УДК 621.311.171

КРАТНІСТЬ РЕЗЕРВУВАННЯ ЕЛЕМЕНТІВ ЕНЕРГОСИСТЕМИ В УМОВАХ КІБЕРБЕЗПЕКИ

Гриб О. Г., Швець С. В., Бортніков О. В.

Національний технічний університет "Харківський політехнічний інститут"

Розглянуто одну із складових кібербезпеки сучасних енергосистем – апаратну безпеку найважливіших елементів системи управління режимами роботи енергосистем. Для підвищення надійності роботи найважливіших елементів системи управління в умовах кібербезпеки запропоновано підхід щодо визначення кратності резервування її елементів при недостатній інформації про ймовірність їх безвідмовної роботи на заданому інтервалі часу.

Постановка проблеми. Однією з тенденцій розвитку світової енергетики є створення концепції й впровадження технологій Smart Grid. Основними досягненими результатами повинна стати автоматизація управління енергосистемою, яка забезпечить її високу надійність і високі економічні показники роботи [1]. У розробленій концепції широко декларується мультиагентний підхід до побудови системи управління енергосистемами, але не приділяється достатня увага тому, що мультиагентна система управління енергосистемою повинна забезпечувати надійне й безпечне функціонування й управління [2]. У цьому випадку проблема надійності й безпеки мультиагентної системи управління режимами роботи енергосистеми перебуває в протиріччі між основними принципами її організації. Така система управління є принципово вразливою з погляду кібербезпеки, і необхідні нові способи забезпечення її безпеки й стійкості стосовно неякісних і недружніх даних. Згідно зі стандартом [3] кібернетична безпека полягає в спробі досягнення й збереження властивостей безпеки у ресурсів енергосистеми або споживача. Якщо ці питання не вирішені, то вразлива система управління енергосистемою стане причиною великих техногенних аварій по усьому світу.

Аналіз останніх досліджень і публікацій. Серед основних задач забезпечення кібербезпеки в Smart Grid для енергосистем є забезпечення доступності, при одночасному забезпеченні цілісності й конфіденційності. Це означає, що енергосистема повинна бути безпечною й забезпечувати захист від кібернетичних загроз [4]. Сьогодні відомі два види дистанційного деструктивного впливу на мікропроцесорні системи: кібернетичні атаки й навмисні деструктивні електромагнітні впливи [5]. Сучасні тенденції розвитку систем управління енергосистем, такі як постійне ускладнення апаратної і програмної частин цифрових компонентів; збільшення кількості виконуваних ними функцій; перехід з оптоволоконних на менш захищені канали зв'язку (Ethernet, Wi-Fi) – усе це й багато чого іншого суттєво полегшує реалізацію кіберзагроз. З одного боку, відбувається постійний ріст вразливості систем управління енергосистем, а з іншого – постійне вдосконалювання методів дистанційного деструктивного впливу. У результаті, ці два найнебезпечніші вектори розвитку стрімко рухаються назустріч один одному. Для протистояння дистанційному деструктивному впливу на енергосистему у вигляді кіберзагроз існують сучасні програмні та апаратні методи [2, 4, 5]. Серед апаратних методів відокремлюються методи, суть яких полягає у виділенні важливих функцій управління протиаварійної і режимної автоматики, цифрового релейного захисту та інших систем, які захищають силове обладнання від пошкодження, та запровадження кратного резервування цих елементів [6]. Даний підхід забезпечить необхідний рівень кібербезпеки енергосистеми при заданих значеннях надійності ключових елементів.

Мета статті. Визначення кратності резервування елементів енергосистем при недостатній інформації про ймовірність їх безвідмовної роботи на заданому інтервалі часу в умовах кібербезпеки.

Основні матеріали дослідження. Розглядається систему управління режимами енергосистеми, яка складається з окремих підсистем. Причому, відмова кожної з них приводить до відмови системи. Кожна з підсистем може бути реалізована $u_{i(l_i)}$ способами, які характеризуються різними значеннями параметрів. Потрібно визначити варіанти кожної підсистеми, які доставляють екстремум цільової функції надійності P з ймовірностями не нижче заданих управлінь, при цьому витрати не повинні перевершувати задані межі.

Математична модель цієї задачі має такий вигляд: визначити варіант системи управління енергосистеми v_0, який доставляє максимум функції

$$P(v) = \prod_{j=1}^{n} P_j(u_{j(l_j)}), \tag{1}$$

при наявності обмежень

$$\begin{gathered} g_p(v) = \sum_{j=1}^{n} g_p(u_{j(l_j)}) \le g_p^* \quad (p = 1, \ ..., q), \\ g_p(v) = \sum_{j=1}^{n} g_p(u_{j(l_j)}) \ge g_p^* \quad (p = q+1, \ ..., Q), \\ v \in V, \quad u_{j(l_j)} \in U_j \quad (j = 1, \ ..., n), \end{gathered} \tag{2}$$

де $U_j = \{u_{j(1)}, ..., u_{j(l_j)}, ..., u_{j(\xi_j)}\}$ $(j = 1, \ ..., n)$ – сукупність елементів різних типів, які можуть бути використані в j-ї підсистемі, кількість елементів у множині U_j рівно ξ_j;

$$V = \prod_{j=1}^{n} U_j; \qquad (3)$$

де V – множина принципово можливих варіантів системи управління режимами енергосистеми;

$P_j(u_{j(l_j)})$ – імовірність безвідмовної роботи на заданому інтервалі часу елемента *j*-ї підсистеми l_j -го типу;

$g_p(u_{j(l_j)})$ – значення *p*-го обмежуючого фактора для елемента *l*-го типу *j*-ї підсистеми;

$g_p(v)$ – кількість *p*-го обмежуючого фактора, витраченого на всю систему;

g_p^* – максимально можлива кількість *p*-го обмежуючого фактора для всієї системи в цілому.

У випадку, коли обмеження на мінімально припустимі значення ймовірності відсутні, то мінімальну кратність резервування можна визначити в такий спосіб.

1. Будемо додавати в *j*-й підсистемі по одному елементу того типу, який має максимальну надійність, до того часу, поки, нарешті, при додаванні чергового елемента не відбудеться порушення хоча б одного з обмежень. Якщо ж обмеження порушуються відразу, то розглядається наступний по надійності тип елементів.

2. Обчислимо значення надійності для побудованої в такий спосіб системи

$$P^* = \prod_{k=1}^{n} (1 - (1 - P_j(u_{k(l_k)})))^{\lambda_{k(l_k)}+1}, \qquad (4)$$

де $P_j(u_{k(l_k)}), (k \neq j)$ – максимально можлива надійність, яку має один з типів елементів, що використовується в k-й підсистемі;

$P_j(u_{j(l_j)})$ – надійність елемента l_j -го типу, що використовується в j-й підсистемі;

$\lambda_{j(l_j)}$ – кількість резервних елементів *j*-ї підсистеми l_j -го типу.

3. З виразу $P^* \le 1 - (1 - P_j(u_{j(l_j)})^{\lambda^{**}_{j(l_j)}+1}$ визначимо $\lambda^{**}_{j(l_j)}$ – мінімально можлива кількість резервних елементів, необхідних для досягнення надійності, рівної P^* або більше. Ясно, що максимум надійності буде досягатися для величин $\lambda_{j(l_j)}$, які, принаймні, не менше отриманих величин $\lambda^{**}_{j(l_j)}$.

Якщо визначена в такий спосіб або за відповідним співвідношенням [6] мінімальна кратність резервування рівна $\lambda^{**}_{j(l_j)}$ хоча б для одного $j = 1, ..., n$, то максимальна кратність резервування $\lambda^{*}_{j(l_j)}$, яка обумовлена виразом у [6], може бути уточнена виразом:

$$\overline{\lambda}^{*}_{j(l_j)} = \min_{p=1,...,q} \left[\frac{g_p^* - \sum_{k=1, k\neq j}^{n} (\lambda^{**}_{j(l_j)} + 1) g_p(u_{k(l_k)})}{g_p(u_{k(l_k)})} - 1 \right]. \qquad (5)$$

Запишемо тепер математичну модель задачі оптимального резервування ("паралельного"):

$$P(v) = \prod_{j=1}^{n} P_j\left(u_{j(l_j)}^{\lambda_{j(l_j)}}\right) \to \max, \qquad (6)$$

при наявності обмежень

$$\begin{aligned} g_p(v) &= \sum_{j=1}^{n} g_p\left(u_{j(l_j)}^{\lambda_{j(l_j)}}\right) \le g_p^* \quad (p = 1, ..., q), \\ g_p(v) &= \sum_{j=1}^{n} g_p\left(u_{j(l_j)}^{\lambda_{j(l_j)}}\right) \ge g_p^* \quad (p = q+1, ..., Q), \\ v \in V'' &= \prod_{j=1}^{n} U_j'', \quad u_{j(l_j)}^{\lambda_{j(l_j)}} \in U_j'' \quad (j = 1, ..., n), \end{aligned} \qquad (7)$$

де наявність у варіанті системи

$$v = \left(u_{1(l_1)}^{\lambda_{1(l_1)}}, ..., u_{j(l_j)}^{\lambda_{j(l_j)}}, ..., u_{n(l_n)}^{\lambda_{n(l_n)}}\right), \qquad (8)$$

змінної $u_{j(l_j)}^{\lambda_{j(l_j)}} \in U_j''$ означає, що в обраному варіанті системи в j-й підсистемі в якості основного й резервних елементів обрані елементи l_j -го типу й обрана кратність резервування рівна $\lambda_{j(l_j)}$, причому $\lambda^{**}_{j(l_j)} \le \lambda_{j(l_j)} \le \lambda^{*}_{j(l_j)}$.

В обмеженнях (7) доданки в лівих частинах, що визначають значення *p*-го обмежуючого фактора для *j*-ї підсистеми (для основного й резервних елементів), перепишуться в такий спосіб

$$g_p\left(u_{j(l_j)}^{\lambda_{j(l_j)}}\right) = (\lambda_{j(l_j)} + 1) g_p(u_{j(l_j)}). \qquad (9)$$

Імовірність безвідмовної роботи *j*-ї підсистеми у виразі (3) визначається в наступному виді

$$P_j\left(u_{j(l_j)}^{\lambda_{j(l_j)}}\right) = 1 - (1 - P_j(u_{j(l_j)}))^{\lambda_{j(l_j)}+1}. \qquad (10)$$

Множина можливих варіантів технічної реалізації *j*-ї підсистеми з резервуванням має вигляд

$$U_j'' = \left\{ \begin{matrix} u_{j(l_j)}^{\lambda_{j(l_j)}} \mid l_j = 1, ..., \xi_j'; \\ \lambda_{j(l_j)} = \lambda^{**}_{j(l_j)}, ..., \lambda^{*}_{j(l_j)} \end{matrix} \right\}; \quad (j = 1, ..., n); \qquad (11)$$

число елементів у цій множині

$$\left|U_j''\right| = \prod_{j=1}^{n} \sum_{l_j=1}^{\xi_j} (\lambda^*_{j(l_j)} - \lambda^{**}_{j(l_j)} + 2). \qquad (12)$$

Задачу (6)-(7) перепишемо в такий спосіб: максимізувати

$$f(\overline{v}) = \sum_{j=1}^{n} f_j(\overline{u}_{j(t_j)}), \qquad (13)$$

при умовах

$$\begin{aligned} & g_p(\overline{v}) = \sum_{j=1}^{n} g_p(\overline{u}_{j(t_j)}) \le g_p^* \quad (p = 1, \ ..., q), \\ & g_p(\overline{v}) = \sum_{j=1}^{n} g_p(\overline{u}_{j(t_j)}) \ge g_p^* \quad (p = q+1, \ ..., Q), \\ & \overline{v} \in \overline{V} = \prod_{j=1}^{n} \overline{U}_j, \quad \overline{u}_{j(t_j)} \in \overline{U}_j \quad (j = 1, \ ..., n), \end{aligned} \qquad (14)$$

де $f(v) = \lg P(v)$;

$$\overline{U}_j = \left\{ \overline{u}_{j(t_j)} \mid t_j = 1, ..., \sum_{l_j=1}^{\xi_j} \left(\left|\lambda_{j(l_j)}\right| + 1 \right) \right\} -$$

множина можливих варіантів j-ї підсистеми;

$$\left|\overline{U}_j\right| = \left|U_j''\right|; \ \left|\overline{V}\right| = \left|V''\right|.$$

Введення множин $\overline{U}_j$ є просто результатом заміни змінної $u_{j(l_j)}^{\lambda_{j(l_j)}}$ на $\overline{u}_{j(t_j)}$ з відповідною зміною множини значень.

Висновки. Поряд з розвитком технологічної інфраструктури енергетики для створення Smart Grid необхідний розвиток і вдосконалення сучасних інформаційних технологій. Однак, використання новітніх технологій – це нові ризики.

В основі складових кібербезпеки енергосистем – інформаційна й апаратна безпека найважливіших елементів системи управління режимами енергосистеми. Для забезпечення необхідного рівня надійності роботи енергосистеми в умовах кібербезпеки запропонований методичний підхід у вигляді визначення кратності резервування цих елементів при недостатній інформації про ймовірність їх безвідмовної роботи на заданому інтервалі часу.

Список використаних джерел

1. Воропай Н. И. Интеллектуальные электроэнергетические системы: концепция, состояние, перспективы / Н. И. Воропай // Автоматизация и IT в энергетике. – 2011. – № 3. – С. 11–16.

2. Массель Л. В. Киберопасность как одна из стратегических угроз энергетической безопасности России / Л. В. Массель, Н. И. Воропай, С. М. Сендеров [и др.] // Вопросы кибербезопасности. – 2016. – № 4(17). – С. 2-10.

3. Марков А. С. Корпоративные информационные системы управления событиями информационной безопасности / А. С. Марков, Ю. В. Рауткин, А. А. Фадин // Труды XVIII Байкальской Всероссийской конференции. – Иркутск, 2013. – С. 412–416.

4. Массель Л. В. Использование современных информационных технологий в Smart Grid как угроза кибербезопасности энергетических систем России / Л. В. Массель // Труды Международной конференции "Кибербезопасность-2013". – К.: Институт специальной связи и защиты информации НТУ Украины "КПИ", 2013. – №1 (3). – С. 56-65.

5. Гуревич В. И. Уязвимости микропроцессорных реле защиты: проблемы и решения / В. И. Гуревич. – М.: Инфра-Инженерия, 2016. – 256 с.

6. Швець С. В. Формування задачі синтезу енергосистеми в умовах кібербезпеки / С. В. Швець, О. Г. Гриб, О. В. Бортніков // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Технічні науки. Випуск 187 "Проблеми енергозабезпечення та енергозбереження в АПК України". – Харків: ХНТУСГ, 2017. – С. 10-11.

Аннотация

КРАТНОСТЬ РЕЗЕРВИРОВАНИЯ ЭЛЕМЕНТОВ ЭНЕРГОСИСТЕМЫ В УСЛОВИЯХ КИБЕРБЕЗОПАСНОСТИ

Гриб О. Г., Швец С. В., Бортников А. В.

Рассмотрена одна из составляющих кибербезопасности современных энергосистем – аппаратная безопасность важнейших элементов системы управления режимами работы энергосистем. Для повышения надежности работы важнейших элементов системы управления в условиях кибербезопасности предложен подход к определению кратности резервирования её элементов при недостаточной информации о вероятности их безотказной работы на заданном интервале времени.

Abstract

RESERVATION OF ELEMENTS OF THE ENERGY SYSTEM IN THE CONDITIONS OF CYBERSECURITY

O. Gryb, S. Shvets, A. Bortnikov

One of the components of cybersecurity of modern energy systems is considered - hardware security of the most important elements of the system for managing the operating modes of power systems. To increase the reliability of the most important elements of the control system in cybersecurity, an approach is proposed to determine the redundancy of its elements with insufficient information about the probability of their trouble-free operation at a given time interval.