УДК 621.311

АНАЛИЗ КИБЕРБЕЗОПАСНОСТИ ЦИФРОВОЙ ПОДСТАНЦИИ С ПОЗИЦИЙ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ[1]

Колосок Ирина Николаевна

Д.т.н., ведущий научный сотрудник лаборатории «Управление функционированием электроэнергетических систем», e-mail: kolosok@isem.irk.ru

Коркина Елена Сергеевна

К.т.н., старший научный сотрудник лаборатории «Управление функционированием электроэнергетических систем», e-mail: korkina@isem.irk.ru

Институт систем энергетики им. Л.А. Мелентьева СО РАН,

664130 г. Иркутск, ул. Лермонтова 130

Аннотация. Цифровая подстанция (ЦПС) - важное звено технологического управления электроэнергетической системой. В связи с «цифровизацией» энергетики и развитием электроэнергетических систем на основе инновационных средств и технологий современные объекты электроэнергетики, в том числе и цифровые подстанции, необходимо рассматривать как сложные комплексные кибер-физические системы. В статье рассмотрена структура цифровой подстанции с позиций кибер-физической системы, выполнен анализ факторов, влияющих на «глубину» снижения функциональности цифровой подстанции при кибератаках, реакцию кибернетической и физической подсистем ЦПС на различные атаки, а также предложены меры противодействия кибератакам для этих подсистем.

Ключевые слова: цифровая подстанция, кибербезопасность, кибер-физическая система, кибератаки.

Цитирование: Колосок И.Н., Коркина Е.С. Анализ кибербезопасности цифровой подстанции с позиций киберфизической системы // Информационные и математические технологии в науке и управлении. 2019. № 3 (15). С. 121–131. DOI: 10.25729/2413-0133-2019-3-11

Введение. Современная электроэнергетическая система (ЭЭС) и ее объекты – это сложные системы, состоящие из двух тесно взаимосвязанных между собой подсистем: физической (технологической) и информационно-управляющей. По мере «цифровизации» ЭЭС [2, 12] информационно-коммуникационная подсистема, выполняющая функции управления, становится сопоставимой по сложности и уязвимости с физической подсистемой. Таким образом, современные объекты энергетики можно в полной мере отнести к кибер-физическим системам (КФС).

Концепция кибер-физической системы (КФС) основана на интеграции вычислительных ресурсов в физические процессы [13]. В КФС датчики, коммуникации и информационные (интеллектуальные) системы интегрированы в единую цепочку создания продукции. Именно кибер-физические системы служат основой интеллектуального распределенного управления при функционировании ЭЭС.

[1]Работа выполнена при поддержке гранта РФФИ (№19-07-00351 А)

В [11] рассматривается надежность КФС электроэнергетического объекта. Электрооборудование отнесено к категории физических компонентов (ФК) – это технические устройства первичного оборудования, управляемые с помощью аналоговых сигналов. К категории кибернетических компонентов (КК) отнесены интеллектуальные устройства, обеспечивающие сбор, обработку и передачу информации в цифровом виде от физических компонентов в Центр Управления или для взаимодействия ФК.

При оценке работоспособности КФС один из основных показателей – уровень надёжности и безопасности. КФС должны быть работоспособны в непредвиденных обстоятельствах, адаптироваться и восстанавливаться.

Процесс «цифровизации» энергетических систем, использование интеллектуальных технологий, сложного технического, информационного и коммуникационного оборудования повысили риски в области кибербезопасности энергетических предприятий, в том числе и ЦПС. В [10] отмечается возрастание угроз кибербезопасности с связи с развитием концепции интеллектуальных энергетических систем, в рамках которой предусматривается повышение уровня компьютеризации и интеллектуализации энергетики.

Наиболее уязвимыми к кибератакам (КА) являются компоненты информационно-коммуникационной подсистемы, но поскольку в КФС обе подсистемы тесно взаимосвязаны, то потеря и недостоверность информации вследствие КА на информационно-коммуникационную подсистему могут привести к выработке и реализации неправильных управляющих воздействий и к развитию аварийных ситуаций в физической подсистеме как самой ЦПС, так и в ЭЭС в целом.

В свою очередь, отказ элемента физической подсистемы может привести к аварийному состоянию электрической части и способствовать выходу из строя системы управления информационно-коммуникационной подсистемы [7].

В статье будет рассмотрена структура ЦПС с позиций КФС, взаимосвязь физических и кибернетических компонентов, выполнен анализ возможных кибератак, рассмотрены способы их обнаружения и предложены меры для уменьшения влияния последствий кибератак на надежность функционирования ЦПС.

1. Структура ЦПС. Взаимосвязь физических и кибернетических компонентов ЦПС. Электрическая подстанция (ПС) служит для преобразования, распределения и передачи электроэнергии и является важным элементом технологического управления в ЕЭС. Основные функции ПС:

- технологическая связь и передача данных;
- управление противоаварийной автоматикой;
- релейная защита и автоматика;
- автоматизированная система управления технологическим процессом (АСУ ТП);
- учет электроэнергии и мощности (АИИСКУЭ);
- видеонаблюдение, пожарная и охранная сигнализации.

Цифровая подстанция с технической точки зрения – это обычная подстанция, выполняющая основные технологические функции передачи, преобразования, распределения и снабжения электроэнергией потребителей, но в которой информация, необходимая для выполнения технологических задач различными устройствами и электрооборудованием, передается в цифровом виде на основе международного стандарта IEC 61850 (в России – МЭК 61850) по оптоволоконным каналам связи [14, 6].

По результатам опроса ведущих российских и зарубежных специалистов в области ЦПС, проведенного в журнале «Цифровая Подстанция», можно сформулировать определение: ЦПС – это подстанция с высоким уровнем автоматизации управления, в которой практически все процессы информационного обмена между элементами подстанции, обмена с внешними системами, а также управления работой ПС осуществляются в цифровом виде на основе протоколов МЭК61850.

ЦПС – важное звено технологического управления, в сфере её функционирования находится управление противоаварийной автоматикой (ПА), микропроцессорными устройствами (МП) релейной защиты (РЗ), АСУ ТП, АИИСКУЭ, коммуникационная сеть. ЦПС выбрана в качестве примера КФС – там есть первичное, вторичное оборудование, устройства сопряжения, специализированное программное обеспечение (ПО) и др.

Архитектура ЦПС, показанная на рис.1, разделяется на три уровня (снизу вверх) [1]:

- уровень первичного оборудования (процесса): интеллектуальные первичные устройства и оптические кабели, по которым на уровень ячейки идет передача значений напряжения и тока;
- уровень ячейки (присоединения): терминалы МП РЗА, контроллеры присоединений и другое оборудование, традиционно называемое «вторичным»;
- станционный уровень: коммуникации внутри подстанции и элементы системы управления, включая оперативные блокировки и функции самодиагностики на верхнем уровне.

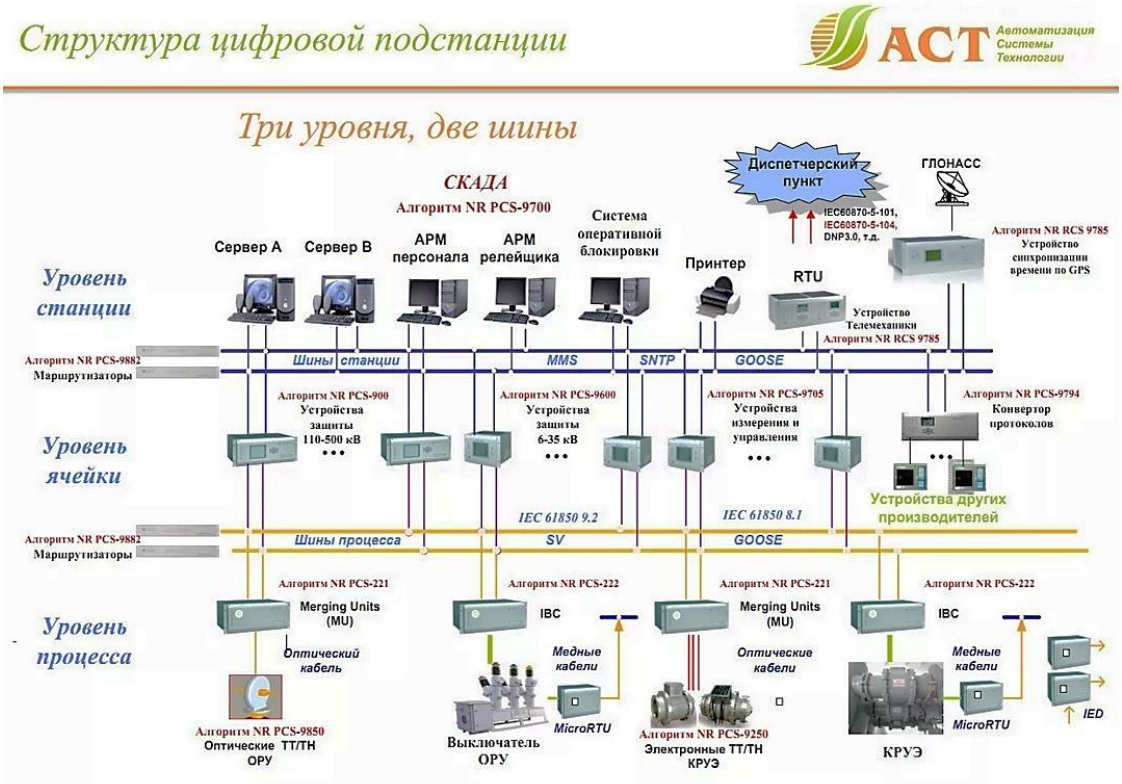

Рис. 1. Структура ЦПС

1.1. Уровень первичного оборудования. ЦПС основана на такой коммуникационной архитектуре, в которой измерения в реальном времени и другие данные передаются от первичного оборудования и встроенных датчиков через шину процесса устройствам,

выполняющим свои функции на основе этих измерений (токи и напряжения, давление и температура для КРУЭ). Наиболее важным является то, что интеллектуальные устройства и системы на подстанции (терминалы РЗА, РАС, PMU модули, измерительные центры, контроллеры присоединений) могут мгновенно обрабатывать данные.

Шина процесса также является связью, по которой информация от первичного оборудования распределительного устройства (РУ) поступает в операторский пункт управления (ОПУ). В полностью цифровой архитектуре команды управления первичным оборудованием также передаются по шине процесса. Таким образом, шина процесса позволяет реализовывать критически важные по времени функции [6].

1.2. Уровень ячейки. Устройства между шиной процесса и станционной шиной называются «вторичным оборудованием». В ЦПС - это интеллектуальные электронные устройства (ИЭУ), которые взаимодействуют:

- с первичным оборудованием через шину процесса;
- с другими устройствами в ячейке;
- с цифровой системой управления через станционную шину.

Они спроектированы для работы в реальном времени с обеспечением безопасности и удовлетворяют требованиям, предъявляемым МЭК 61850. ИЭУ обеспечивают совместимость решений, работу приложений по поддержанию стабильности работы, интеграцию в WACS[2] систему и гораздо лучшую ситуационную наблюдаемость подстанции. Протокол МЭК 61850 позволяет обеспечить полную интеграцию между устройствами. Это дает возможность оптимального использования информации для непрерывного и надежного управления работой подстанции [7].

Ключевые элементы архитектуры: терминалы РЗА, контроллеры присоединений, коммутаторы и Ethernet сеть, измерительные центры, шлюзы, шкафы (в которых оборудование смонтировано, настроено и обеспечено электропитанием), интерфейс оператора, устройства синхронизации времени. Поскольку энергетика относится к сфере объектов критической информационной инфраструктуры (КИИ) согласно ФЗ-187[3] , ключевым элементом являются и приложения по обеспечению кибернетической безопасности.

1.3. Станционный уровень. В ЦПС станционная шина это гораздо больше, чем стандартная шина обмена данными в SCADA системе, т.к. она позволяет большому количеству клиентов выполнять обмен данными, поддерживает соединение устройств точка-точка и подключение шлюзов для организации взаимодействий между подстанциями.

ИЭУ выполняют свои критичные по времени функции, такие как защита, контроль синхронизма и другие задачи с прямым подключением к шине процесса. Дополнительно, другие клиенты на подстанции также могут получать при необходимости доступ к этим данным. Например, функции защиты и управления могут быть распределены между несколькими ИЭУ.

Также существует необходимость распределения информации между локальными и удаленными операторами, что позволяет отображать текущее состояние подстанции в реальном времени. Это требует организации взаимодействия между интерфейсом оператора,

[2] Wide Area Control System – широкомасштабная система управления на основе синхронизированных векторных измерений
[3] ФЗ-187“О безопасности критической информационной инфраструктуры Российской Федерации” от 26.07.2017

шлюзами и удаленными серверами управления. Одна или больше рабочих станций могут выполнять команды от оператора сети, могут использоваться как инженерная станция для конфигурации ИЭУ или как локальный концентратор информации, и выполнять функции архивирования. Система мониторинга в реальном времени также может включать специальные рабочие станции для отображения состояния и просмотра архива по каждому типу первичного оборудования [11].

1.4. Информационный обмен. ЦПС базируется на международном стандарте МЭК 61850, первая глава которого определяет трёхуровневую архитектуру системы автоматизации. Там же приведены Перечень интерфейсов и их назначение [4]:

- обмен сигналами функций защиты между уровнями присоединения и станции, между уровнем присоединения одного объекта и уровнем присоединения смежного объекта;
- обмен данными в рамках уровня присоединения, между уровнем станции и удаленным рабочим местом инженера, а также в рамках уровня станции;
- обмен сигналами функций управления между уровнем станции и удаленным диспетчерским центром, между уровнями присоединения двух различных объектов.

2. Кибербезопасность ЦПС с позиций КФС [5, 8, 9, 15, 16]. Для обеспечения информационно-технологической защищённости ЦПС должна обладать свойствами устойчивости, адаптивности, восстанавливаемости, которые могут быть развиты на основе глубокого анализа проблем безотказной работы ЦПС. Отличительной особенностью ЦПС является передача информации через сеть с коммутацией пакетов Ethernet, настроенную специальным образом (шина процесса и шина подстанции – в терминологии МЭК 61850). В связи с этим закрытость объекта больше не является барьером для злоумышленника, и, если не принять специальных защитных мер, все данные на верхнем уровне автоматизации подстанции с внедрением этого Стандарта могут стать доступными для кибератак. Кроме того, к угрозам безопасности обычной подстанции, которые на ЦПС, как правило, усиливаются, добавляются угрозы вмешательства в работу шины процесса и систему синхронизации времени. Киберустойчивость (или киберупругость) энергосистемы – относительно новый термин, характеризующий её способность восстанавливаться после реализации явно направленных или скрытых кибератак. Согласно ФЗ №187 “средствами, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, являются технические, программные, программно-аппаратные и иные средства … , а также криптографические средства защиты такой информации”.

Анализируя компоненты ЦПС, показанные на рис. 1, и их функции, можно разделить все оборудование ЦПС на физическую и кибернетическую подсистемы (компоненты) следующим образом:

- к физическим компонентам (ФК) ЦПС относится электрооборудование (трансформаторы, выключатели, разъединители и др.) и установленное на них измерительное оборудование (измерительные ТТ и ТН… и др.),
- к кибернетическим (КК): шина процесса, станционная шина, аналого-цифровые преобразователи, коммутаторы, ИЭУ, маршрутизаторы, терминалы, серверы, систему SCADA, WAMS, АСУ ТП, АСКУЭ, автоматизированные рабочие места (АРМ) технологов и др.

Многие ФК находятся под мониторингом и управлением кибер-компонентами. Некоторые ФК, такие, как удаленные терминальные блоки (RTU), компьютеризированы, т. е. имеют встроенное ПО и подключены к КК, например, к SCADA-серверам. Линия передачи данных является аналогом линии электропередачи в электросети, она физическая по своей природе даже при использовании технологии беспроводной связи. Все компьютеризированные компоненты отнесены к ФК, при этом аппаратное обеспечение отделено от программного обеспечения, работающего на таких ФК.

Кибер-компоненты (ПО, данные) отделены от физических компонентов, которые являются их хостами. КК означают фактический читаемый компьютером код и данные, которые находятся на каком-либо физическом компоненте.

Ряд известных кибератак – “отказ в обслуживании” (DoS–атака), внедрение вирусов и программного обеспечения с “закладками”, подмена сигналов GPS/ потока мгновенных значений (SV-потока)/ MMS и GOOSE-сообщений, переполнение трафика и пр. – являются прямыми угрозами работоспособности ЦПС. В Таблице 1 сопоставляются последствия, к которым ведут атаки в информационной и физической подсистемах ЦПС, и возможные меры противодействия этим атакам.

Таблица 1.

КИБЕР-АТАКА	**Последствия**		**Меры противодействия**	
	Киберподсистема	**Физическая подсистема**	**Киберподсистема**	**Физическая подсистема**
1. Анализ сетевого трафика	Кража данных о сетевой конфигурации объекта	Для технологического процесса угрозы нет	Шифрование	Не требуются
2.Специали-зированное вредоносное ПО, “закладки”, вызывающие ошибки в работе ОС Windows	Проникновение в операционную систему Windows	РАБОТА В РУЧНОМ РЕЖИМЕ	В силу того, что нет разработанных антивирусов, приходится ликвидировать такую аппаратуру.	РАБОТА В РУЧНОМ РЕЖИМЕ
3.Атака по изменению прикладного ПО путем внедрения вредоносного ПО	• Взлом серверов и рабочих станций, • удаленное управление вычислительными ресурсами, • администрирование каналов	• Некорректная работа программных приложений. • Срабатывание аппаратных и программных закладок. • Нежелательное отключение/срабатывание интеллектуаль-ных устройств.	• Авторизация пользователей; • Системы обнаружения и предотвращения вторжения; • установка антивируса; • запрет использования флэш-карт, замена их на CD.	Использование традиционных аналоговых цепей
4.DoS–атака (отказ в обс-луживании)	Вывод из строя маршрутизатора, коммутатора многочисленными запросами к сети	• Задержка управления; • отказ отключения/ срабатывания интеллекту-альных устройств	• Строгие правила аутентификации, возможность идентификации IP-адреса злоумышленника	Дублирование IED-устройств и каналов

КИБЕР-АТАКА	Последствия		Меры противодействия	
	Киберподсистема	**Физическая подсистема**	**Киберподсистема**	**Физическая подсистема**
5.Задержка передачи пакетов вследствие изменения маршрута	Потеря информационных пакетов	Задержка команд управления	Закрытие портов; усиление защиты коммутаторов/маршрутизаторов/ NMS ("система управления сетью")	Использование традиционных аналоговых цепей или РАБОТА В РУЧНОМ РЕЖИМЕ
6.Наведение повторных кибер- или физических атак	Срабатывает как атака по изменению маршрута в сети	Задержка команд управления	Системы обнаружения вторжения	Использование традиционных аналоговых цепей или РАБОТА В РУЧНОМ РЕЖИМЕ
7.Подмена сигналов GPS	Ошибка синхронизации времени	Возможно рассогласование команд на отключение/срабатывание интеллектуальных устройств	Использование VLAN ("виртуальная локальная сеть"); мониторинг направления антенны; дублирование приемников	Мониторинг состояния оборудования
8.Подмена SV-потока, MMS-, GOOSE-сообщений	SV-поток – это измерения первичного оборудования, GOOSE-управляющие сигналы, MMS- обмен с верхним уровнем управления	Нежелательное отключение/ срабатывание; отказ отключения/ срабатывания	Аутентификация сообщений	Мониторинг состояния оборудования
9.Проникновение через Интернет корпоративной сети (через web- или FTP-сервер)	Кража, искажение и стирание информации	• Некорректная работа программных приложений, • неверные команды управления, • нежелательное отключение/срабатывание интеллектуальных устройств.	Корректное конфигурирование сетевых операционных систем и средств защиты	Использование традиционных аналоговых цепей или РАБОТА В РУЧНОМ РЕЖИМЕ
10.Проникновение в локальную сеть ПС с последующим искажением информации (ЧМИ)	4 категории воздействия на структуру человеко-машинного интерфейса: повреждение памяти, управление учетными данными, отсутствие аутентификации / авторизации и небезопасные значения по умолчанию	Формирование ложных команд на управление сетью, электронным оборудованием, отключение элементов сети;	• Строгие правила доступа к сети, правильная конфигурация Firewall. • Приглашение только сертифицированных специалистов для наладки.	Использование традиционных аналоговых цепей или РАБОТА В РУЧНОМ РЕЖИМЕ

На недавно введенных в эксплуатацию пилотных российских цифровых подстанциях (ЦПС 35/6 кВ «Бабайки», ПС 110/10 кВ имени М.П. Сморгунова, ПС 500 кВ «Тобол», ЦПС 110/20кВ Медведевская) осуществлены следующие меры по предотвращению различных угроз работоспособности ЦПС и защитные средства для их кибер-физических систем [3]. Это 100% дублирование сети, высокая степень автоматизации и управляемости оборудования, самодиагностики и учета аварийных событий, организация на РЗА двух параллельных систем: цифровой и классической, полная изолированность шины процесса и

шины подстанции от внешней сети для исключения возможности постороннего дистанционного вмешательства, применена технология параллельного резервирования.

Заключение. Процесс «цифровизации» энергетических систем, использование интеллектуальных технологий, сложного технического, информационного и коммуникационного оборудования повысили риски в области кибербезопасности энергетических предприятий, в том числе и цифровой подстанции. Среди основных направлений цифровизации электроэнергетики важное место отводится развитию цифровых технологических систем производства, транспорта, диспетчеризации и потребления электроэнергии. Цифровая подстанция является одним из пилотных проектов развития цифровизации электроэнергетики.

Потеря и недостоверность информации вследствие кибератак на информационно-коммуникационную подсистему могут привести к выработке и реализации неправильных управляющих воздействий и к развитию аварийных ситуаций в физической подсистеме как самой ЦПС, так и в ЭЭС в целом, поэтому проблема киберустойчивости объектов энергетики является критически важной и должна решаться как техническими средствами, так и организационными, включая повышение квалификации оперативного персонала.

СПИСОК ЛИТЕРАТУРЫ

1. АСТ. Автоматизация. Системы. Технологии. Режим доступа: http://autosystech.ru/?page_id=676 (дата обращения 14.05.19).
2. Воропай Н.И., Губко М.В., Ковалев С.П., Массель Л.В., Новиков Д.А., Райков А.Н., Сендеров С.М., Стенников В.А. Проблемы развития цифровой энергетики в России // Проблемы управления. 2019. №1. С. 2–14.
3. Воропай Н.И., Колосок И.Н., Коркина Е.С. Проблемы повышения киберустойчивости цифровой подстанции // Релейная защита и автоматизация. 2019. Т. 34. № 1. С. 78–83.
4. Головин А., Аношин А. Структура стандарта МЭК 61850 // Цифровая подстанция. 2012. Режим доступа: http://digitalsubstation.com/blog/2012/10/18/struktura-standarta-me-k-61850/ (дата обращения 28.06.18)
5. Зинин В.М., Подлесный А.М., Карантаев В.Г. Цифровая подстанция – объект критической инфраструктуры // Автоматизация и IT в энергетике. 2017. №4(93). С. 28–32.
6. Иванченко А.Ф. Управление и оперативное обслуживание подстанций Единой национальной электрической сети. Часть 1 // Энергетик. 2018. № 10. Библиотечка электротехника. 96 с.
7. Куликов А.Л., Зин ин В.М. Создание системы кибербезопасности в электроэнергетике РФ с учетом реализации Концепции ИЭС ААС // ЭЭ ПиР. 2015. №5(32). С. 122–126.
8. Куликов А.Л., Зинин В.М., Петров А.А. Обеспечение кибербезопасности в технологии «Цифровой подстанции» с учетом импортозамещения // Релейная защита и автоматика энергосистем. Материалы Межд. научно-технической конференции. 2017. С. 941–944.
9. Левшин В.П., Шурдов М.А. Кибербезопасная ЦПС // Электроэнергия. Передача и распределение. 2018. №4(49). С. 24–26.

10. Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г. и др. Киберопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. №4(17). С. 2–10.
11. Обычайко Д.С., Шихин В.А. Разработка комбинированного метода оценки эксплуатационной надёжности КФС // Материалы Всеросс. НТконф. “Инф.технологии в электротехнике и электроэнергетике”. Чебоксары. 2018. С. 118–121.
12. Холкин Д. Цифровая энергетика: что это такое? // Цифровая подстанция. 2018. №10. С. 52–55.
13. Цветков В.Я. Распределенное интеллектуальное управление // Государственный Советник. 2017. №1. С. 16–22.
14. Цифровая подстанция. Эффективные решения // Журнал «ИСУП». Режим доступа: http://isup.ru/articles/6/13855/ (дата обращения 14.05.19)
15. Gouglidis A., Green B., Hutchison D., Alshawish A., and Hermann de Meer. Surveillance and security: protecting electricity utilities and other critical infrastructures. Available at: https://doi.org/10.1186/s42162-018-0019-1. (accessed 16.01.19)
16. Mehrdad S., Mousavian S., Madraki G., Dvorkin Yu. Cyber-physical resilience of electrical power systems against malicious attacks: A review // Current Sustainable / Renewable Energy Reports. Available at: https://doi.org/10.1007/s40518-018-0094-8 (accessed 28.06.18)

UDK 621.311

AN ANALYSIS OF CYBER SECURITY OF A DIGITAL SUBSTATION IN TERMS OF CYBER PHYSICAL SYSTEM [4]

Irina N. Kolosok
Professor, Leading Researcher of Laboratory of Electric Power Systems Operation and Control,
e-mail: kolosok@isem.irk.ru
Elena S. Korkina
Doctor, Senior Researcher of Laboratory of Electric Power Systems Operation and Control,
e-mail: korkina@isem.irk.ru
Melentiev Energy Systems Institute Siberian Branch of the Russian Academy of Sciences
130, Lermontov Str., 664033, Irkutsk, Russia

Abstract. Digital substation is an important component in the technological control of electric power system. In the context of the energy sector digitalization and the development of electric power systems based on innovative tools and technologies, modern electric power facilities, including digital substations, must be viewed as complex integrated cyber-physical systems. The paper gives consideration to the structure of a digital substation from the perspective of a cyber-physical system. An analysis of the factors affecting the extent to which the functionality of a digital substation is reduced during cyberattacks, and the factors contributing to its speedy restoration is made.

[4]This study is supported by RFBR grant №19-07-00351 A.

Keywords: Digital substation, cyber security, electric power system, cyber physical system.

References

1. AST. Avtomatizatsiya. Sistemy. Tekhnologii [Automation. Systems. Technology.] Available at: http://autosystech.ru/?page_id=676 (accessed 14.05.19) (in Russian)
2. Voropai N.I., Gubko M.V., Kovalev S.P., Massel' L.V., Novikov D.A., Rajkov A.N., Senderov S.M., Stennikov V.A. Problemy razvitiya cifrovoj energetiki v Rossii [Digital Energy Development Problems in Russia] // Problemy upravleniya = Control Sciences. 2019. №1. Pp. 2–14. (in Russian)
3. Voropai N.I., Kolosok I.N., Korkina E.S Problemy povysheniya kiberustojchivosti cifrovoj podstancii [An Increase in Cyber Resilience of Digital Substation] // Relejnaya zashchita i avtomatizaciya = Relay Protection and Automation. 2019. V.34. № 1. Pp. 78–83. (in Russian)
4. Golovin A., Anoshin A. Struktura standarta MEK 61850 [IEC 61850 Standard Structure] // Cifrovaya podstanciya = Digital substation. 2012. Available at: http://digitalsubstation.com/blog/2012/10/18/struktura-standarta-me-k-61850/ (accessed 28.06.18) (in Russian)
5. Zinin V.M., Podlesnyj A.M., Karantaev V.G. Cifrovaya podstanciya – ob"ekt kriticheskoj infrastruktury [Digital substation – object of critical infrastructure] // Avtomatizaciya i IT v energetike = Automation and IT in power engineering. 2017. № 4 (93). Pp. 28–32. (in Russian)
6. Ivanchenko A.F. Upravlenie i obsluzhivanie podstanciej ENES [Management and maintenance of substations of National Power Grid.] // Energetik (Bibliotechka elektrotekhnika) = Power Engineer (Application). 2018. 96 p. (in Russian).
7. Kulikov A.L., Zinin V.M. Sozdanie sistemy kiberbezopasnosti v elektroenergetike RF s uchetom realizacii Koncepcii IES AAS [Creation of a cybersecurity system in the electric power industry of the Russian Federation taking into account the implementation of the IES AAS Concept] // EE PiR = Electric Power. Transmission and Distribution. 2015. №5 (32). Pp. 122–126. (in Russian)
8. Kulikov A.L., Zinin V.M., Petrov A.A. Obespechenie kiberbezopasnosti v tekhnologii «Cifrovoj podstancii» s uchetom importozameshcheniya [Cyber security of a digital substation in the “Digital Substation” technology with account of import substitution.] // Relejnaya zashchita i avtomatika energosistem = Relay protection and automatic of energy systems. St.-Petersburg. 2017. Pp. 941–944. (in Russian)
9. Levshin V.P., Shurdov M.A. Kiberbezopasnaya CPS [Cyber secure DSS] // Elektroenergiya. Peredacha i raspredelenie = Electric Power. Transmission and Distribution. 2018. №4 (49). Pp. 24–26. (in Russian)
10. Massel L., Voropay N., Senderov S., Massel A. Kiberopasnost' kak odna iz strategicheskih ugroz energeticheskoj bezopasnosti Rossii [Cyber Danger as One of the Strategic Threats to Russia’s Energy Security] // Voprosy kiberbezopasnosti = Cybersecurity issues. 2016. №4(17). Pp. 2–10. (in Russian)
11. Obychaiko D.S., Shikhin V.A. Razrabotka kombinirovannogo metoda ocenki ekspluatacionnoj nadyozhnosti KFS [Development of a combined method for assessing the operating reliability of cyber-physical systems] // Materialy Vseross. NTkonf.

"Inf.tekhnologii v elektrotekhnike i elektroenergetike" = Proc. of XI All-Russia Conference "IT in power engineering". Cheboksary. 2018. Pp. 118–121. (in Russian)

12. Holkin D. Cifrovaya energetika: chto eto takoe? [Digital power engineering: what is it?] // Cifrovaya podstanciya = Digital substation. 2018. №10. Pp. 52–55. (in Russian)
13. Cvetkov V.Ya. Raspredelennoe intellektual'noe upravlenie [Distributed Intelligent Control] // Gosudarstvennyj Sovetnik = State Advisor. 2017. №1. Pp. 16–22. (in Russian)
14. Cifrovaya podstanciya. Effektivnye resheniya [Digital substation. Effective Solutions] // Zhurnal «ISUP» = Magazine «Informatization and management systems in industry». Available at: http://isup.ru/articles/6/13855/ (accessed 14.05.19) (in Russian)
15. Gouglidis A., Green B., Hutchison D., Alshawish A., and Hermann de Meer. Surveillance and security: protecting electricity utilities and other critical infrastructures. Available at: https://doi.org/10.1186/s42162-018-0019-1. (accessed 16.01.19)
16. Mehrdad S., Mousavian S., Madraki G., Dvorkin Yu. Cyber-physical resilience of electrical power systems against malicious attacks: A review // Current Sustainable / Renewable Energy Reports. Available at: https://doi.org/10.1007/s40518-018-0094-8 (accessed 28.06.18)