УДК 621

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ ЦИФРОВЫХ ПОДСТАНЦИЙ

Алексеев Ф.В.[1], студент гр. АУСм-1-24, I курс
Научный руководитель: Гатауллин А.М.[1], к.т.н., доцент
[1]Казанский государственный энергетический университет
г. Казань

В последнее время в России реализуется концепция интеллектуальной энергосистемы, в состав которой входит идеология, основные технологии и механизмы развития интеллектуальной ЭЭС, а также иерархия управления Единой энергетической системой (ЕЭС)[1]. В данной работе будет уделено внимание цифровой подстанции как элементу нового поколения, в котором используются цифровые устройства защиты и управления [2].

Подстанции позволяют управлять системой распределения и потоком электрической энергии. В состав основных функций входит сбор и передача данных с основного оборудования, контроль управления, релейная защита и автоматизированная система управления технологическими процессами, а также учет электрической энергии и мощности.

Подстанции играют ключевую роль в энергосистеме, что делает их кибербезопасность одним из обязательных приоритетов. Недостаточная квалификация рабочего персонала создает значительную уязвимость. Так, сотрудники, имеющие доступ и базовые навыки работы с терминалами релейной защиты, могут получить несанкционированный контроль над оборудованием и данными, изменив при этом его настройки. Использование сетей общего пользования, в состав которых входит GSM, Интернет, значительно повышает риск подобных атак, осуществляемых через интерфейс «Человек-машина» [3].

В прошлом, безопасность подстанций обеспечивалась их изоляцией, надежной внутренней инфраструктурой связи и закрытыми протоколами. Переход к «цифровой» энергетике, с применением интеллектуальных систем и сложного оборудования, привел к резкому росту киберугроз, особенно для цифровых подстанций.

Цифровые подстанции, работающие на основе автоматизированного управления и цифрового обмена данными по протоколам IEC 61850 через Ethernet, уязвимы к кибератакам. Шины процесса и подстанции создают дополнительные возможности для злоумышленников. Это включает в себя вторжение в процессы реального времени и нарушение синхронизации, расширяя при этом спектр угроз, по сравнению с «традиционными» подстанциями.

Для эффективной защиты цифровых подстанций необходимо разработать системы, обладающие стабильностью, адаптивностью и восстанавливаемостью, что в свою очередь требует всестороннего анализа уязвимостей кибербезопасности.

В данной статье представлен подход к анализу устойчивости цифровых подстанций к кибератакам и их способности к восстановлению после успешных атак, основанный на использовании дерева угроз и атак. Рассматриваются конкретные кибератаки, их последствия для функционирования цифровых подстанций, а также предлагаются соответствующие меры защиты.

Особое внимание уделяется архитектуре управления Единой энергетической системой, которая организована иерархически, с участием региональных, межрегиональных и центрального диспетчерских центров. [4]

Системы SCADA, обеспечивающие связь диспетчерских центров с объектами энергетики, является критически важным элементом, но часто содержит уязвимости. устанавливаются в автоматизированные системы управления всей системой диспетчеризации и соединяют центры управления с подсистемами. В состав оборудования SCADA входят рабочие станции, серверы, коммуникационные процессоры и каналы связи. «Традиционные» протоколы связи, используемые в SCADA, часто не обеспечивают достаточной защиты от злонамеренного вторжения в корпоративную сеть, что создает уязвимость при доступе к локальной сети подстанции. Отсутствие или неправильная настройка брандмауэра на входе в локальную сеть облегчает проникновение вредоносного ПО, что может привести к нарушению или прекращению работы информационной системы подстанции. Повысить уровень кибербезопасности можно путем создания защищенной периметральной сети с системой обнаружения вторжений и брандмауэром. В этой сети серверы обмениваются данными с внешней сетью, а брандмауэр контролирует трафик, позволяя внешней сети получать только запрошенные данные.

Подстанции различаются по структуре, уровню автоматизации и безопасности. Несмотря на различия, большинство из них подвержены схожим киберугрозам. К наиболее опасным относятся DoS-атаки, внедрение вредоносного ПО, подмена сигналов GPS/SV/MMS/GOOSE и переполнение трафика, которые могут напрямую повлиять на работоспособность цифровой подстанции.

Для разработки эффективных мер защиты от потенциальных кибератак необходимо сначала выявить слабые места и уязвимости на территории подстанции, а также определить возможные угрозы кибербезопасности. Для этой цели в данной статье применяется технология дерева неисправностей, хорошо зарекомендовавшая себя в теории надежности сложных технических систем.[5] Данный метод, первоначально использовавшийся в системах военной авиации, а затем в атомной энергетике и других отраслях промышленности, позволяет систематически анализировать причины и

последствия сбоев и отказов.[6] Грамотно построенное дерево атак позволяет существенно снизить уровень уязвимостей и рисков.[7] Для анализа кибербезопасности цифровой подстанции было построено дерево угроз и атак (рис.1), наглядно демонстрирующее уязвимости и возможные сценарии кибератак.

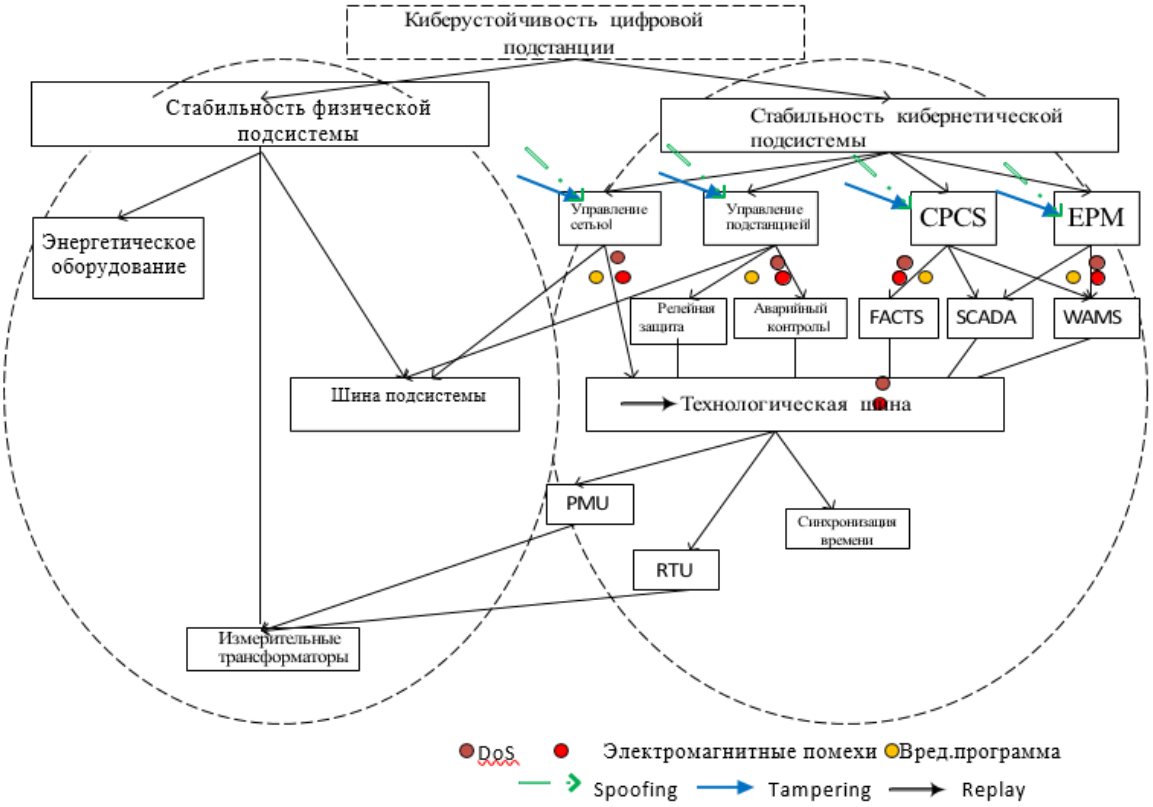

Рис.1. Дерево угроз и атак цифровой подстанции

Индивидуальное дерево угроз и атак, разработанное для каждой цифровой подстанции, представляет собой мощный инструмент для анализа и планирования защиты. Оно позволяет выявить уязвимости в информационно-коммуникационных системах, оценить эффективность текущих мер кибербезопасности и определить направление для дальнейшего усиления защиты конкретного энергообъекта. [8]

Проанализировав данное дерево, можно сделать вывод, что киберустойчивость цифровых подстанций обеспечивается не только техническими и организационными мерами, но и использованием статистических методов обработки измерительной информации. Сочетание этих подходов позволяет минимизировать риски ошибок в управлении энергосистемой во время кибератак.[9]

В дальнейшем планируется внедрить на уровне подстанции алгоритмы обобщенной оценки состояния [10,11], которые будут анализировать как рабочие параметры, так и состояние оборудования связи. Это станет возможным благодаря тому, что измерения – как логические, к которым относятся телесигналы, так и аналоговые (телеметрия), выполняются

синхронно, собираются в единую систему в одном месте и оцифровываются с использованием стандартных протоколов. Технологическая шина и шина подстанции обеспечивают доступ к обширному объему измерительной информации, регистрируемой на подстанции, что позволит существенно повысить эффективность оценки состояния.

Также нерешенными остаются проблемы безопасной передачи, хранения и обработки диагностической информации состояния изоляции силовых трансформаторов [12], других типов изоляторов [13]. Для цифровых подстанций важно передавать диагностическую информацию в режиме мониторинга [14], что является причиной увеличения интенсивности трафика и, как следствие, роста вероятности успешных кибератак. Эта проблема наиболее актуальна в связи с применением информационно емких датчиков УВЧ диапазона электромагнитного излучения [15] для мониторинга состояния изоляторов воздушных линий электропередачи [16], изоляции кабелей [17] умных сетей.

Реализация вычислительных алгоритмов локальной обобщенной оценки состояния непосредственно на уровне подстанции позволит существенно повысить качество проверки телесигналов, отражающих состояние элементов сети, и данных телеметрии. Это, в свою очередь, минимизирует риски ошибок в управлении энергосистемой, возникающих из-за искажения измерительной информации на цифровой подстанции в результате кибератак.

В последнее время угроза кибератак, направленных на вредоносное вторжение в информационные системы, становится все более актуальной для электроэнергетики и других отраслей, где информационные ресурсы используются для управления производственными процессами. В связи с этим, применение простых в реализации, но эффективных инструментов для анализа и предотвращения киберугроз становится жизненно необходимым. Одним из таких инструментов является дерево угроз и атак, разработанное на основе технологии анализа дерева неисправностей, используемой в теории надежности сложных технических систем.

Предлагаемое дерево угроз и атак охватывает все ключевые компоненты информационно-технологической системы управления цифровыми подстанциями. Наглядная древовидная структура позволяет легко идентифицировать наиболее вероятные уязвимости. Для каждой уязвимости определены потенциальные киберугрозы и атаки, а также разработаны соответствующие меры противодействия, направленные на предотвращение атак или минимизацию их последствий для работоспособности подстанции.

Список литературы:

1. Фортов В. И Макаров А. (2012). Концепция интеллектуальной энергетической системы России с активно-адаптивной сетью. Московское АО »НТЦ ФСК ЕЭС". 235 с.
2. А. Епифанов. Мы видим большой потенциал в цифровых подстанциях. Электричество // Передача и распределение. № 1 (34), 2016 , с. 6-9.
3. Алымов И.С. Проблемы информационной безопасности подстанции и пути их решения / И.С. Алымов//Цифровая подстанция [электронный ресурс] – 2016. – Режим доступа: http://digitalsubstation.com/blog/2016/02/17/problemy - информационной-безопасности-установки-и-возможности-их-решения/
4. Определение DSP и приоритетных технологий DSP // Цифровая подстанция. № 9, 2018, с. 10-20.
5. Ю.Б. Гук. Расчет надежности энергообъекта. (Ленинград.: ЭнергоАтомИздат, 1988. – 224 с.
6. Эриксон К.А. Анализ дерева неисправностей – Режим доступа: http://www.eecs.ucf.edu/~hlugo/cop4331/ericson-fta- tutorial.pdf
7. Колосок И., Коркина Е., Тихонов А. Анализ надежности программного обеспечения для оценки состояния на базе SCADA и WAMS // Исследование энергетических систем, Том 1, № 1 (2018): с.100- 107.
8. Видьяшри Нагараджу, Лэнс Фионделла и Тьерри Ванджи. Обзор моделирования и анализа дерева ошибок и атак для управления киберрисками. Международный симпозиум по технологиям для национальной безопасности. IEEE, 2017.
9. Колосок И.Н., Коркина Е.С. Роль государственной оценки в обеспечении киберфизической безопасности электроэнергетической системы.// Материалы 88-й междунар. науч.-практ. конф. Научный семинар по методологическим проблемам исследования надежности крупных энергетических систем, 2014, выпуск 67, Сыктывкар: Коми НЦ УРО РАН, 2016, с. 386-395.
10. Г.Н. Коррес, П.Дж. Кацикас, Г.Э. Чатзаракис. “Идентификация ошибок аналоговых и топологических измерений при оценке обобщенного состояния”, Journal of Materials Processing Technology, том 161, стр. 121-127, 2005.
11. А. Симоес Коста, Э.М. Лоренко, Л. Кользани. “Определение зоны пониженной аномалии для обработки ошибок топологии при оценке обобщенного состояния”, Труды конференции IEEE Power Tech conference, Лозанна, стр. 137-142, 2007.
12. Гатауллин А.М., Матухин В.Л., Наумов Б.А. СИСТЕМА МОНИТОРИНГА И ДИАГНОСТИРОВАНИЯ (СМИД) ВЫСОКОВОЛЬТНОГО ЭЛЕКТРООБОРУДОВАНИЯ НА ОСНОВЕ АНАЛИЗА СТАТИСТИЧЕСКИХ ПАРАМЕТРОВ ЧАСТИЧНЫХ РАЗРЯДОВ.

Известия высших учебных заведений. Проблемы энергетики. 2013. № 7-8. С. 19-26.

13. Gataullin A.M. HIGH VOLTAGE ELECTRICAL INSULATORS DIAGNOSTICS BY PARTIAL DISCHARGES CHARACTERISTICS. В сборнике: Proceedings - 2020 International Ural Conference on Electrical Power Engineering, UralCon 2020. 2020. С. 426-430.

14. Gataullin A.M. ONLINE MONITORING OF THE PORCELAIN INSULATOR UNITS STATE. В сборнике: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. 2020. С. 9271631.

15. Gataullin A.M. DEVELOPMENT OF METHOD FOR HIGH-VOLTAGE ELECTRICAL EQUIPMENT INSULATORS MONITORING IN UHF RANGE OF ELECTROMAGNETIC RADIATION. В сборнике: Proceedings - 2020 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2020. 2020. С. 9112023.

16. Гатауллин А.М. НЕРАЗРУШАЮЩИЙ МЕТОД ДИАГНОСТИКИ ФАРФОРОВЫХ ИЗОЛЯТОРОВ ВОЗДУШНЫХ ЛИНИЙ ЭЛЕКТРОПЕРЕДАЧИ 6/10 КВ. Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. 2015. № 4 (231). С. 82-90.

17. Gataullin A.M. ONLINE TECHNOLOGY OF INSULATORS CONDITION MONITORING IN SMART GRID POWER SUPPLY SYSTEMS. В сборнике: 2019 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2019. 2019. С. 8934770.