РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 850 734**(13) **C1**

(51) МПК
G06F 11/07 (2006.01)
H02J 13/00 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 11/0703 (2025.08); H02J 13/00034 (2025.08)

(21)(22) Заявка: **2025112729, 15.05.2025**

(24) Дата начала отсчета срока действия патента:
15.05.2025

Дата регистрации:
13.11.2025

Приоритет(ы):
(22) Дата подачи заявки: **15.05.2025**

(45) Опубликовано: **13.11.2025** Бюл. № **32**

Адрес для переписки:
603155, г. Нижний Новгород, ул. Минина, 24, ОИСиВД НГТУ, Отдел интеллектуальной собственности и выставочной деятельности

(72) Автор(ы):
Куликов Александр Леонидович (RU),
Лоскутов Антон Алексеевич (RU),
Карантаев Владимир Геннадьевич (RU)

(73) Патентообладатель(и):
Федеральное государственное бюджетное образовательное учреждение высшего образования "Нижегородский государственный технический университет им. Р.Е. Алексеева" (НГТУ) (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2727525 C1, 22.07.2020. RU 2798437 C1, 22.06.2023. US 20190006837 A1, 03.01.2019. US 20190334932 A1, 31.10.2019. US 20200358283 A1, 12.11.2020.**

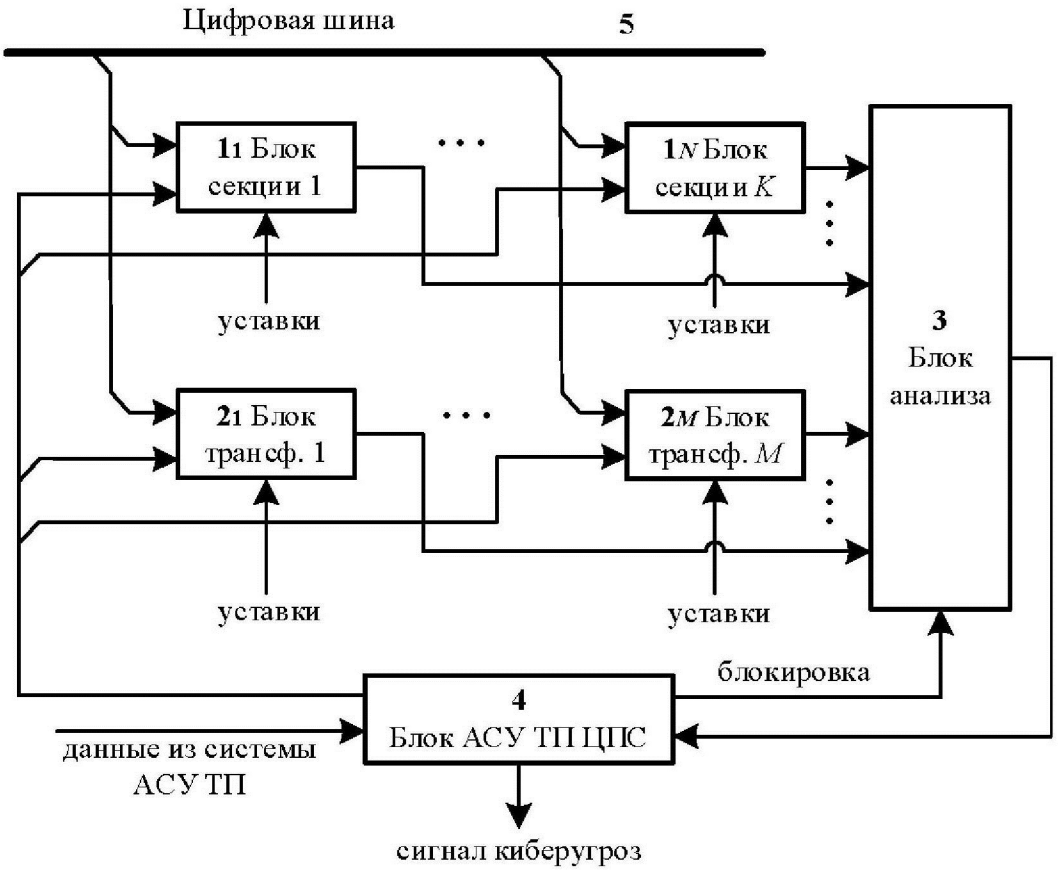
(54) Способ выявления киберугроз цифровых подстанций

(57) Реферат:

Изобретение относится к электротехнике. Технический результат заключается в обеспечении выявления киберугрозы на цифровых подстанциях. Указанный результат достигается благодаря способу выявления киберугроз цифровых подстанций, заключающемуся в том, что подстанцию разделяют на силовые узлы, измеряют фазные токи присоединений и напряжения, передают данные по цифровой шине; контролируют исправность трансформаторов тока, суммируют пофазно токи всех присоединений каждого узла с учетом направления; фиксируют случаи, когда трансформаторы исправны и сумма токов узла равна нулю, что означает отсутствие угроз; также фиксируют случаи, когда трансформаторы исправны, но сумма токов не равна нулю, превышает порог, а скорость изменения токов выше скорости переходных процессов при повреждениях, что характеризует киберугрозы, к которым также относят и наличие данных о токах при отсутствии напряжения на узле; сигнал о киберугрозе выдают в АСУ ТП, но блокируют при информации об ошибках персонала, повреждениях оборудования или включении узлов в работу; связи блоков устройства выполняют отдельно от цифровой шины. 1 ил., 1 табл.

RU 2850734 C1

RU 2850734 C1



Фиг. 1

RU 2850734 C1

RU 2850734 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 850 734**(13) **C1**

(51) Int. Cl.
G06F 11/07 (2006.01)
H02J 13/00 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 11/0703 (2025.08); H02J 13/00034 (2025.08)

(21)(22) Application: **2025112729, 15.05.2025**

(24) Effective date for property rights:
15.05.2025

Registration date:
13.11.2025

Priority:
(22) Date of filing: **15.05.2025**

(45) Date of publication: **13.11.2025** Bull. № **32**

Mail address:
603155, g. Nizhnij Novgorod, ul. Minina, 24, OISiVD NGTU, Otdel intellektualnoj sobstvennosti i vystavochnoj deyatelnosti

(72) Inventor(s):
Kulikov Aleksandr Leonidovich (RU),
Loskutov Anton Alekseevich (RU),
Karantaev Vladimir Gennadevich (RU)

(73) Proprietor(s):
federalnoe gosudarstvennoe biudzhetnoe obrazovatelnoe uchrezhdenie vysshego obrazovaniia "Nizhegorodskii gosudarstvennyi tekhnicheskii universitet im. R.E. Alekseeva" (NGTU) (RU)

(54) METHOD FOR DETECTING CYBER THREATS TO DIGITAL SUBSTATIONS

(57) Abstract:

FIELD: electrical engineering.

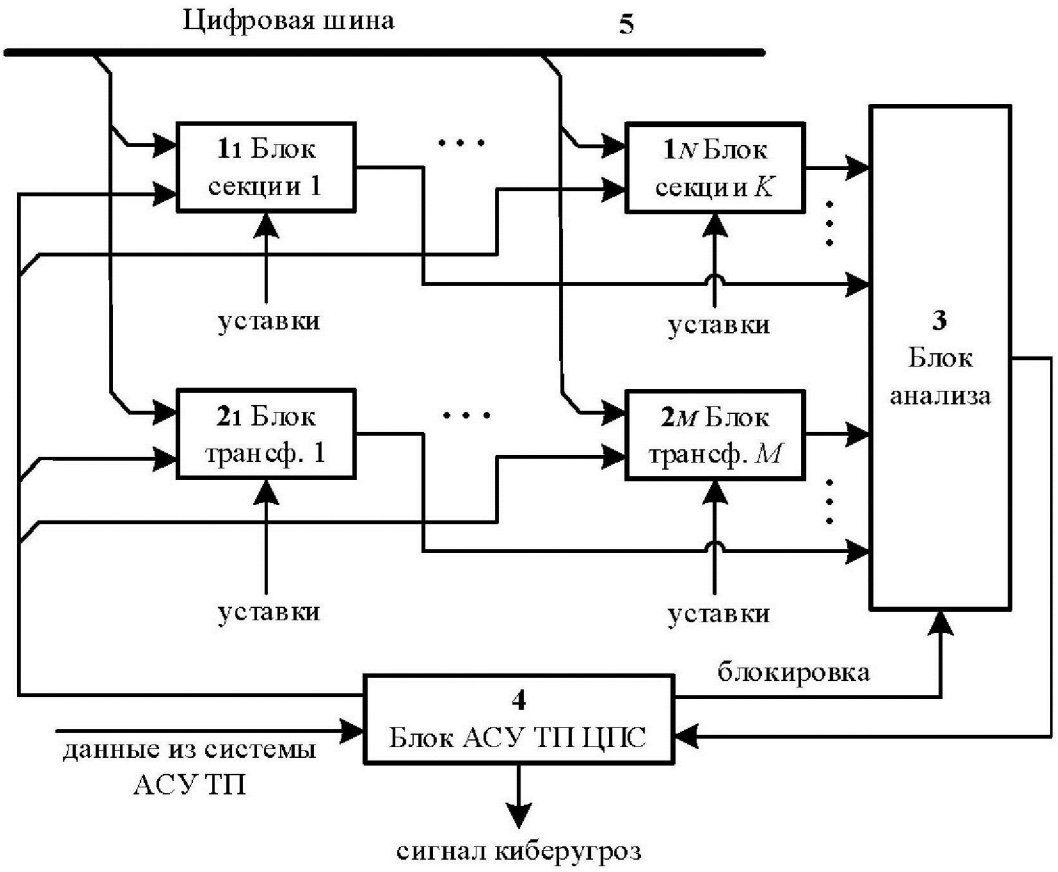
SUBSTANCE: specified result is achieved thanks to a method for detecting cyber threats to digital substations, which consists of dividing the substation into power nodes, measuring the phase currents of connections and voltages, and transmitting data via a digital bus; current transformers are checked for serviceability, the currents of all connections of each node are summed up phase by phase, taking into account the direction; cases are recorded when the transformers are serviceable and the sum of the node currents is zero, which means there are no threats; also record cases when transformers are operational, but the sum of currents is not zero, exceeds the threshold, and the rate of change of currents is higher than the rate of transient processes in case of damage, which characterises cyber threats, which also include the presence of data on currents in the absence of voltage at the node; a cyber threat signal is sent to the automated control system, but is blocked when information about personnel errors, equipment damage or the activation of nodes is received; the device's block connections are separate from the digital bus.

EFFECT: ensuring the detection of cyber threats at digital substations.

1 cl, 1 dwg, 1 tbl

RU 2850734 C1

RU 2850734 C1



Фиг. 1

RU 2850734 C1

RU 2850734 C1

Изобретение относится к электротехнике, в частности к способам выявления киберугроз цифровых подстанций.

Известен программно-аппаратный комплекс системы поддержки принятия решений по управлению подсистемой релейной защиты и автоматики цифровой подстанции в условиях проведения в отношении нее компьютерных атак [Патент РФ на изобретение №2798437, МПК G06F 17/40, опубл. 22.06.2023, бюл. № 18]. Программно-аппаратный комплекс содержит взаимодействующие между собой модуль «интерфейс инженера знаний», модуль «интерфейс получения данных из внешней базы знаний», модуль «редактор баз знаний», модуль «база экспертных данных», модуль «система управления базой знаний», модуль «база знаний для распознавания ситуации», модуль «база знаний для формирования рекомендаций», модуль «машина логического вывода», модуль «расчет надежности», модуль «распознавание ситуации и подготовка рекомендаций», модуль «подсистема объяснений», модуль «лингвистический процессор», модуль «база данных с информацией от внешних систем», модуль «интерфейс приема данных от системы обеспечения информационной безопасности СОИБ», модуль «интерфейс пользователя», модуль «интерфейс обмена данными с АСУ ТП», модуль «подготовка и обработка журналов логирования», модуль «база данных для хранения журналов», модуль «интерфейс обмена данными с системой оперативных журналов ОЖУР».

Программно-аппаратный комплекс системы поддержки принятия решений по управлению подсистемой релейной защиты и автоматики цифровой подстанции обеспечивает возможность получения стационарного коэффициента готовности интеллектуального электронного устройства (ИЭУ) релейной защиты и автоматики (РЗА) цифровой подстанции (ЦПС) с учетом многофакторного анализа, что позволяет оценить вероятность застать ИЭУ РЗА ЦПС в работоспособном состоянии в произвольный момент времени, оценить надежность ИЭУ РЗА в определенных условиях, а также повысить качество оперативно-технологического управления подсистемой РЗА ЦПС при проведении в отношении нее компьютерных атак.

Способ реализуется в системе поддержки принятия решений (СППР), которая развертывается в центрах управления электрическими сетями (ЦУС), и не позволяет выявлять киберугрозы на цифровых подстанциях, поскольку программно-аппаратный комплекс позволяет лишь оценивать усредненный вероятностный показатель стационарного коэффициента готовности ИЭУ РЗА ЦПС.

Известен способ мониторинга, защиты и управления оборудованием электрической подстанции [Патент РФ на изобретение №2727525, МПК H02J 13/00, опубл. 22.07.2020, бюл. № 21], заключающийся в том, что организуют локальную вычислительную сеть путем соединения интеллектуальных электронных устройств, сетевых коммутаторов, компьютеров и другого оборудования электрической подстанции, имеющего сетевые интерфейсы, выполняют фиксацию параметров состояния оборудования электрической подстанции, проводят передачу и прием информационных пакетов данных о параметрах состояния оборудования, выполняют анализ параметров состояния оборудования, осуществляют выработку сигналов управляющих воздействий.

Согласно предложению токи и напряжения измеряют при помощи цифровых трансформаторов, снабженных резистивными, емкостными или резистивно-емкостными делителями напряжения, малогабаритными трансформаторами тока, катушками Роговского, первичными преобразователями постоянного тока и датчиками диагностики технического состояния, в измерительно-коммуникационных блоках цифровых трансформаторов выполняют фильтрацию и нормирование сигналов первичных преобразователей тока и напряжения, аналого-цифровое преобразование сигналов

первичных преобразователей тока и напряжения, первичную обработку оцифрованных сигналов, выполняют диагностику первичных преобразователей тока и напряжения и измерительно-коммуникационного блока, определяют действующие значения токов и напряжений, углов между ними, активную, реактивную и полную мощности, мощность искажений и соответствующие указанным мощностям энергии, определяют показатели качества электрической энергии, выполняют алгоритмы релейной защиты и автоматики, формируют кадры данных с мгновенными значениями тока и напряжения и отправляют указанные кадры данных смежным интеллектуальным электронным устройствам через сетевые интерфейсы, формируют пакеты данных с диагностической информацией, пакеты данных с действующими значениями тока и напряжения, угла между ними, активной, реактивной и полной мощностями, мощностью искажений и соответствующие указанным мощностям энергии, пакеты данных с показателями качества электрической энергии и отправляют указанные пакеты данных автоматизированной системе управления технологическими процессами, при действии защиты вырабатывают цифровые сигналы управляющих воздействий, выполняют преобразование данных сигналов в дискретные, формируют управляющие воздействия посредством выходных реле и одновременно формируют кадры данных с управляющими воздействиями, отправляют кадры данных с управляющими воздействиями смежным интеллектуальным электронным устройствам, и записывают в файл данных мгновенные значения тока и напряжения, затем формируют записи в журнал диагностики при возникновении неисправностей и других диагностических событий, записи в журнал учета электрической энергии в непрерывном режиме, записи в журнал показателей качества электрической энергии в непрерывном режиме и при наступлении соответствующих событий, записи в журнал релейной защиты и автоматики при действии защиты, при этом файлы данных, журналы и текущие данные диагностики, учета электрической энергии, показатели качества электрической энергии передают по запросам автоматизированной системы управления технологическими процессами.

Способ направлен на создание системы мониторинга, защиты и управления оборудованием электрической подстанции, обеспечивающим повышение надежности и быстродействия релейной защиты и автоматики, обеспечивающем надежную работу системы учета и определения показателей качества электрической энергии, упрощение эксплуатации электрических подстанций.

Однако известный способ не позволяет выявлять киберугрозы на цифровых подстанциях.

Наиболее близким техническим решением является способ релейной защиты и управления электрической подстанции [Патент РФ на изобретение №2727525, МПК H02J 13/00, опубл. 22.07.2020, бюл. № 21], заключающийся в том, что измеряют фазные токи всех присоединений силовых узлов подстанции и измеряют напряжения на этих узлах, передают в цифровом виде измеренные токи и напряжения по цифровой шине, управляют оборудованием подстанции путем реализации централизованных применительно к подстанции алгоритмов мониторинга, защиты и управления.

Согласно предложения электрическую подстанцию условно разделяют на силовые узлы, в каждом из которых соединяются несколько электрических присоединений, контролируют исправность всех датчиков сигналов и устройств управления присоединений каждого силового узла подстанции, регистрируют токи и напряжения, суммируют пофазно фазные токи, с учетом их направления, всех присоединений каждого силового узла подстанции, если все датчики и устройства управления присоединений силового узла исправны и сумма токов, с учетом их направления, всех присоединений

силового узла подстанции равна нулю, то управляют каждым присоединением силового узла подстанции путем реализации локальных применительно к присоединению алгоритмов мониторинга, защиты и управления, если выявлена неисправность датчика или устройства управления присоединения силового узла подстанции, то ток этого присоединения определяется косвенным способом, как сумма токов других присоединений с обратным знаком, и прекращают управлять этим присоединением силового узла подстанции путем реализации локальных применительно к присоединению алгоритмов мониторинга, защиты и управления, вместо этого управляют этим присоединением силового узла подстанции путем реализации централизованных применительно к силовому узлу подстанции алгоритмов мониторинга, защиты и управления с параметрами, соответствующими параметрам срабатывания локальных применительно к присоединению алгоритмов мониторинга, защиты и управления, если же все датчики и устройства управления присоединений силового узла исправны, но сумма токов, с учетом их направления, всех присоединений силового узла подстанции не равна нулю и превышает пороговое значение, то принимают решение, что повреждение произошло непосредственно в силовом узле подстанции и отключают этот узел с помощью выключателя присоединения, по которому осуществляется питание этого силового узла подстанции.

Хотя способ-прототип обеспечивает повышение надежности работы релейной защиты и управления за счет комбинированного централизованного и локального управления и косвенных измерений, но он не позволяет выявлять киберугрозы на цифровых подстанциях.

Задача изобретения состоит в разработке способа, позволяющего выявлять киберугрозы на цифровых подстанциях.

Поставленная задача достигается способом выявления киберугроз цифровых подстанций, заключающимся в том, что электрическую подстанцию условно разделяют на силовые узлы, в каждом из которых соединяются несколько электрических присоединений, измеряют фазные токи всех присоединений силовых узлов подстанции и измеряют напряжения на этих узлах, передают в цифровом виде измеренные токи и напряжения по цифровой шине, контролируют исправность всех трансформаторов тока, регистрируют токи и напряжения, суммируют пофазно фазные токи, с учетом их направления, всех присоединений каждого силового узла подстанции, фиксируют случаи, когда все трансформаторы тока присоединений силового узла исправны и сумма токов, с учетом их направления, всех присоединений силового узла подстанции равна нулю, также фиксируют случаи, когда трансформаторы тока присоединений силового узла исправны, но сумма токов, с учетом их направления, всех присоединений силового узла подстанции не равна нулю и превышает пороговое значение.

Согласно предложению контролируют состояние вторичных цепей трансформаторов тока с использованием токов обратной и нулевой последовательностей, контролируют скорость изменения измеренных токов присоединений силового узла для выявления отличий кибератак на цифровую подстанцию от повреждений и переключений в прилегающей к цифровой подстанции электрической сети, случаи, когда все трансформаторы тока присоединений любого силового узла исправны и сумма токов, с учетом их направления, всех присоединений силового узла подстанции равна нулю считают случаями с отсутствием киберугроз цифровой подстанции, а случаи, когда трансформаторы тока присоединений любого силового узла исправны, но сумма токов, с учетом их направления, всех присоединений силового узла подстанции не равна нулю, превышает пороговое значение и дополнительно скорость изменения токов

присоединения выше скорости протекания переходных процессов при повреждениях и переключениях в электрической сети, считают случаями, характеризующими киберугрозы цифровой подстанции, к таким случаям также относят факты наличия данных о ненулевых измеренных токах присоединений, поступающих из цифровой шины подстанции, в условиях отсутствия напряжения на силовом узле, выдают сигнал, характеризующий киберугрозы, с выхода устройства, реализующего способ выявления киберугроз цифровых подстанций, на вход автоматизированной системы управления технологическими процессами цифровой подстанции, блокируют выдачу сигнала, характеризующего киберугрозы, с выхода устройства при наличии информации в автоматизированной системе управления технологическими процессами цифровой подстанции об ошибочных действиях оперативного и эксплуатационного персонала, повреждениях силовых узлов подстанции, насыщении трансформаторов тока их присоединений, повреждениях во вторичных цепях измерительных трансформаторов напряжения силовых узлов, а также о включении в работу силовых узлов подстанции, дополнительно связи блоков, входящих в состав устройства, выполняют отдельно от цифровой шины подстанции для предотвращения искажений передаваемых сигналов в условиях кибератак.

На фиг. 1 приведен пример устройства, реализующего способ выявления киберугроз цифровых подстанций.

Устройство (фиг. 1) содержит: блоки контроля секций шин $1_1 \ldots 1_K$; блоки контроля трансформаторов $2_1 \ldots 2_M$; блок анализа 3; блок автоматизированной системы управления технологическими процессами (АСУ ТП) цифровой подстанции (ЦПС) 4; цифровую шину 5.

Способ выявления киберугроз цифровых подстанций реализуется следующим образом.

Способ обеспечивает выявление киберугроз цифровых подстанций, связанных с подменой измерений токов и напряжений, а также реализуемых путем кибератак на цифровую шину подстанции (специализированную локальную вычислительную сеть), или датчики измерений и устройства обработки токов и напряжений. При этом для выявления киберугроз измеренные значения токов и напряжений контролируются на цифровой шине ЦПС, а также используются данные поступающие из системы АСУ ТП ЦПС через блок 4. Следует отметить, что за счет выполнения связей блоков устройства (фиг. 1) отдельно и независимо от цифровой шины 5 обеспечивается функционирование устройства в условиях кибератак на цифровую шину 5.

Пример устройства (фиг. 1), реализующего способ, выполняет контроль силовых узлов ЦПС для выявления кибератак. В состав устройства входят блоки контроля секций шин ЦПС $1_1 \ldots 1_K$ и блоки контроля трансформаторов (автотрансформаторов) $2_1 \ldots 2_M$. Однако в состав ЦПС могут входить и другие силовые узлы (например, устройства продольной компенсации, вставки постоянного тока и другие), но принципы реализации способа выявления киберугроз цифровых подстанций, а также совокупность операций контроля остается такой же, как в устройстве (фиг. 1), требуется лишь дополнение устройства (фиг. 1) соответствующими блоками контроля.

Контроль исправности измерительных цепей напряжения силовых узлов ЦПС осуществляется устройством релейной защиты ЦПС [Шнеерсон Э.М. Цифровая релейная защита. – М.: Энергоатомиздат, 2007, с. 476-479]. При неисправности измерительных цепей напряжения сигналы от устройств релейной защиты через систему АСУ ТП ЦПС и блок 4 поступают на входы блоков $1_1 \ldots 1_K$ и $2_1 \ldots 2_M$ в соответствии с

принадлежностью устройства релейной зашиты силовому узлу.

При использовании на цифровой шине ЦПС группы протоколов МЭК 61850 присоединение и передача мгновенных значений токов и напряжений от соответствующих датчиков осуществляется подпиской блоков контроля $1_1 \ldots 1_K$ и $2_1 \ldots 2_M$ на требуемые SV-потоки в соответствии со стандартом МЭК 61850-9.2.

Перед началом функционирования устройства в блоки контроля $1_1 \ldots 1_K$ и $2_1 \ldots 2_M$ заносятся уставочные (пороговые) значения, необходимые для контроля токов силовых узлов и соответствующие небалансам токов.

Функционирование устройства (фиг. 1), реализующего способ выявления киберугроз ЦПС, основано на использовании измеренных значений токов и напряжений на присоединениях силовых узлов. Программное обеспечение устройства (фиг. 1) включает специальные алгоритмы контроля технологических процессов на подстанции (контроля подмены измерений), которые в совокупности образуют систему выявления киберугроз. Алгоритмы основаны прежде всего на контроле соответствия информации о процессах, происходящих на подстанции и передающейся по локальной вычислительной сети (цифровой шине 5), известным законам физики и электротехники.

Алгоритмы устройства (фиг. 1) реализуют следующие функции диагностики:

– контроль уровня токов небаланса на секциях шин подстанции;

– контроль уровня тока небаланса силового трансформатора;

– контроль состояния вторичных цепей трансформаторов тока с использованием метода симметричных составляющих;

– контроль скорости изменения токов при изменении конфигурации сети.

Контроль уровня токов небаланса на секциях шин подстанции

В основе алгоритма контроля уровня токов небаланса на шинах ЦПС лежит анализ информации о входных и выходных токах шины. По первому закону Кирхгофа геометрическая сумма токов в узле должна быть равна нулю. Тогда, отклонение геометрической суммы от нуля на величину, большую, чем определенный порог (уставка), учитывающий погрешности средств измерения, может свидетельствовать о наличии повреждения на шинах ЦПС. Если, к примеру, повреждения на шине ЦПС отсутствуют, а значение геометрической суммы токов больше параметра (порога) срабатывания, то алгоритм сигнализирует о возможном стороннем вмешательстве в работу оборудования ЦПС на уровне локальной вычислительной сети (цифровой шины 5).

Параметром срабатывания выступает модуль тока небаланса, складывающийся из токов намагничивания каждого из трансформаторов тока (ТТ), участвующих в измерениях. При этом ток небаланса будет равен геометрической разности токов намагничивания ТТ присоединений, в которых токи направлены от шины и ТТ присоединений, в которых токи направлены к шине [Чернобровов Н.В., Семенов В.А. Релейная защита энергетических систем: Учебн. пособие для техникумов. – М.: Энергоатомиздат, 1998].

В отличие от способа-прототипа в способе выявления киберугроз ЦПС при идентификации киберугроз помимо соблюдения условий первого закона Кирхгофа дополнительно учитываются результаты контроля:

– повреждений на шинах (ошиновках);

– возможности насыщения ТТ;

– обрыва вторичных цепей трансформаторов напряжения;

– ошибочных действий эксплуатационного персонала.

Указанная выше контрольная информация поступает в блок анализа 3 из системы

АСУ ТП ЦПС через блок 4. В условиях возникновения указанных выше событий происходит блокировка сигнала с выхода блока 3 устройства фиг. 1.

Для обеспечения возможности более гибкой отстройки критерия срабатывания при контроле уровня токов небаланса на шинах ЦПС, когда величина небаланса токов зависит от их величины, может применяться настраиваемая «тормозная» характеристика [например, Циглер Г. Цифровая дифференциальная защита. Принципы и область применения. М., Знак, 2008]. Она представляет собой зависимость критерия срабатывания ($I_{ср}$) алгоритма контроля от тока торможения ($I_{торм}$). В качестве тормозного тока может использоваться, например, удвоенная величина модуля тока небаланса по присоединениям.

Например, для задания тормозной характеристики используются два параметра для тока срабатывания ($I_{ср1}$ и $I_{ср2}$) и два параметра для тока торможения ($I_{торм1}$ и $I_{торм2}$). В процедуре сравнения участвует измеренный ток торможения $I_{торм}$ и значения $I_{торм1}$ и $I_{торм2}$. На основании их сопоставления формируется решение о принадлежности измеренного тока торможения к одному из трех отрезков (таблица 1).

Таблица 1 – Условия выбора критерия срабатывания алгоритма контроля

Участок характеристики	Ток торможения $I_{торм}$	Ток срабатывания $I_{ср}$
I	$I_{торм} < I_{торм1}$	$I_{ср} = I_{ср1}$
II	$I_{торм1} < I_{торм} < I_{торм2}$	$I_{ср} = \frac{I_{ср2} - I_{ср1}}{I_{торм2} - I_{торм1}} I_{торм}$
III	$I_{торм} > I_{торм2}$	$I_{ср} = I_{ср2}$

Для отстройки алгоритма контроля уровня токов небаланса на шинах ЦПС от режимов КЗ, блоки контроля $1_1 \ldots 1_K$ могут оснащаться модулем контроля производной. Модуль контроля производной позволяет оценить скорость изменения физической величины во времени. Короткие замыкания приводят к аварийному режиму, отличному от нормального режима работы электрической сети. Любой переход электрической сети на новый режим работы сопровождается переходным процессом, при котором скорость изменения электрических величин всегда конечна и ее можно измерить. Если физическая величина (параметры токов и напряжений) изменяется мгновенно, то это противоречит законам электротехники, поскольку ее производная стремится к бесконечности. Выявление указанного факта позволит с высокой долей вероятности сделать вывод о неадекватности данных протекающим физическим процессам на ЦПС, а значит о возможности их подмены в результате кибератаки. Для того чтобы найти производную электрической величины, необходимо разделить разность двух ее последовательно измеренных мгновенных значений на время между измерениями этих значениями. Поскольку цифровой сигнал, например, тока представляет собой квантованные по уровню и дискретизированные по времени отсчеты аналогового сигнала, то

$$I(n) = [I(n) - I(n\text{-}1)] / \Delta t; \Delta t = 1 / f_д = T / N,$$

где n – номер отсчета, $f_д$ – частота дискретизации T – период сигнала промышленной частоты (0,02 с), N – количество отчетов на период промышленной частоты.

Полученную таким образом производную тока сравнивают с пороговыми (уставочными) значениями, а превышение (принижение) уставочного значения будет свидетельствовать о выходе производной тока за физически возможные пределы.

Модуль контроля производной может быть также выполнен в виде

специализированного программного обеспечения каждого из блоков контроля $1_1 \ldots 1_K$.

Контроль состояния вторичных токовых цепей ТТ с использованием метода симметричных составляющих

Дополнительно в устройстве (фиг. 1) осуществляется контроль исправности измерительных ТТ отдельных присоединений, используя информацию с измерительных ТТ смежных присоединений. Алгоритм контроля предполагает оперирование токами и напряжениями прямой, обратной и нулевой последовательностей. В нормальном режиме работы ЦПС несимметрия токов фаз невелика, величины токов обратной и нулевой последовательностей имеют малую величину и не превышают параметры срабатывания (уставки). Обрыв токовых цепей одного из измерительных ТТ может привести к появлению сигнала тока обратной и/или нулевой последовательности на выводах фильтров симметричных составляющих, подключенных к поврежденному ТТ. В блоках контроля $1_1 \ldots 1_K$ осуществляется анализ сигналов с выходов с фильтров симметричных составляющих присоединений шины и, если на одном из присоединений появляются токи обратной и/или нулевой последовательностей, формируется сигнал об обрыве цепей соответствующего ТТ. Если токи обратной и/или нулевой последовательности появляются одновременно на всех контролируемых присоединениях, то это свидетельствует о наличии повреждения на шине ЦПС. При отсутствии фильтров симметричных составляющих на присоединениях секций шин расчет симметричных составляющих производится в блоках контроля $1_1 \ldots 1_K$.

Если токи нулевой последовательности появляются только при протекании тока через землю (КЗ на землю), то токи обратной последовательности небольшой величины могут появляться во время переходных процессов в нормальных режимах функционирования ЦПС, что требует дополнительной отстройки параметра срабатывания по величине токов обратной последовательности на присоединениях.

Таким образом, с выходов блоков контроля $1_1 \ldots 1_K$ выдается сигнал о возможных киберугрозах ЦПС в блок 3 анализа в случае:

– когда трансформаторы тока присоединений любого силового узла исправны, но сумма токов, с учетом их направления, всех присоединений силового узла подстанции не равна нулю, превышает пороговое значение и дополнительно скорость изменения токов присоединения выше скорости протекания переходных процессов при повреждениях и переключениях в электрической сети;

– наличия данных о ненулевых измеренных токах присоединений, поступающих из цифровой шины подстанции, в условиях отсутствия напряжения на силовом узле.

Контроль уровня тока небаланса силового трансформатора

Аналогичный контролю уровня токов небаланса на шинах подстанции с небольшими изменениями в устройстве (фиг. 1) реализуется контроль уровня тока небаланса силового трансформатора. Отличие в функционировании блоков контроля уровня токов небаланса на секциях шин в блоках $2_1 \ldots 2_M$ контроля уровня тока небаланса силового трансформатора необходимо дополнительно учитывать коэффициенты трансформации, группы соединения обмоток, потери электрической мощности в трансформаторе. Применительно к схеме устройства фиг. 1 в блоки $2_1 \ldots 2_M$ из цифровой шины ЦПС поступают значения токов на вводах и выводах трансформаторов, где осуществляется их пофазное сложение. При этом токи на стороне низкого напряжения приводятся к токам на стороне высокого напряжения делением на коэффициент трансформации

$$I_{\text{нн}*} = I_{\text{нн}} / K_{\text{Т}};\ K_{\text{Т}} = U_{\text{ВН}} / U_{\text{НН}},$$

где K_T – коэффициент трансформации; $I_{НН*}$ – приведенный ток со стороны высокого напряжения.

Из получившейся суммы токов в блоках контроля $2_1 \ldots 2_M$ выделяется модуль тока небаланса и сравнивается с параметром срабатывания (уставкой).

Функционирование устройства (фиг. 1) и его блоков контроля $2_1 \ldots 2_M$ должно осуществляться с учетом следующей контрольной информации:

– ошибочных действий персонала;

– повреждений в силовом трансформаторе;

– насыщения ТТ;

– обрыва вторичных цепей ТТ;

– обрыва вторичных цепей трансформаторов напряжения;

– включения в работу (пуска) силового трансформатора.

Указанная выше контрольная информация поступает в блок анализа 3 из системы АСУ ТП ЦПС через блок 4. В условиях возникновения указанных выше событий происходит блокировка сигнала с выхода блока 3 устройства фиг. 1.

Для гибкой настройки параметров контроля уровня тока небаланса силового трансформатора, по аналогии с контролем уровня токов небаланса на шинах ЦПС может применяться тормозная характеристика. Также возможна интеграция модуля измерения скорости изменения тока небаланса, аналогично контролю уровня токов небаланса на шинах ЦПС.

По аналогии с блоками контроля $1_1 \ldots 1_K$ с выходов блоков $2_1 \ldots 2_M$ выдается сигнал о возможных киберугрозах ЦПС в блок 3 анализа в случае:

– когда трансформаторы тока присоединений любого силового узла исправны, но сумма токов, с учетом их направления, всех присоединений силового узла подстанции не равна нулю, превышает пороговое значение и дополнительно скорость изменения токов присоединения выше скорости протекания переходных процессов при повреждениях и переключениях в электрической сети;

– наличия данных о ненулевых измеренных токах присоединений, поступающих из цифровой шины подстанции, в условиях отсутствия напряжения на силовом узле.

Блок 3 анализа предназначен для определения силовых узлов ЦПС, в отношении которых возможны киберугрозы в результате кибератак. Результатом функционирования блока 3 является номер (номера) силового узла (узлов) ЦПС, в отношении которых возможны киберугрозы. Эта информация с выхода блока 3 анализа через блок 4 АСУ ТП ЦПС выдается в систему АСУ ТП ЦПС, а также на верхний уровень управления в центр управления сетями (ЦУС). При блокирующих сигналах с выхода блока 4 на вход блока 3 анализа, указанная выше информация о номере (номерах) силового узла (узлов) ЦПС с выхода устройства (фиг. 1) не выдается.

Следует отметить, что, с точки зрения технической реализации, блоки 1-4 устройства, реализующего способ выявления киберугроз цифровых подстанций, могут быть выполнены в виде промышленных компьютеров.

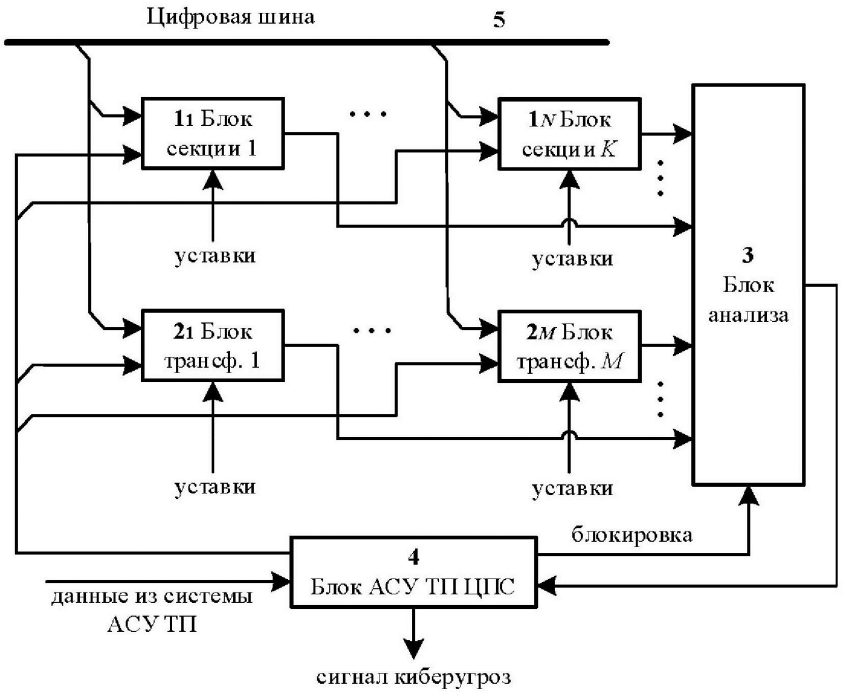
Таким образом, за счет введения специальных процедур контроля за токами и напряжениями силовых узлов, а также использования дополнительной контрольной информации из системы АСУ ТП ЦПС достигается задача изобретения, состоящая в разработке способа, позволяющего выявлять киберугрозы на цифровых подстанциях.

(57) Формула изобретения

Способ выявления киберугроз цифровых подстанций, заключающийся в том, что электрическую подстанцию условно разделяют на силовые узлы, в каждом из которых

соединяются несколько электрических присоединений, измеряют фазные токи всех присоединений силовых узлов подстанции и измеряют напряжения на этих узлах, передают в цифровом виде измеренные токи и напряжения по цифровой шине, контролируют исправность всех трансформаторов тока, регистрируют токи и напряжения, суммируют пофазно фазные токи, с учетом их направления, всех присоединений каждого силового узла подстанции, фиксируют случаи, когда все трансформаторы тока присоединений силового узла исправны и сумма токов, с учетом их направления, всех присоединений силового узла подстанции равна нулю, также фиксируют случаи, когда трансформаторы тока присоединений силового узла исправны, но сумма токов, с учетом их направления, всех присоединений силового узла подстанции не равна нулю и превышает пороговое значение, отличающийся тем, что контролируют состояние вторичных цепей трансформаторов тока с использованием токов обратной и нулевой последовательностей, контролируют скорость изменения измеренных токов присоединений силового узла для выявления отличий кибератак на цифровую подстанцию от повреждений и переключений в прилегающей к цифровой подстанции электрической сети, случаи, когда все трансформаторы тока присоединений любого силового узла исправны и сумма токов, с учетом их направления, всех присоединений силового узла подстанции равна нулю, считают случаями с отсутствием киберугроз цифровой подстанции, а случаи, когда трансформаторы тока присоединений любого силового узла исправны, но сумма токов, с учетом их направления, всех присоединений силового узла подстанции не равна нулю, превышает пороговое значение и дополнительно скорость изменения токов присоединения выше скорости протекания переходных процессов при повреждениях и переключениях в электрической сети, считают случаями, характеризующими киберугрозы цифровой подстанции, к таким случаям также относят факты наличия данных о ненулевых измеренных токах присоединений, поступающих из цифровой шины подстанции, в условиях отсутствия напряжения на силовом узле, выдают сигнал, характеризующий киберугрозы, с выхода устройства, реализующего способ выявления киберугроз цифровых подстанций, на вход автоматизированной системы управления технологическими процессами цифровой подстанции, блокируют выдачу сигнала, характеризующего киберугрозы, с выхода устройства при наличии информации в автоматизированной системе управления технологическими процессами цифровой подстанции об ошибочных действиях оперативного и эксплуатационного персонала, повреждениях силовых узлов подстанции, насыщении трансформаторов тока их присоединений, повреждениях во вторичных цепях измерительных трансформаторов напряжения силовых узлов, а также о включении в работу силовых узлов подстанции, дополнительно связи блоков, входящих в состав устройства, выполняют отдельно от цифровой шины подстанции для предотвращения искажений передаваемых сигналов в условиях кибератак.

1


Цифровая шина
5
11 Блок секции 1
1N Блок секции K
уставки
уставки
21 Блок трансф. 1
2M Блок трансф. M
уставки
уставки
3
Блок анализа
блокировка
4
Блок АСУ ТП ЦПС
данные из системы АСУ ТП
сигнал киберугроз

Фиг. 1