Роль кибербезопасности цифровых подстанций в цифровизации электроэнергетики / Антонов Р.Б., Сидоров В.А., Медведев М.С. и др.// Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 6(32) с. 157–163

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

РОЛЬ КИБЕРБЕЗОПАСНОСТИ ЦИФРОВЫХ ПОДСТАНЦИЙ В ЦИФРОВИЗАЦИИ ЭЛЕКТРОЭНЕРГЕТИКИ

Антонов Р.Б., [1]Сидоров В.А., Медведев М.С., Алиусманов Г.Э., Климчук И.В.
ФГБОУ ВО "Национальный исследовательский университет "МЭИ", Москва, Россия (111250, г.Москва, Красноказарменная ул., 14), e-mail: [1]SidorovVaAl@yandex.ru

В данном исследовании рассмотрена кибербезопасность цифровых подстанций в парадигме цифровизации электроэнергетики: проанализирована актуальность киберзащиты ЦПС, рассмотрены требования, предъявляемые к кибербезопасности современных ЦПС.

Ключевые слова: Цифровая подстанция (ЦПС), МЭК 61850, кибербезопасность, киберугроза, кибератака.

THE ROLE OF CYBER SECURITY OF DIGITAL SUBSTATIONS IN THE DIGITALIZATION OF THE POWER INDUSTRY

Antonov R.B., [1]Sidorov V.A., Medvedev M.S., Aliusmanov G.E., Klimchuk I.V.
"National Research University "MPEI", Moscow, Russia (111250, Moscow, Krasnokazarmennaya st., 14), e-mail: [1]SidorovVaAl@yandex.ru

This study provides an overview of existing national and foreign software systems for the configuration and verification of electronic documentation in the SCL language developed in the design of digital substations.

Keywords: Digital substation (DS), IEC 61850, cybersecurity, cyber threat, cyber attack.

Развитие энергетической системы и ее «цифровизация» требуют создания высокотехнологичных современных объектов для ее управления — цифровых подстанций (ЦПС). Цифровые подстанции представляют собой сложную систему, совмещающую физическую (технологическую) и информационно-управляющую подсистемы. Физическая подсистема включает в себя первичное оборудование, управляемое аналоговыми сигналами, а информационно-управляющая подсистема — цифровые устройства, предназначенные для сбора, обработки и передачи информации в цифровом виде [1].

Постоянное усложнение информационно-управляющей подсистемы, использование на ЦПС сложных интеллектуальных устройств приводят к уязвимости ЦПС для киберугроз. В целях обеспечения надежной работы ЦПС необходима эффективная система информационной безопасности.

Цифровая трансформация электроэнергетики реализуется посредством формирования единой среды на базе национальных стандартов взаимодействия и универсального формата информационного обмена, разрабатываемых с учетом стандартов Международной электротехнической комиссии (МЭК) [2].

В стратегии развития единой энергетической системы (ЕЭС) следующим этапом является создание цифровых электрических сетей. Согласно стандарту ПАО "Россети", цифровые электрические сети представляют собой организационно-технические комплексы, объединяющие электросетевые объекты, которые оборудованы цифровыми системами для измерения параметров режима сети, контроля состояния оборудования и линий электропередачи, защиты и автоматического предотвращения аварий, а также системами управления сетью и объектами. Взаимный информационный обмен между этими компонентами осуществляется по единым протоколам, обеспечивая синхронизацию по времени [3]. Такие цифровые электрические сети обеспечивают тесное информационное взаимодействие между элементами сети, позволяя передавать данные посредством цифрового обмена. Технологическую связь цифровых электрических сетей и передачу по ним данных в данной концепции осуществляют цифровые подстанции. В контексте эволюции энергетической инфраструктуры, сейчас приоритетным направлением является создание ЦПС и повышение эффективности их работы.

Одной из главных задач создания цифровых подстанций является обеспечение технических условий для перехода к автономным подстанциям, где не требуется постоянное присутствие дежурного персонала, а управление осуществляется из диспетчерских центров или центра управления системой (ЦУС). Кроме того, важным аспектом является интеграция подстанций в цифровые электрические сети. Для выполнения поставленных задач цифровые подстанции должны обеспечивать надежное исполнение их основных технологических функций [4].

Согласно стратегическим направлениям государственной политики в области обеспечения безопасности автоматизированных систем управления технологическими процессами (АСУ ТП), ЦПС являются критически важными объектами инфраструктуры Российской Федерации. Нарушение или прекращение их функционирования имеет серьезные последствия, включая потерю управления, разрушение инфраструктуры, необратимые отрицательные изменения или разрушение экономики страны, региона или административно-территориальной единицы, а также значительное ухудшение безопасности жизнедеятельности населения, проживающего на этих территориях, на продолжительное время [5].

Защита и конфиденциальность обмена информацией, как между устройствами, так и между пользователями системы, обеспечиваются системой информационной безопасности (ИБ) цифровых подстанций.

Для определения угроз информационной безопасности необходимо осуществлять оценку потенциала, оборудования и мотивации потенциальных нарушителей, а также изучать предполагаемые уязвимости в оборудовании и терминалах релейной защиты. Важно также анализировать возможные варианты атак на систему информационной безопасности и учитывать результаты нарушения признаков безопасности информации (таких как целостность, доступность и конфиденциальность). Это позволит эффективно управлять рисками и принимать соответствующие меры по обеспечению безопасности информационных систем.

Концепция развития релейной защиты и автоматики электросетевого комплекса от ПАО «Россети» идентифицирует следующие потенциальные и технически реализуемые угрозы информационной безопасности [6]:

- целенаправленное искажение команд управления и другой информации;
- навязывание ложных команд управления или ложной информации, специально созданных злоумышленником;
- несанкционированные доступ к устройствам, изменение конфигурации технических средств;
- перенаправление (изменение маршрутов) потоков данных для деструктивного воздействия;
- вызов сбоев в работе технических средств или создание неисправностей в них;
- умышленное или непреднамеренное уничтожение или изменение данных, системного и прикладного программного обеспечения системы и устройств релейной защиты и автоматики (РЗА);
- кража, разглашение информации, которая может быть использована для нарушения функционирования устройств релейной защиты.
- инфицирование программного обеспечения автоматизированного рабочего места (АРМ) оперативного персонала и АРМ РЗА компьютерными вирусами;
- сканирование сети технологической связи;
- отказ в обслуживании технических средств РЗА.

К непосредственным источникам угроз информационной безопасности можно отнести [6]:

- иностранные разведывательные службы государств, которые проводят враждебную политику в отношении нашей страны и стремятся нарушить функционирование энергетического комплекса в особый период или во время подготовки и ведения войны;
- террористические организации, криминальные структуры и отдельные лица, такие как хакеры, внутренние и другие нарушители, а также группы лиц, которые используют деструктивные информационные методы для реализации своих корыстных или иных интересов в системах оперативно-технологического управления;
- конкурирующие фирмы и организации.

Самым уязвимым к киберугрозам местом в современной электроэнергетике является оборудование на микропроцессорах, легко поддающееся перепрошивке.

Существуют несколько компонентов цифровой подстанции, которые с наибольшей вероятностью могут стать объектами кибератак и привести к нарушению ее функционирования [7]:

- коммуникационные сети энергообъекта, включая коммутаторы и маршрутизаторы, то есть шины процесса и станции в соответствии с МЭК 61850;
- цифровые устройства релейной защиты, противоаварийной автоматики и АСУ ТП;
- внешние цифровые каналы, которые обеспечивают технологическую и оперативную связь с другими энергообъектами и диспетчерскими пунктами.

Объектами защиты для вышеперечисленных компонентов ЦПС являются [8]:

- данные о параметрах и состоянии управляемого объекта или процесса. Такие данные включают в себя входную (выходную) информацию, управляющую (командную)

информацию, контрольно-измерительную информацию и другую критически важную (технологическую) информацию;

- программно-технический комплекс (ПТК), который включает в себя технические средства, такие как АРМы, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры и исполнительные устройства, а также программное обеспечение (ПО), включающее микропрограммное, общесистемное и прикладное программное обеспечение.

В случае, когда все терминалы РЗА будут объединены в единую локальную сеть, результатом кибератаки может стать полная потеря управления энергообъектом или же несанкционированное управление им. После возврата управления над объектом потребуется обширный ряд пусконаладочных работ продолжительностью до нескольких месяцев, поскольку в результате кибератаки возможны изменение конфигураций цифрового оборудования, нарушение работы ПО энергообъекта.

Пусть несколько соседних подстанций станут целью кибератаки. В таком случае, можно ожидать полного отключения электроснабжения для значительной части потребителей, включая критически важные объекты. Кроме того, следует учитывать возможные повреждения первичного оборудования, которое могло получить ущерб вследствие длительного неотключения короткого замыкания в период кибератаки. Важно отметить, что традиционные системы дальнего резервирования на смежных цифровых подстанциях также могут подвергнуться кибератаке.

Таким образом, важно сохранять некоторые управляющие функции на электромеханическом оборудовании, а не переводить их полностью в цифровые системы. Это позволит немедленно восстановить работу электроэнергетических объектов, несмотря на возможные атаки, которые могут повлиять на цифровые устройства. Совместное использование цифрового и электромеханического оборудования является эффективным методом обеспечения информационной безопасности.

Какие требования предъявляются к кибербезопасности современных ЦПС?

Система информационной безопасности ЦПС должна обеспечивать: целостность информации (отсутствие ее противоправного изменения), доступность информации (свободное использование информации при наличии права доступа), неотказуемость (гарантия невозможности отрицания факта выполнения действий пользователем), подотчетность (однозначная прослеживаемость совершенных действий), подлинность (обеспечение идентичности субъекта или ресурса требованиям), конфиденциальность информации [3].

Информационная безопасность должна обеспечиваться на следующих объектах ПТК ЦПС: АРМы, промышленные серверы, сетевое и телекоммуникационное оборудование, узел связи ЦПС и сеть технологической связи, каналы передачи данных, программируемые логические контроллеры, исполнительные устройства с микропрограммным обеспечением, программное обеспечение, средства защиты информации, оборудование видеонаблюдения.

При этом система обеспечения ИБ включает в себя следующий комплекс организационных и технических мер защиты: применение технических устройств на территории цифровой подстанции, использование аппаратно-программных устройств защиты информации, использование программных средств защиты информации, организационные

меры обеспечения защиты, обеспечивающие безопасные условия работы цифровых подстанций.

Данный комплекс мер должен включать в себя:

- идентификацию и аутентификацию;
- управление доступом;
- ограничение программной среды;
- защиту машинных носителей информации;
- аудит безопасности;
- антивирусную защиту;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности;
- обеспечение доступности;
- защиту технических средств и систем;
- защиту автоматизированной системы и ее компонентов;
- реагирование на компьютерные инциденты;
- управление конфигурацией;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

Процесс "цифровизации" в энергетических системах, применение интеллектуальных технологий и сложного оборудования для обработки информации и коммуникаций, значительно увеличили риски в области кибербезопасности энергетических предприятий, включая цифровые подстанции. Кибератаки на информационно-коммуникационную подсистему ЦПС могут привести к потере и фальсификации информации, что может привести к неправильным управляющим воздействиям и развитию аварийных ситуаций, как на уровне цифровых подстанций, так и в энергосистеме в целом. Поэтому обеспечение киберустойчивости объектов энергетики является критически важной проблемой, которая требует технических и организационных решений, включая повышение квалификации оперативного персонала.

Список литературы

1. Колосок И.Н., Коркина Е.С. Анализ кибербезопасности цифровой подстанции с позиции киберфизической системы [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/analiz-kiberbezopasnosti-tsifrovoy-podstantsii-s-pozitsiy-kiberfizicheskoy-sistemy (дата обращения: 16.06.2023).
2. «Системный оператор: создание Единой цифровой модели ЕЭС – основной итог унификации информационного обмена в электроэнергетике» [Электронный ресурс]. Режим доступа: https://www.so-ups.ru/news/press-release/press-release-view/news/17771/ (дата обращения: 16.06.2023).
3. СТО ПАО «Россети» Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110- 220 кВ и узловых цифровых подстанций напряжением 35 кВ.

4. Чичёв С. И., Калинин В. Ф., Глинкин Е. И. Методология проектирования цифровой подстанции в формате новых технологий. Москва: Издательский дом «Спектр», 2014, 228 с.
5. «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/ons_doc_LAW_150730/ (дата обращения: 18.06.2023).
6. «Приложение №1 к протоколу Правления ПАО «Россети». Концепция развития релейной защиты и автоматики электросетевого комплекса» [Электронный ресурс]. Режим доступа: https://www.rosseti.ru/upload/iblock/1da/2igrtje3suvjhgtjr8ubv5v7jauxqinl.pdf (дата обращения: 18.06.2023).
7. Осак А.Б., Бузина Е.Я. Влияние человеческого фактора при обеспечении кибербезопасности на надежность объектов электроэнергетики и живучесть электроэнергетических систем [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/vliyanie-chelovecheskogo-faktora-pri-obespechenii-kiberbezopasnosti-na-nadezhnost-obektov-elektroenergetiki-i-zhivuchest (дата обращения: 19.06.2023).
8. «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» ФСТЭК Приказ от 14 марта 2014 г. N31 [Электронный ресурс]. Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 20.06.2023).

References

1. Kolosok I.N., Korkina E.S. Cybersecurity Analysis of a Digital Substation from the Position of a Cyber-Physical System [Electronic resource]. Access mode: https://cyberleninka.ru/article/n/analiz-kiberbezopasnosti-tsifrovoy-podstantsii-s-pozitsiy-kiberfizicheskoy-sistemy (date of access: 06/16/2023).
2. "System Operator: Creation of the Unified Digital Model of the UES - the main result of the unification of information exchange in the electric power industry" [Electronic resource]. Access mode: https://www.so-ups.ru/news/press-release/press-release-view/news/17771/ (date of access: 06/16/2023).
3. STO PJSC "Rosseti" Digital supply center. Requirements for the technological design of digital substations with a voltage of 110-220 kV and nodal digital substations with a voltage of 35 kV.
4. Chichev S. I., Kalinin V. F., Glinkin E. I. Methodology for designing a digital substation in the format of new technologies. Moscow: Spektr Publishing House, 2014, 228 p.
5. "The main directions of state policy in the field of ensuring the safety of automated control systems for production and technological processes of critically important infrastructure facilities of the Russian Federation" [Electronic resource]. Access mode: https://www.consultant.ru/document/cons_doc_LAW_150730/ (date of access: 06/18/2023).

6. Appendix No. 1 to the minutes of the Management Board of PJSC Rosseti. The concept of development of relay protection and automation of the electric grid complex" [Electronic resource]. Access mode: https://www.rosseti.ru/upload/iblock/1da/2igrtje3suvjhgtjr8ubv5v7jauxqinl.pdf (date of access: 06/18/2023).
7. Osak A.B., Buzina E.Ya. The influence of the human factor in ensuring cybersecurity on the reliability of electric power facilities and the survivability of electric power systems [Electronic resource]. Access mode: https://cyberleninka.ru/article/n/vliyanie-chelovecheskogo-faktora-pri-obespechenii-kiberbezopasnosti-na-nadezhnost-obektov-elektroenergetiki-i-zhivuchest (date of access: 06/19/2023).
8. "On approval of the requirements for ensuring the protection of information in automated control systems for production and technological processes at critical facilities that pose an increased danger to human life and health and to the environment" FSTEC Order dated March 14, 2014 N31 [Electronic resource] . Access mode: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (date of access: 06/20/2023).