СПИСОК ЛИТЕРАТУРЫ

1. СТО 56947007-29.120.70.99-2011. Методические указания по выбору параметров срабатывания устройств РЗА подстанционного оборудования производства ООО НПП «ЭКРА». – ОАО «ФСК ЕЭС», 2011. – 216 с.
2. ЭКРА.656453.031 Р. Шкаф защиты трансформатора типа ШЭ2607 041. – ООО НПП «ЭКРА», 2020. – 179 с.

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ЦИФРОВЫХ ПОДСТАНЦИЙ

В.В. Ясунов

Томский политехнический университет, ИШЭ, ОЭЭ, группа 5А21

Научный руководитель: В.Е. Рудник, к.т.н., ассистент ОЭЭ ИШЭ ТПУ

Введение

В статье рассматривается проблема обеспечения кибербезопасности цифровых подстанций в условиях глобального технологического развития. Анализ включает в себя анализ и выделение видов цифровых подстанций, их сравнение, преимущества и недостатки реализации существующей архитектуры, а также меры по обеспечению кибербезопасности цифровых подстанций, включая использование современных технологий и методов защиты данных.

Объектом исследования служит цифровая электрическая подстанция.

Предметом исследования служит обеспечение кибербезопасности электрического оборудования на подстанции.

Статья представляет интерес для специалистов в области электроэнергетики, кибербезопасности и информационных технологий, а также для всех, кто интересуется проблемами обеспечения безопасности цифровых систем.

Основная часть

Согласно нормативным правовым актам федеральной сетевой компании (системный оператор) [1], цифровой подстанцией называется подстанция, в которой организация всех потоков информации при решении задач мониторинга, анализа и управления осуществляется в цифровой форме, а параметры такой передачи определяются единым файлом электронного проекта. В качестве основной среды передачи данных в рамках цифровой подстанции используется локальная вычислительная сеть (ЛВС) на базе технологии Ethernet, а в качестве коммуникационных протоколов применяются протоколы, описанные стандартом Международной электротехнической комиссии

Для цифровой постанции разработан стандарт по передачи цифровых сигналов международной энергетической компании МЭК 61850, имплементацию которого в России сделали такие компании, как «Россети», «Единый системный оператор». Выделяют три вида архитектуры цифровой подстанции [2]

Первый вид предполагает подключение устройств релейной защиты и автоматики, контроллеров присоединения, счетчиков электрической энергии в систему АСУ ТП (автоматизированная система управления технологическим процессом) по единому протоколу информационного обмена – MMS (Multimedia Messaging Service). При этом передача управляющих команд, сигналов между устройствами уровня присоединения, измерений и т. д. между устройствами осуществляется по контрольным медным кабелям, распространено название «условно цифровая», так как данный тип станции архитектурно не позволяет управлять с помощью электронно-вычислительных машин (ЭВМ) данной подстанцией, но позволяет снимать показания электроприборов и передавать их на ЭВМ для дальнейших принятий решений.

Второй тип предполагает также предполагает использование протокола MMS для передачи данных в систему АСУ ТП. Помимо этого, дискретные сигналы от устройств уровня присоединения к преобразователям дискретных сигналов, а также передача данных устройств уровня присоединения между собой осуществляется по протоколу GOOSE (Generic Object-Oriented Substation Event), который позволяет управлять устройствами релейной защиты и автоматики. Протокол служит для замены медных кабельных связей, предназначенных для передачи дискретных сигналов между устройствами. Под событиями в определении понимаются срабатывания и пуски устройств РЗА, изменения положения коммутационного оборудования и так далее. К данному виду предъявляются дополнительные требования по обеспечению безопасности – шкафы преобразователей дискретных сигналов, установленные в непосредственной близости от первичного оборудования.

Третий тип предполагает реализацию второго вида подстанций, однако данный вид подстанций с устройствами уровня присоединения должны выполняться в соответствии с протоколом SV (Sampled Values), который служит для получения значений от электротехнических устройств на подстанции.

Другими словами, существуют три типа цифровых станций, которые отличаются протоколами передачи данных. Первый тип – «условно цифровой» – предполагает подключение устройств релейной защиты и автоматики к АСУ ТП по единому протоколу MMS и передачу команд по контрольным медным кабелям. Второй тип использует протокол GOOSE для обмена данными между устройствами уровня присоединения, что позволяет управлять устройствами релейной защиты и автоматики без использования медных кабелей. Третий тип основан на втором и использует протокол SV для получения значений от электротехнических устройств. На рис. 1 схематично показаны отличия данных архитектур [3]

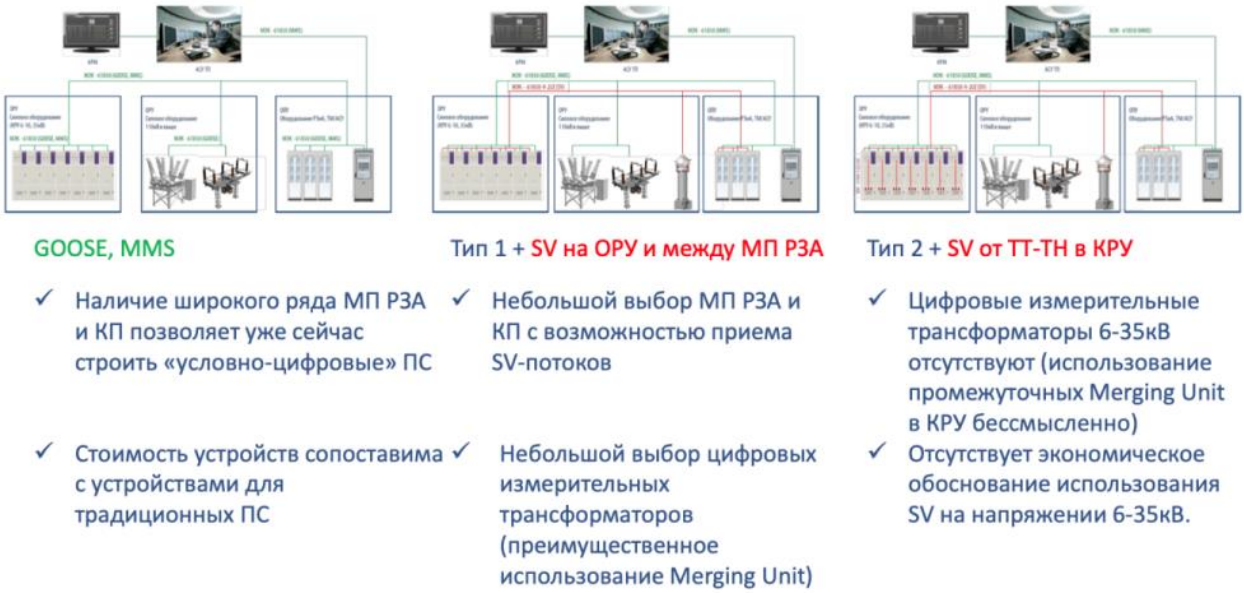

Рис. 1. Сравнение архитектур цифровых подстанций

Можно сказать, что цифровые подстанции позволяют снимать метрики с электроприборов, а также дистанционно управлять приборами управления, тем самым позволяя создать на основе данных цифрового двойника и использовать его на «цифровом полигоне» для тестирования и улучшения передачи и потребления электроэнергии. Такие преимущества несут такие риски, которые позволяют злоумышленникам получить доступ извне к локальной сети, что может привести к колоссальным потерям. Для предотвращения этого используются защитные протоколы, а также меры по предотвращению несанкционированного взлома.

Согласно оцениванию рисков реализации кибератак [4] наибольную угрозу для цифровых подстанций представляют заражение оборудование вредоностного обеспечения, несанкционированное уничтожение чувствительных данных, внедрение вредоносных программ для скрытого доступа к информационным ресурсам, однако в обзоре отсутствуют меры защиты от таких атак, поэтому необходимо дополнить материал.

Для обеспечения кибербезопасности [5] в области заражения оборудования следует использовать следующие практики: использование SIEM решений (Security Information and Event Management) – это комплексное решение для обеспечения информационной безопасности, которое объединяет управление информацией о безопасности (SIM) и управление событиями безопасности; использование антивирусных программ; ограничение доступа на установку программного обеспечения со стороны пользователя, а также предварительное тестирование на уязвимости программ до установки на промышленное оборудование.

В случае, когда идет речь об угрозе несанкционированного удаления чувствительных данных следует использовать следующие практики: использование системы резервирования данных, которые могут быть реализованы как использование готовых сервисов или запуск и наладка ЭВМ согласно рекомендациям ФСТЭК или ФСБ: SecaaS (Security as a service), Raid Массив, VPS; разделение архитектуры информационных сервисов предприятия на «микросервисы» с установлением сообщений между сервисами; ограничение пользователей ЭВМ на запись и чтение данных.

Бывают случаи, когда необходимо защита от внедрения вредоносных программ для скрытого доступа к информационным ресурсам. Для защиты необходимо придерживаться и использовать следующие практики: использование многоуровневой защиты, разделение ЭВМ сетей, разрешение доступа на чтение и запись по аутинфикации, использование отечественных операционных систем, адаптированных под промышленное оборудование, использование антивирусных программ

В заключение хотелось бы отметить, что в данной презентации проанализирована существующие угрозы и риски, связанные с цифровизацией электроэнергетической отрасли, а также предложение мер по повышению уровня защиты цифровых подстанций от кибератак для распространенных уязвимостей.

СПИСОК ЛИТЕРАТУРЫ

1. СТО 56947007-29.240.10.299-2020. – Россети: [сайт]. – URL: https:// www.rosseti.ru/upload/iblock/545/t0vad6zka3qcfwt4dqjpv1v3ubtqaffw.pdf?ysclid=m3buddaiwj970753695 (дата обращения: 10.11.2024).
2. Практическая реализация требований серии стандартов МЭК 61850 на энергетических объектах России / В.В. Никитин, Т.Б. Эзирбаев, А.С. Варавин, Р.А.М. Магомадов // Грозненский естественнонаучный бюллетень. – 2022. – Т. 7, № 2(28). – С. 118–127. – DOI 10.25744/genb.2022.92.42.013. – EDN DGLNKN.
3. Презентация: Требования предъявляемые к оборудованию подстанций работающему в составе Цифровых ПС. [Электронный ресурс] // Digital Substation : [сайт]. – URL: https:// digitalsubstation.com/wp-content/uploads/2018/12/10-Slesarchuk-Trebovaniya-k-oborud-TSPS-LEP.pdf (дата обращения: 12.11.2024).
4. Карпенко В.Г. Карантаев В.И. Разработка экспертной системы для оценки влияния деструктивных воздействий компьютерных атак на подстанции с высшим классом напряжения 500 кВ с децентрализованной архитектурой вторичных подсистемр // Современные тенденции развития цифровых систем релейной защиты и автоматики: Материалы науч.-техн. конф. Чебоксары. – 2021. – № 1. – С. 186–199.
5. Не тушите свет: как защитить АСУ ТП от атак с Industroyer и подобным ВПО / [Электронный ресурс]. – URL: https:// SecurityLab.ru : [сайт]. – URL: https:// www.securitylab.ru/analytics/516258.php?ysclid=m3dzk902hg602351283 (дата обращения: 12.11.2024).