ПОВЫШЕНИЕ КИБЕРБЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГЕТИЧЕСКИХ СИСТЕМ МЕТОДАМИ ОЦЕНИВАНИЯ СОСТОЯНИЯ[1]

Колосок И.Н.[2], Гурина Л.А.[3]

Создание интеллектуальных энергетических систем (ИЭС) предусматривает внедрение системы широкомасштабного мониторинга режимов (WAMS), обеспечивающей использование информационных, вычислительных и цифровых технологий измерения, передачи и обработки параметров режима при решении задач управления. В этой связи отмечена повышенная уязвимость к кибератакам системы управления. Управление ИЭС включает в себя мониторинг, прогнозирование и планирование поведения системы на основе результатов оценивания состояния электроэнергетических систем (ЭЭС). Поэтому, ***целью*** *статьи является разработка математического аппарата получения точных оценок переменных режима как в нормальных, так и критических ситуациях, возникающих при успешно реализованных кибератаках.*

Метод исследования *заключается в анализе возможных кибератак на систему SCADA[4] и WAMS и поиске путей решения задач управления при нарушении информационной безопасности ИЭС. Особое внимание уделено DoS-атакам, последствием которых является отказ устройств измерения и обработки информации.*

Полученные результаты *состоят в разработке алгоритма оценивания состояния на основе метода внутренних точек, обеспечивающего требуемую точность при низком качестве информации и-за нарушения доступности данных измерений. Практические расчеты показали эффективность применения предложенного подхода оценивания состояния ЭЭС при кибератаках.*

Ключевые слова: *SCADA, WAMS, кибератаки, измерения, полнота, достоверность, метод внутренних точек*

DOI:1021681/2311-3456-2018-3-63-69

Введение

Развитие электроэнергетических систем осуществляется в соответствии с реализацией концепции Smart Grid, определяемой в России как интеллектуальная энергетическая система (ИЭС). Большое значение приобретает внедрение систем широкомасштабного мониторинга режимов и управление ИЭС на основе современных интеллектуальных информационно-коммуникационных технологий, средств и технологий измерений, передачи, обработки и представления информации [1]. Увеличивается использование информационных и вычислительных средств в информационно-коммуникационной инфраструктуре ИЭС, вследствие чего, повышается уязвимость ИЭС к кибератакам. Поэтому для надежного функционирования ИЭС задачи управления должны решаться с учетом появившихся киберугроз, влияющих на качество режимной информации.

Для оперативного и противоаварийного управления ИЭС используются параметры текущего режима, получаемые путем решения задачи оценивания состояния (ОС) по измерениям, поступающим от системы SCADA и WAMS (Wide Area Measurement Systems) [2].

В случае успешно реализованных кибератак на систему SCADA и WAMS, может произойти потеря данных, поступающих от измерительных устройств, также измерения могут содержать ошибки [3], не обнаруживаемые традиционными подходами при решении задачи ОС [4].

Цель статьи состоит в разработке математического аппарата получения точных оценок переменных режима как в нормальных, так и в критических ситуациях, возникающих при успешно реализованных кибератаках.

Метод исследования заключается в анализе возможных кибератак на систему SCADA и WAMS и поиске путей решения задач управления при нарушении информационной безопасности ИЭС.

Результатом работы является разработанный алгоритм оценивания состояния ИЭС на основе метода внутренних точек, обеспечивающий требуемую точность при низком качестве информации, обусловленном нарушением доступности данных измерений. Интервальная постановка задачи ОС учитывает не только законы электрических цепей (уравнения установившегося ре-

1. Работа выполнена в рамках научного проекта III.17.4.2. программы фундаментальных исследований СО РАН, рег. № АААА-А17-117030310438-1
2. Колосок Ирина Николаевна, доктор технических наук, Институт систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск Россия, kolosok@isem.irk.ru
3. Гурина Людмила Александровна, кандидат технических наук, доцент, Институт систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск, Россия, gurina@isem.irk.ru
4. программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки отображения и архивирования информации об объекте мониторинга или управления

жима), но и допустимые технологические пределы изменения параметров режима (ограничения-неравенства) [5].

Предлагаемый подход к решению задачи оценивания состояния позволяет получать оценки неизмеренных переменных режима в случае отказа в работе измерительных устройств и обнаруживать искаженную информацию в измерениях при реализованных кибератаках на измерительные системы. Тем самым повышается точность результатов ОС. Практические расчеты показали эффективность применения предложенного подхода ОС.

Кибербезопасность системы управления ИЭС

При исследовании проблем кибербезопасности ИЭС выделено две подсистемы – управляющая (информационно-коммуникационная) и управляемая (технологическая). К информационно-коммуникационной подсистеме относятся системы SCADA, WAMS. В качестве управляемой рассматриваются объекты управления (электрические станции, подстанции, передающие и распределительные сети) [6].

Иерархическая структура системы управления ИЭС показана на рис. 1.

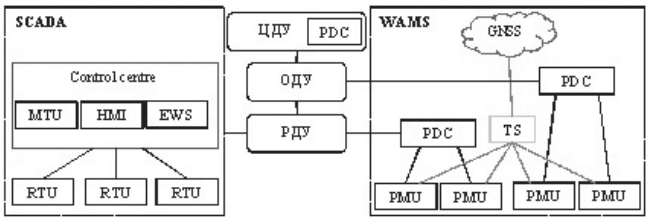

Рис. 1 Иерархическая структура системы управления ИЭС

Системы SCADA, предназначенные для поддержки действий диспетчерского персонала при оперативном и противоаварийном управлении ИЭС, включают в себя: установленные на подстанциях удаленные устройства телемеханики (RTU - Remote Terminal Unit) для снятия телесигналов о состоянии коммутационного оборудования и телеизмерений параметров режима, каналы связи; диспетчерские пункты управления (MTU – Master Terminal Unit), обеспечивающие человеко-машинный интерфейса (HMI – Human Machine Interface) между оператором (EWS – Engineering Work Station) и системой.

Российский аналог WAMS – система мониторинга переходных режимов представляет собой совокупность регистраторов синхронизированных векторных измерений (PMU), концентраторов векторных данных (PDC) на всех уровнях диспетчерского управления (центральное диспетчерское управление, объединенное диспетчерское управление, региональное диспетчерское управление), каналов передачи информации между регистраторами, концентраторами данных и диспетчерскими центрами ОАО «СО ЕЭС»[5], а также средств обработки полученной информации. Синхронизация измерений WAMS осуществляется при помощи глобальных навигационных спутниковых систем GPS/ГЛОНАСС (GNSS – Global Navigation Satellite Systems). Прием сигналов от GNSS ведется сервером времени (TS – Time Server), предназначенным для формирования сигналов точного времени и дальнейшей синхронизации измерений PMU [7,8].

Функциональными компонентами управляющей подсистемы являются измерительные подсистемы, подсистемы передачи данных, подсистемы обработки данных, подсистемы синхронизации времени.

Анализ [9-13] показал возможные кибератаки на функциональные компоненты систем SCADA и WAMS.

Разведывательные атаки позволяют злоумышленнику определить слабые места и потенциальные цели в архитектуре системы SCADA и WAMS. В подсистеме измерения и обработки данных целью этих атак может быть определение IP-адресов подключенных PMU, RTU, PDC, MTU. Такая информация может быть использована для проведения атак внедрения ложных данных и отказа в обслуживании. В подсистеме передачи данных может производиться сканирование сети, протоколов передачи сети, анализ сетевого трафика.

Атаки внедрения ложных данных направлены на нарушение целостности, доступности и достоверности данных или же работоспособности системы управления. Такие атаки могут быть реализованы внедрением ложных данных в измерения или в команды. Они могут быть направлены против одного или нескольких RTU/PMU, а также против PDC, который принимает потоки синхронизированных данных от нескольких PMU и формирует единый поток вывода. Это делает MTU/PDC идеальной мишенью для вторжения, чтобы затем манипулировать большим количеством синхронизированных измерений [14, 15].

Атаки отказа в обслуживании (DoS-атаки) негативно влияют на доступность данных измерений. Отказ в обслуживании может прекратить передачу измерений от PMU или RTU в управляющие центры, передачу управляющих воздействий или и то, и другое. Кроме этого, при осуществлении атаки отказа в обслуживании может прекратиться работа PMU, PDC и супер-PDC системы WAMS или RTU, MTU системы SCADA, что чревато потерей наблюдаемости системы.

Атаки повторного воспроизведения позволяют злоумышленникам перехватывать и сохранять потоки данных для повторной ретрансляции и манипуляции ими, а также вводить ложные управляющие сигналы в систему. Успешно реализованные атаки могут привести к аварийным ситуациям в технологической подсистеме.

Основная цель реализации **атаки создания помех** – это зашумление каналов передачи данных сигналами помех для нарушения связи между компонентами систем SCADA и WAMS.

Атаки, направленные на GNNS называются атаками синхронизации времени. К ним относятся **спуфинг-**

5. Акционерное общество «Системный оператор Единой энергетической системы» - специализированная организация, единолично осуществляющая централизованное оперативно-диспетчерское управление в Единой энергетической системе России.

Таблица 1. Расход трафика

<table>
<tr><td>Присоединение к сети</td><td>Анализ портов</td><td>Использование свободных портов</td><td rowspan="5">Расход трафика</td></tr>
<tr><td rowspan="3">Анализ трафика</td><td>Знание структуры пакетов данных</td><td>Заполнение сети</td></tr>
<tr><td colspan="2">Небезопасная межсетевая защита</td></tr>
<tr><td colspan="2">Нахождение лазеек в протоколах</td></tr>
<tr><td colspan="3">Заполнение сети случайными данными</td></tr>
</table>

Таблица 2. Недостаток ресурсов

<table>
<tr><td>Знание операционной системы</td><td colspan="2">Планирование повреждений операционной системы</td><td rowspan="2">Недостаток ресурсов</td></tr>
<tr><td>Получение доступа к сети</td><td>Анализ трафика</td><td>Синхронная атака</td></tr>
</table>

Таблица 3. Ошибки программного обеспечения

Присоединение к сети	Путь обхода системы защиты	Модификация значений ключа	Ошибки программного обеспечения

атаки. Здесь противник может манипулировать временными метками измерений, что может привести к неточным действиям по управлению. При проведении таких атак подделывается сигнал GPS, так что формирование выборки измерений PMU происходит несинхронно, что позволяет производить измерения PMU с неправильными метками времени.

Успешно проведенные кибератаки влияют на качество решения задач управления ИЭС – планирование режимов, прогнозирование, мониторинг, оценивание состояния и т.д. Поэтому необходимо развитие и разработка методов решения задач управления, обеспечивающих надежное функционирование ИЭС при кибервторжениях [16].

Установлено, что наиболее уязвимыми к кибератакам являются устройства измерения системы SCADA и WAMS. Особого внимания заслуживают DoS-атаки, влияющие на работоспособность этих устройств.

DoS-атаки на систему SCADA и WAMS

В [13] описаны 3 категории DoS-атак на измерительные устройства:

- расход трафика;
- недостаток или исчерпание ресурсов;
- ошибки программного обеспечения.

Способы и пути успешной реализации DoS-атак представлены в табл. 1-3.

Последствия проведенных DoS-атак приводят к задержке поступления данных от измерительных устройств, потере данных или RTU/PMU может прекратить отвечать на запросы MTU/PDC.

В [13] предложены меры по предотвращению кибер-вторжений в системы управления: шифрование данных, ограничение доступа к сети с помощью межсетевых экранов, защита операционной системы и т.д.

С функциональной точки зрения, как отмечено выше, успешно реализованные кибератаки влияют на качество функционирования ИЭС и точность решения задач управления. В статье рассмотрена задача ОС ЭЭС, используемая для формирования модели текущего режима, на базе которой затем решаются задачи оперативного и противоаварийного управления.

Оценивание состояния по данным SCADA и WAMS

В нашей стране основателем школы оценивания состояния электроэнергетической системы является проф. А.З. Гамм. В его работах рассмотрены методические вопросы ОС, поставлены основные задачи, входящие в комплекс проблем ОС, и предложены пути их решения. В основе решения задачи ОС в данной работе заложены принципы, сформулированные Гаммом А.З.

Задача оценивания состояния электроэнергетической системы состоит в поиске таких расчетных значений (оценок) измеряемых параметров режима $\hat{y}$, которые *наиболее близки* к измеренным значениям $\bar{y}$ в смысле некоторого критерия и удовлетворяют уравнениям электрической цепи

$$w(y,z)=0, \qquad (1)$$

связывающие измеренные y и неизмеренные z параметры режима. В качестве критерия при ОС чаще всего используется сумма взвешенных квадратов отклонений оценок от измерений:

$$J(y)=(\bar{y}-\hat{y})^T R_y^{-1}(\bar{y}-\hat{y}), \qquad (2)$$

где R_y – диагональная матрица, элементы которой равны дисперсиям измерений σ^2, $\bar{y}$ – вектор измерений SCADA и WAMS, включающий модули U_i и фазы δ_i узловых напряжений, генерации активных $P_{Гi}$ и реактивных $Q_{Гi}$ мощностей в узлах, перетоки мощностей в трансформаторах и линиях P_{ij}, Q_{ij}, токи в узлах и в линиях I_i, I_{ij}, φ_{ij} – углы между током и напряжением:

$$\bar{y}=\{P_i,Q_i,P_j,Q_j,U_i,\delta_i,I_i,I_j,\varphi_j\}.$$

Для получения узловых инъекций P_i, Q_i в дополнение к телеизмерениям генерации используются псевдоизмерения узловых нагрузок.

Учет ограничений при оценивании состояния ЭЭС

В общем случае при решении задачи ОС необходимо учитывать несколько типов ограничений.

1. Уравнения установившегося режима (1), которым должны удовлетворять найденные оценки измеренных y и неизмеренных z параметров режима.

2. Полученные при ОС расчетные значения некоторых параметров режима должны находиться в определенных технологических пределах. Активные и реактивные генерации в узлах должны находиться внутри пределов, определяемых графиком выработки мощности; на перетоки мощности по линиям могут быть заданы пределы, определяемые пропускной способностью линии; в нагрузочных узлах должно быть обеспечено правильное направление (знак) узловой инъекции и т.д.

Поэтому при решении задачи ОС помимо ограничений, задаваемых в форме равенств, необходимо также учитывать ограничения в форме неравенств, задаваемые как для измеренных y:

$$y_{\min} \le y \le y_{\max}, \quad (3)$$

так и для неизмеренных параметров режима z:

$$z_{\min} \le z \le z_{\max}, \quad (4)$$

где $y_{\min}, y_{\max}, z_{\min}, z_{\max}$ – априори известные нижние и верхние границы изменения значений переменных, входящих в векторы y и z соответственно.

Следует отметить, информация об ограничениях и их учет при решении задачи оценивания состояния является чрезвычайно полезной: она позволяет априори выявить грубые ошибки в измерениях, предельные значения генераций реактивных мощностей могут использоваться в качестве псевдоизмерений в ненаблюдаемых узлах, ограничения содержат достоверную информацию о физически возможных технологических пределах оборудования, поэтому их учет позволяет повысить качество оценок и получить решение, отражающее физическое состояние ЭЭС. Особенно важно их использование при наметившейся тенденции роста киберугроз и их осуществлении на системы управления ИЭС, способствующие искажению и потере измерительной информации [3].

В таких случаях при решении задачи ОС может быть использован метод внутренних точек (МВТ) [17-19], позволяющий учитывать не только ограничения (1),(3) [2, 4, 20], но и ограничения (4) [5] в случае потери информации из-за реализованных кибератак.

Метод внутренних точек

Требуется минимизировать (2) при ограничениях (1), (3), (4).

В общем случае, ограничения (1) нелинейные. После линеаризации представим их в виде:

$$Ay + Bz = \eta,$$

где A, B - матрицы коэффициентов при измеренных и неизмеренных переменных соответственно, $\eta \neq 0$ - ошибка линеаризации.

Алгоритм внутренних точек состоит из 2 этапов:

1. Ввод в область допустимых решений;

2. Оптимизация в области допустимых решений и заключается в итерационном нахождении:

$$y^{(k+1)} = y^{(k)} + \lambda^{(k)}\Delta y^{(k)},$$
$$z^{(k+1)} = z^{(k)} + \lambda^{(k)}\Delta z^{(k)}, \quad (5)$$

где $\Delta y^{(k)}$, $\Delta z^{(k)}$ - направления корректировки текущего приближения, $\lambda^{(k)}$ - величина шага вдоль этого направления.

На этапе ввода в допустимую область для поиска направлений корректировки $\Delta y^{(k)}$, $\Delta z^{(k)}$ текущих приближений $y^{(k)}$, $z^{(k)}$ (k - номер итерации) минимизируется функция

$$F^{(k)} = \frac{1}{2}\sum_{j=1}^{m}\frac{(\Delta y_j^{(k)})^2}{d_j^{(k)}} + \frac{1}{2}\sum_{j=1}^{n}\frac{(\Delta z_j^{(k)})^2}{g_j^{(k)}} \to \min, \quad (6)$$

где $d_j^{(k)}$, $g_j^{(k)}$ - квадратичные весовые коэффициенты, определяемые как

$$d_j^{(k)} = (\min\{y_{\max j} - y_j^{(k)}, y_j^{(k)} - y_{\min j}\})^2, j = 1,...,m.$$
$$g_j^{(k)} = (\min\{z_{\max j} - z_j^{(k)}, z_j^{(k)} - z_{\min j}\})^2, j = 1,...,n$$

,

при ограничениях

$$A\Delta y^{(k)} + B\Delta z^{(k)} - \eta = r^{(k)}, \quad (7)$$

где $r^{(k)}$ - вектор невязок на k-й итерации

Обозначим диагональные матрицы

$$D = diag(d^{(k)}), G = diag(g^{(k)}).$$

Задача решается методом неопределенных множителей Лагранжа. Исходя из условий оптимальности, запишем

$$\Delta y = D^{(k)}A^T u, \Delta z = G^{(k)}B^T u, \quad (8)$$

где u - вектор множителей Лагранжа.

Подставив (7) в (6), получим систему линейных уравнений относительно u,

$$AD^{(k)}A^T u + BG^{(k)}B^T u = r^{(k)}, \quad (9)$$

Найдя вектор u, исходя из (8) определяем направления улучшения решения $\Delta y^{(k)}$, $\Delta z^{(k)}$.

На этапе оптимизации в области допустимых решений минимизируется функция

$$F^{(k)} = \frac{1}{2}\sum_{j=1}^{m}\frac{(\Delta y_j^{(k)})^2}{d_j^{(k)}} + \frac{1}{2}\sum_{j=1}^{n}\frac{(\Delta z_j^{(k)})^2}{g_j^{(k)}} + J(y^{(k)} + \Delta y) \to \min, \quad (10)$$

где

$$J(y^{(k)} + \Delta y) = J(y^{(k)}) + \frac{1}{2}\sum_{j=1}^{n}\sigma_j^{-2}(\Delta y_j)^2 + c^{(k)}\Delta y,$$

$$c^{(k)} = \nabla J(y)$$

при ограничениях

$$A\Delta y + B\Delta z = \eta. \quad (11)$$

Методом неопределенных множителей Лагранжа находим

$$\Delta y = (D^{(k)})^{-1} + R^{-1})A^T u^{(k)} + c^{(k)}, \Delta z = G^{(k)}B^T u^{(k)}, \quad (12)$$

Шаг корректировки решения определяется по правилу

$$\lambda^{(k)} = \min\{1, \tilde{\lambda}^{(k)}\}$$

где

$$\tilde{\lambda}^{(k)} = \gamma \max\{\lambda : y_{\min} \le y^{(k)} + \lambda \Delta y^{(k)} \le y_{\max}, z_{\min} \le z^{(k)} + \lambda \Delta z^{(k)} \le z_{\max}\} \quad \gamma \in (0,1)$$

Итеративный переход осуществляется по формулам (5).

Критерием останова является удовлетворение условия

$$\xi = \sqrt{2F^{(k)}} < \varepsilon' \qquad (13)$$

т.е. считается, что получено оптимальное решение.

Пример

Для демонстрации предлагаемого подхода была использована 14-узловая тестовая схема IEEE (рис. 1). В каждом узле установлено устройство RTU.

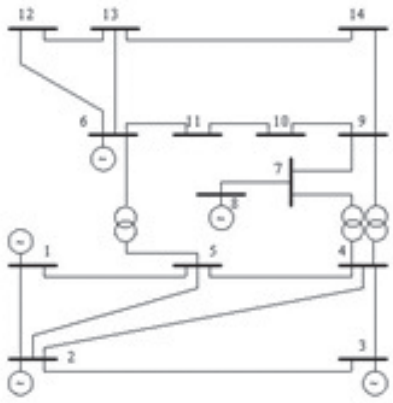

Рис. 2. 14-узловая тестовая схема IEEE

Предположим, что в результате DoS-атаки на систему SCADA вышло из строя RTU второго узла и произошла потеря измерений P_2, Q_2, P_{2-1}, P_{2-3}, Q_{2-3}, P_{2-4}, Q_{2-4}, P_{2-5}, Q_{2-5}, которые образуют вектор z. Вектор y составили следующие измерения

$$y = (P_1, Q_1, U_1, P_4, Q_4, P_5, Q_5, U_5, P_1, Q_1, P_3, Q_3, P_4, Q_4, P_7, Q_7, P_8, Q_8, P_3, Q_3, P_6, Q_6, P_9, Q_9, P_0, Q_0, U_0, P_2, Q_2, Q_{1-2}, P_{1-5}, Q_{1-5}, P_{3-4}, Q_{3-4}, P_{4-5}, Q_{4-5}, P_{4-7}, Q_{4-7}, P_{4-9}, Q_{4-9}, P_{5-6}, Q_{5-6}, P_{6-1}, Q_{6-1}, P_{6-2}, Q_{6-2}, P_{6-3}, Q_{6-3}, P_{7-8}, Q_{7-8}, P_{7-9}, Q_{7-9}, P_{9-0}, Q_{9-0}, P_{9-4}, Q_{9-4}, P_{0-1}, Q_{0-1}, Q_{3-4}, P_{4-3}, P_{2-3}, Q_{2-3})$$

Исходя из технологических условий режима функционирования ЭЭС на неизмеренные переменные наложены ограничений-неравенства:

$$0 \le P_2 \le 50, (MBm),$$
$$0 \le Q_2 \le 50, (MBap),$$
$$-160 \le P_{2-1} \le 0, (MBm),$$
$$0 \le P_{2-3} \le 100, (MBm),$$
$$0 \le Q_{2-3} \le 10, (MBap),$$
$$0 \le P_{2-4} \le 100, (MBm),$$
$$0 \le Q_{2-4} \le 10, (MBap),$$
$$0 \le P_{2-5} \le 100, (MBm),$$
$$0 \le Q_{2-5} \le 10, (MBap).$$

На измерения напряжений ограничения (4) учитываются в диапазоне $\pm 10\%$ от $U_{ном}(кВ)$:

$$65.7 \le U_1 \le 80.3,$$
$$63 \le U_5 \le 70,$$
$$12.6 \le U_{10} \le 15.4.$$

Оценки измеренных y и неизмеренных z параметров режима получены на основе разработанного алгоритма ОС при использовании метода внутренних точек.

Для сопоставления полученных результатов ОС с существующими методами задача также была решена в ПВК «Оценка» [2].

Вычисленные значения критерия минимизации при ОС показаны на рис. 3:

сумма взвешенных квадратов отклонений измерений от эталонных значений;

сумма взвешенных квадратов отклонений полученных оценок измерений в ПВК «Оценка» от эталонных значений;

сумма взвешенных квадратов отклонений полученных предложенным алгоритмом ОС оценок измеренных и неизмеренных параметров режима от эталонных значений.

Полученные результаты подтвердили требуемую точность решения задачи ОС для случая 3 и эффективность использования МВТ при потере измерений.

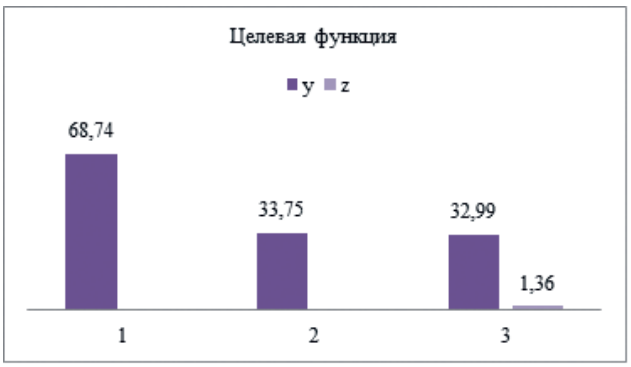

Рис.3 Минимизация целевой функции

Таким образом, предложенный подход позволяет находить оценки не только измеренных параметров режима, но и неизмеренных параметров без поиска вектора состояния в отличие от традиционных методов [2,4].

Выводы

1. В статье приведен анализ кибератак на систему SCADA и WAMS. Особое внимание уделено DoS-атакам, поскольку их успешная реализация может привести к отказу устройств измерения и обработки данных. Тем самым, снижается полнота и достоверность режимной информации.

2. Разработан алгоритм ОС ЭЭС на основе МВТ, позволяющий в случае потери измерений получить их оценки.

3. Результаты расчетов показали эффективность использования предложенного подхода для решения задачи ОС ЭЭС при потере данных вследствие кибератак.

Рецензент: *Массель Людмила Васильевна, профессор, доктор технических наук, главный научный сотрудник ФГБУН Институт систем энергетики им. Л.А. Мелентьева СО РАН, г. Иркутск, Россия. E-mail: massel@isem.irk.ru.*

Литература

1. Voropai N.I., Efimov D.N., Kolosok I.N., Kurbatsky V.G., Glazunova A.M., Korkina E.S., Osak A.B., Tomin N.V., Panasetsky D.A. Smart technologies in emergency control of Russia's unified energy system // IEEE Transactions on Smart Grid. 2013. Т. 4. № 3. Pp. 1732-1740.
2. Глазунова А.М., Колосок И.Н., Коркина Е.С., Гурина Л.А., Аксаева Е.С. Использование СВИ для повышения точности расчета текущего режима ЭЭС методами оценивания состояния // В сборнике: Релейная защита и автоматика энергосистем 2017. Материалы Международной научно-технической конференции. 2017. С. 1081-1087.
3. Gurina L., Kolosok I. Calculation of cyber security index in the problem of power systems state estimation based on SCADA and WAMS measurements // Lecture Notes in Computer Science. 2016. Т. 8985. Pp. 172-177.
4. Глазунова А.М., Колосок И.Н., Съемщиков Е.С. Обнаружение некорректных данных при управлении интеллектуальной энергосистемой методами динамического оценивания состояния // Электричество. 2017. № 2. С. 18-27.
5. Гурина Л.А., Зоркальцев В.И., Колосок И.Н., Коркина Е.С., Мокрый И.В. Оценивание состояния электроэнергетической системы: алгоритмы и примеры линеаризованных задач. – Иркутск: ИСЭМ СО РАН, 2016. – 37 с.
6. Kolosok I., Korkina E., Gurina L. Vulnerability analysis of the state estimation problem under cyber attacks on WAMS // В сборнике: International Conference on Problems of Critical Infrastructures Joint 6th Conference of International Institute for Critical Infrastructures and 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z.A. Styczynski and N.I. Voropai. 2015. Pp. 73-84.
7. Жуков А., Дубинин Д., Опалев О. Развитие систем мониторинга и управления в ЕЭС России. ОАО «СО ЕЭС» // ЭЛЕКТРОЭНЕРГИЯ. Передача и распределение. 2014. № 2(23). С. 52-65.
8. Иванов Ю.В., Черепов А.С., Дубинин Д.М. Системный анализ архитектуры построения и свойств компонентов системы мониторинга переходных режимов // Энергия единой сети. 2016. № 3 (26). С. 62-70.
9. Yao Liu, Peng Ning, Michael K. Reiter. False Data Injection Attacks against State Estimation in Electric Power Grids // CCS'09 Proceedings (9-13 November 2009, Chicago, Illinois, USA). Pp. 21-32.
10. Kebina Manandhar, Xiaojun Cao, Yao Liu. Detection of Faults and Attacks Including False Data Injection Attacks in Smart Grid Using Kalman Filter // IEEE Transactions of Control of Network Systems. Vol. 1, No 4, December 2014. Pp. 370-379.
11. Liang Heng, Jonathan J. Makela, Alejandro D. Dom´ınguez-Garc´ıa, Rakesh B. Bobba, William H. Sanders, and Grace Xingxin Gao. Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture // 2014 Power and Energy Conference at Illinois (PECI) Proceedings. Pp. 1-7.
12. Mohd Rihan, Mukhtar Ahmad, M. Salim Beg. Vulnerability Analysis of Wide Area Measurement System in the Smart Grid // Smart Grid and Renewable Energy [Online] (Sep. 2013). Pp. 1-7. Available: http://www.scirp.org/journal/sigre.
13. Kalluri, R., Mahendra, L., Kumar, R.K.S., Prasad, G.L.G. Simulation and impact analysis of denial-of-service attacks on power SCADA // (2017) 2016 National Power Systems Conference, NPSC 2016, статья № 7858908. DOI: 10.1109/NPSC.2016.7858908.
14. Колосок И.Н., Гурина Л.А. Достоверизация измерений при оценивании состояния ИЭС как средство повышения кибербезопасности системы SCADA // В сборнике: Методические вопросы исследования надежности больших систем энергетики Международный научный семинар им. Ю.Н. Руденко. 2014. С. 296-306.
15. Колосок И.Н., Гурина Л.А. Достоверизация данных синхронизированных векторных измерений при кибератаках на СМПР // Информационные и математические технологии в науке и управлении. 2017. № 1 (5). С. 19-29.
16. Колосок И.Н., Коркина Е.С., Гурина Л.А. Анализ надежности результатов оценивания состояния по данным PMU при кибератаках на WAMS // В сборнике: Методические вопросы исследования надежности больших систем энергетики: Актуальные проблемы надежности систем энергетики Международный научный семинар им. Ю.Н. Руденко. 2015. С. 231-237.
17. Гурина Л.А., Зоркальцев В.И., Колосок И.Н., Коркина Е.С. Развитие методов оценивания состояния электроэнергетических систем на базе симметричной двойственности // В сборнике: Математическое моделирование, оптимизация и информационные технологии. Материалы 5-й международной конференции. 2016. С. 97-110.
18. Зоркальцев В.И. Поиск допустимых решений алгоритмами внутренних точек // Сибирский журнал вычислительной математики. 2016. Том 19. № 3. С. 249-265.
19. Зоркальцев В.И., Мокрый И.В. Алгоритмы внутренних точек в линейной оптимизации // Сибирский журнал индустриальной математики. 2018. Т. 21. № 1(73). С. 11-20.
20. Хохлов М.В., Готман Н.Э. Робастное обобщенное оценивание состояния ЭЭС: метод на основе целочисленного линейного программирования // В сборнике: Методические вопросы исследования надежности больших систем энергетики Материалы Международного научного семинара им. Ю.Н. Руденко. 2017. С. 495-504.

IMPROVEMENT OF CYBERSECURITY OF SMART GRID BY STATE ESTIMATION METHODS[6]

Kolosok I.N.[7], Gurina L.A.[8]

6. This study is supported by the Siberian Branch of the Russian Academy of Sciences (Project III.17.4.2) of the Federal Program of Scientific Research (№ AAAA-A17-117030310438-1).
7. Irina Kolosok, Dr.Sc., Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, Irkutsk, Russia, kolosok@isem.irk.ru.
8. Liudmila Gurina, Ph.D., Associate Professor, Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, Irkutsk, Russia, gurina@isem.irk.ru.

Abstract. *Development of Smart Grid involves the introduction of Wide Area Measurement System (WAMS), which provides the use of information, computing and digital technologies for measuring, transmitting and processing operating parameters when solving control problems. In this regard, the increased vulnerability to cyberattacks of the control system was noted. The control of Smart Grid includes monitoring, forecasting and planning of the system operation based on its Electric Power System state estimation results. Therefore, the goal of the paper is to develop a mathematical instrument to obtain accurate estimates of the state variables in both favorable and critical situations that arise due to cyberattacks. The research method suggests analyzing possible cyberattacks on SCADA system and WAMS, and finding the ways to solve control problems for the case of Smart Grid information insecurity. Particular attention is paid to DoS-attacks which result in failures of measuring and processing devices. The result of the research is an algorithm developed for state estimation based on the interior point method that provides the required accuracy with low quality of information due to unavailability of measurement data. Practical calculations demonstrate the effectiveness of the proposed approach to EPS state estimation under cyberattacks.*

Keywords: *SCADA, WAMS, cyberattacks, measurements, completeness, reliability, interior point method*

References

1. Voropai N.I., Efimov D.N., Kolosok I.N., Kurbatsky V.G., Glazunova A.M., Korkina E.S., Osak A.B., Tomin N.V., Panasetsky D.A. Smart technologies in emergency control of Russia's unified energy system // IEEE Transactions on Smart Grid. 2013. T. 4. № 3. Pp. 1732-1740.
2. Glazunova A.M., Kolosok I.N., Korkina E.S., Gurina L.A., Aksaeva E.S. Ispol`zovanie SVI dlya povy`sheniya tochnosti rascheta tekushhego rezhima E`E`S metodami ocenivaniya sostoyaniya // V sbornike: Relejnaya zashhita i avtomatika e`nergosistem 2017. Materialy` Mezhdunarodnoj nauchno-texnicheskoj konferencii. 2017. S. 1081-1087.
3. Gurina L., Kolosok I. Calculation of cyber security index in the problem of power systems state estimation based on SCADA and WAMS measurements // Lecture Notes in Computer Science. 2016. T. 8985. Pp. 172-177.
4. Glazunova A.M., Kolosok I.N., S``emshhikov E.S. Obnaruzhenie nekorrektny`x danny`x pri upravlenii intellektual`noj e`nergosistemoj metodami dinamicheskogo ocenivaniya sostoyaniya // E`lektrichestvo. 2017. № 2. S. 18-27.
5. Gurina L.A., Zorkal`cev V.I., Kolosok I.N., Korkina E.S., Mokry`j I.V. Ocenivanie sostoyaniya e`lektroe`nergeticheskoj sistemy`: algoritmy` i primery` linearizovanny`x zadach. – Irkutsk: ISE`M SO RAN, 2016. – 37 s.
6. Kolosok I., Korkina E., Gurina L. Vulnerability analysis of the state estimation problem under cyber attacks on WAMS // V sbornike: International Conference on Problems of Critical Infrastructures Joint 6th Conference of International Institute for Critical Infrastructures and 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z.A. Styczynski and N.I. Voropai. 2015. Pp. 73-84.
7. Zhukov A., Dubinin D., Opalev O. Razvitie sistem monitoringa i upravleniya v EE`S Rossii. OAO «SO EE`S» // E`LEKTROE`NERGIYa. Peredacha i raspredelenie. 2014. № 2(23). S. 52-65.
8. Ivanov Yu.V., Cherepov A.S., Dubinin D.M. Sistemny`j analiz arxitektury` postroeniya i svojstv komponentov sistemy` monitoringa perexodny`x rezhimov // E`nergiya edinoj seti. 2016. № 3 (26). S. 62-70.
9. Yao Liu, Peng Ning, Michael K. Reiter. False Data Injection Attacks against State Estimation in Electric Power Grids // CCS'09 Proceedings (9-13 November 2009, Chicago, Illinois, USA). Pp. 21-32.
10. Kebina Manandhar, Xiaojun Cao, Yao Liu. Detection of Faults and Attacks Including False Data Injection Attacks in Smart Grid Using Kalman Filter // IEEE Transactions of Control of Network Systems. Vol. 1, No 4, December 2014. Pp. 370-379.
11. Liang Heng, Jonathan J. Makela, Alejandro D. Dom´ınguez-Garc´ıa, Rakesh B. Bobba, William H. Sanders, and Grace Xingxin Gao. Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture // 2014 Power and Energy Conference at Illinois (PECI) Proceedings. Pp. 1-7.
12. Mohd Rihan, Mukhtar Ahmad, M. Salim Beg. Vulnerability Analysis of Wide Area Measurement System in the Smart Grid // Smart Grid and Renewable Energy [Online] (Sep. 2013). Pp. 1-7. Available: http://www.scirp.org/journal/sigre.
13. Kalluri, R., Mahendra, L., Kumar, R.K.S., Prasad, G.L.G. Simulation and impact analysis of denial-of-service attacks on power SCADA // (2017) 2016 National Power Systems Conference, NPSC 2016, stat`ya № 7858908. DOI: 10.1109/NPSC.2016.7858908.
14. Kolosok I.N., Gurina L.A. Dostoverizaciya izmerenij pri ocenivanii sostoyaniya IE`S kak sredstvo povy`sheniya kiberbezopasnosti sistemy` SCADA // V sbornike: Metodicheskie voprosy` issledovaniya nadezhnosti bol`shix sistem e`nergetiki Mezhdunarodny`j nauchny`j seminar im. Yu.N. Rudenko. 2014. S. 296-306.
15. Kolosok I.N., Gurina L.A. Dostoverizaciya danny`x sinxronizirovanny`x vektorny`x izmerenij pri kiberatakax na SMPR // Informacionny`e i matematicheskie texnologii v nauke i upravlenii. 2017. № 1(5). S. 19-29.
16. Kolosok I.N., Korkina E.S., Gurina L.A. Analiz nadezhnosti rezul`tatov ocenivaniya sostoyaniya po danny`m PMU pri kiberatakax na WAMS // V sbornike: Metodicheskie voprosy` issledovaniya nadezhnosti bol`shix sistem e`nergetiki: Aktual`ny`e problemy` nadezhnosti sistem e`nergetiki Mezhdunarodny`j nauchny`j seminar im. Yu.N. Rudenko. 2015. S. 231-237.
17. Gurina L.A., Zorkal`cev V.I., Kolosok I.N., Korkina E.S. Razvitie metodov ocenivaniya sostoyaniya e`lektroe`nergeticheskix sistem na baze simmetrichnoj dvojstvennosti // V sbornike: Matematicheskoe modelirovanie, optimizaciya i informacionny`e texnologii. Materialy` 5-j mezhdunarodnoj konferencii. 2016. S. 97-110.
18. Zorkal`cev V.I. Poisk dopustimy`x reshenij algoritmami vnutrennix tochek // Sibirskij zhurnal vy`chislitel`noj matematiki. 2016. Tom 19. № 3. S. 249-265.
19. Zorkal`cev V.I., Mokry`j I.V. Algoritmy` vnutrennix tochek v linejnoj optimizacii // Sibirskij zhurnal industrial`noj matematiki. 2018. T. 21. № 1(73). S. 11-20.
20. Xoxlov M.V., Gotman N.E`. Robastnoe obobshhennoe ocenivanie sostoyaniya E`E`S: metod na osnove celochislennogo linejnogo programmirovaniya // V sbornike: Metodicheskie voprosy` issledovaniya nadezhnosti bol`shix sistem e`nergetiki Materialy` Mezhdunarodnogo nauchnogo seminara im. Yu.N. Rudenko. 2017. S. 495-504.