевой специфики. В рамках киберучений также был сформирован штаб, участники которого в формате командно-штабной тренировки рассматривали последствия реализации указанных выше сценариев, оценивали достаточность типовых планов по ликвидации чрезвычайной ситуации в условиях веерного отключения электроэнергии, а также вырабатывали первоочередные меры по локализации последствий компьютерных атак и недопущению их в будущем. В штаб вошли представители органов государственной власти, а также представители электроэнергетических компаний.

Проведенные киберучения позволили повысить готовность технических специалистов субъектов КИИ к реагированию на компьютерные атаки, провести практическую отработку сценариев взаимодействия, реагирования и противодействия комплексным компьютерным атакам. Участники и регуляторы высоко оценили значимость CERT для координации реагирования субъектов КИИ электроэнергетики на компьютерные атаки, в том числе прогнозирования развития атаки с учетом отраслевой специфики. Наличие в CERT должной компетенции и навыков реагирования на компьютерные атаки в технологическом сегменте электроэнергетики, позволили на основании полученной от субъектов КИИ информации о векторах компьютерных атак в корпоративном сегменте спрогнозировать развитие компьютерной атаки в технологическом сегменте и выдать рекомендации субъектам по устранению уязвимостей, что привело к предотвращению повторных атак на инфраструктуру.

Кроме того, представители регулятора в области информационной безопасности и представители Министерства энергетики отметили необходимость повышения внимания руководства субъектов КИИ электроэнергетики к вопросам информационной

безопасности и повышению осведомленности сотрудников о возможных угрозах и компьютерных атаках. Отдельно была отмечена необходимость проведения киберучений на регулярной основе наряду с проводимыми в настоящее время тренировками оперативного-диспетчерского персонала объектов электроэнергетики.

Список литературы

1. Интегрированный годовой отчет ПАО «ФСК ЕЭС» за 2020 г. https://www.fsk-ees.ru
2. Концепция цифровой трансформации 2030 ПАО «Россети». https://www.rosseti.ru/investment/Kontseptsiya_Tsifrovaya_transformatsiya_2030.pdf
3. *Карпенко В.И., Карантаев В.Г., Архангельский О.Д., Кузнецов А.В., Сютов Д.В.* Анализ последствий влияния кибератак на системы релейной защиты и противоаварийной автоматики подстанций высоких классов напряжений // Релейщик. 2020. № 2 (36). С. 40–42.
4. Цифровое сообщество готовится отражать кибератаки. Исследование глобальных тенденций информационной безопасности на 2018 г. Основные выводы. 2018. https://www.pwc.ru/ru/assets/gsiss-strengthening-digital-society-ru.pdf
5. *Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г.* Киберопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. №4 (17).
6. *Kick J.* Cyber Exercise Playbook. The MITRE Corporation. 2014.
7. *Карантаев В.Г., Архангельский О.Д., Кузнецов А.В., Сютов Д.В.* Опыт проведения киберучений по анализу нарушений работоспособности объектов электроэнергетического комплекса в результате кибератак // Релейщик. 2020. № 1 (35). С. 54–56.

Архангельский Олег Денисович *– руководитель направления методологии и консалтинга Национального киберполигона;* ***Кузнецов Андрей Владимирович*** *– технический директор Национального киберполигона;* ***Сютов Дмитрий Владимирович*** *– руководитель направления инфраструктурных решений Национального киберполигона;* ***Никонёнок Максим Петрович*** *– эксперт по полунатурному моделированию «Ростелеком-Солар».*
Http://rt-solar.ru

Минимизация удельных энергозатрат на производство единицы продукции для крупнейшего деревообрабатывающего комбината страны

АО «Череповецкий фанерно-мебельный комбинат» (г. Череповец Вологодской обл.) по объемам производства фанеры и древесно-стружечных плит входит в пятерку крупнейших предприятий деревообрабатывающей отрасли России. Затраты на электроэнергию составляют существенную долю в технологической себестоимости производства продукции АО «ЧФМК». Основной целью проекта руководство комбината определило минимизацию удельных энергозатрат на производство единицы продукции.

Для решения этой задачи необходимо было создать систему автоматизированного тотального мониторинга потребления электроэнергии как компонента системы энергоменеджмента (энергоменеджмент в реальном времени). Как показало время, это решение оказалось очень дальновидным особенно при работе в условиях экономического кризиса.

НПФ «КРУГ» разработала для АО «ЧФМК» автоматизированную информационно-измерительную систему технического учета электроэнергии (АИИС ТУЭ), которая функционирует на базе программно-технического комплекса КРУГ-2000. Объекты системы (крупные потребители): сушилки, сушильные барабаны, вентиляторы, дымососы, компрессоры, насосы, здания, сооружения и др. На каждом из них установлены электросчётчики.

Функциональность АИИС ТУЭ «ЧФМК»:

- оперативный контроль потребляемой мощности по каждой единице оборудования и др. электропотребителям. Всего 156 ед.;
- оперативный учёт (суммирование) по группам потребителей (по каждому цеху, производству, зданию и др.);
- предоставление информации для контроля соблюдения установленных лимитов (часовых, суточных, месячных) электропотребления для подразделений и цехов;
- предоставление оперативной и достоверной информации для контроля отклонений фактического удельного потребления на единицу продукции от нормативного (план-факт);
- ведение данных, необходимых для расчета небаланса электропотребления по каждой подстанции и предприятию в целом;
- оперативный контроль реактивной мощности;
- предоставление информации для выбора и изменения схемы электроснабжения предприятия для минимизации потерь электроэнергии.

Сервисные функции системы:

- отображение на мониторах АРМ диспетчера (резервируемых) всех параметров учета электроэнергии;
- отображение диагностической информации о наличии связи с приборами учета;
- протоколирование всех событий системы;
- формирование и печать отчетных документов - ведомостей учета;
- синхронизация времени абонентов системы и др.

АИИС ТУЭ «ЧФМК» представляет собой трехуровневую систему.

Первый (нижний) уровень системы включает в себя существующие приборы учета электрической энергии:

- электросчетчики с цифровым выходом (24 ед);
- электросчетчики с импульсным выходом (132 ед.) и счетчики импульсов с цифровым выходом (12 ед.).

Второй (средний) уровень системы представлен шкафом учета с контроллером DevLink-C1000 (4 ед.) для сбора данных с электросчетчиков.

Третий (верхний) уровень содержит:

- резервируемые АРМ диспетчера под управлением SCADA КРУГ-2000, осуществляющие сбор, обработку, хранение и визуализацию данных с контроллеров DevLink-C1000;
- сервер единого времени TimeVisor, осуществляющий синхронизацию времени всех абонентов системы.

Первыми этапами внедрения системы были охвачены центральный распределительный пункт ЦРП-10 и трансформаторные подстанции ТП-3, ТП-4 и ТП-5.

В рамках 3-го этапа внедрения АИИС ТУЭ в адрес предприятия произведена поставка очередных шкафов учета с промышленными контроллерами DevLink-C1000 для интеграции в систему подстанций ТП-6 и ТП-7. Монтажные работы выполняются сотрудниками АО «ЧФМК».

В 2022 г. планируется дальнейшее расширение системы – подключение к ней оставшихся потребителей электроэнергии.

Https://www.krug2000.ru