УДК 004.032 **DOI: 10.20998/2411-0558.2017.50.03**

О.Г. ГРИБ, д-р техн. наук, проф., НТУ "ХПИ",
С.В. ШВЕЦ, канд. техн. наук, доц., НТУ "ХПИ",
А.В. БОРТНИКОВ, асп., НТУ "ХПИ"

СИНТЕЗ ЭЛЕМЕНТОВ ЭНЕРГОСИСТЕМЫ ПО КРИТЕРИЮ НАДЕЖНОСТИ В УСЛОВИЯХ КИБЕРБЕЗОПАСНОСТИ

Среди аппаратных решений киберзащиты современных энергосистем предложено в их инфраструктуре управления вводить резервирование ключевых элементов для повышения надежности и, тем самым, обеспечения необходимого уровня кибербезопасности. Получены соотношения кратности резервирования элементов для случаев наличия и отсутствия ограничений на минимально допустимые значения вероятностей их безотказной работы. Библиогр.: 10 назв.

Ключевые слова: энергосистема; резервирование; надежность; кибербезопасность; инфраструктура управления.

Постановка проблемы. Энергетика, по сути, является инфраструктурной отраслью, ее задача – обеспечение энергоснабжения потребителей с требуемой надежностью и приемлемым качеством энергоносителя.

На протяжении последнего десятилетия обсуждается проблема создания интеллектуальных электроэнергетических систем (ЭЭС) – Smart Grid [1]. Во многих странах это обусловлено несколькими основными факторами: ожидаемым широким распространением сильно флуктуирующих возобновляемых источников энергии, дополнительным спросом на электроэнергию, связанным с постепенным переходом на электромобили, развитием информационных технологий, позволяющих создать качественно новые высокоэффективные системы мониторинга и управления ЭЭС.

Основными достигнутыми результатами должны стать наблюдаемость, контролируемость, автоматизация управления электроэнергетической системой (ЭЭС), обеспечивающие её высокую надёжность и высокие экономические показатели работы [2].

Очевидно, что успешная реализация этой концепции требует повышенного внимания к проблемам кибербезопасности, поскольку усложнение современных информационных технологий увеличивает уязвимость создаваемых систем [3].

С одной стороны, популярность тематики кибербезопасности АСУ ТП и атак на промышленные системы растет, и будет расти с каждым годом. С другой стороны – автоматизация объектов ЭЭС и открываемые

ею новые горизонты для кибервойны являются чересчур лакомым кусочком для террористических организаций и спецслужб недружественных стран, чтобы их игнорировать [4]. И так как степень автоматизации объектов ЭЭС в дальнейшем будет только расти, риски, связанные с кибератаками на эти объекты, также будут расти.

В современных условиях функционирования энергетической отрасли появилась проблема кибератак на критически важные элементы энергосистемы. Из-за их наличия происходят отключения энергоснабжения потребителей разных категорий, которые проявляются в виде недоотпуска электроэнергии. Эти нарушения сопровождаются потерями данных о режимах работы энергосистемы, что, в свою очередь, ведет к усложнению регулированием перетоками мощностей между частями энергосистемы и может вызвать глобальные системные аварии с тяжкими последствиями для единой энергосистемы страны. В связи с этим становятся актуальными исследования, связанные с повышением надежности функционирования самой системы управления режимами энергосистемы.

Анализ литературы. Современные кибератаки отличаются от тех угроз, с которыми мы привыкли иметь дело и против которых у нас есть средства защиты. Стремительное распространение компьютерной среды, развитие информационных технологий и тенденция перехода к интеллектуальной энергетике делают киберугрозы одной из важнейших тактических угроз энергетической безопасности [5].

В современных условиях, кибербезопасность в электроэнергетике являет собой набор средств, стратегий, принципов обеспечения и гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов энергосистем и потребителей [6].

Проблема кибербезопасности для Украины сегодня уже не нова. Стоит вспомнить недавнюю атаку вируса Petya.A, которая произошла 27 июня 2017 года. Наибольший ущерб понесла именно Украина. В результате кибератаки были заблокированы более 12 тысяч компьютеров в различных государственных и частных учреждениях, среди которых "Киевэнерго", Укрэнерго и корпорация ДТЭК.

Дальнейшее развитие концепций Smart Grid и сетецентрического управления [7, 8] существенно обостряет значение обозначенных проблем. Применение беспилотных летательных аппаратов для мониторинга элементов энергосистем [9] создает дополнительные трудности в реализации защитных функций на аппаратном и программном уровнях.

Среди аппаратных методов, обеспечивающих киберзащиту

современных энергосистем, выделяются методы, суть которых заключается в выделении критических функций управления режимами работы защит от повреждения оборудования [10]. Предлагается, с одной стороны, исключить саму возможность кибератаки на эти элементы защиты путем реализации их не на цифровой базе. Второе направление – введение резервирования важнейших элементов системы управления энергосистемы. Данный подход обеспечит требуемый уровень кибербезопасности энергосистемы при заданных значениях надежности ключевых элементов.

Цель статьи. Развитие алгоритмов синтеза системы управления режимами энергосистемы за счет резервирования ключевых элементов при требуемом уровне кибербезопасности.

Основной раздел. Будем рассматривать сложную систему управления режимами энергосистемы, которая состоит из отдельных подсистем. Отказ любой из них приводит к отказу всей системы управления в целом. Каждая из подсистем может быть реализована $u_{i(l_i)}$ способами, характеризующимися различными значениями технико-экономических параметров (надежность, вес, стоимость, габариты, энергопотребление и т.п.). Требуется определить вариант системы (выбрать вариант реализации каждой подсистемы), который доставляет экстремум целевой функции надежности P и обеспечивает успешное решение всех задач управления режимами энергосистемы с вероятностями не ниже заданных, при этом затраты не должны превосходить заданной границы.

Математическая модель этой задачи имеет следующий вид: определить вариант системы управления энергосистемы v_0, доставляющий максимум функции

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

при наличии ограничений

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

где $P_j(u_{j(l_j)})$ – надежность (вероятность безотказной работы на заданном интервале времени) элемента *j*-й подсистемы l_j-го типа; $U_j = \{u_{j(1)}, ..., u_{j(l_j)}, ..., u_{j(\xi_j)}\}$, $(j = 1, ..., n)$ – совокупность элементов различных типов, которые могут быть использованы в *j*-й подсистеме, количество элементов во множестве U_j равно ξ_j;

$$V = \prod_{j=1}^{n} U_j; \tag{3}$$

$g_p(u_{j(l_j)})$ – значение *p*-го ограничивающего фактора для элемента *l*-го типа *j*-й подсистемы; g_p^* – максимально возможное количество *p*-го ограничивающего фактора для всей системы в целом; $g_p(v)$ – количество *p*-го ограничивающего фактора, израсходованного на всю систему; V – множество принципиально возможных вариантов системы управления режимами энергосистемы.

Задачи типа (1), (2) эквивалентны следующей задаче: найти максимум

$$f(v) = \sum_{j=1}^{n} f_j(u_{j(l_j)}) \tag{4}$$

при наличии (2), где $f_j(u_{j(l_j)}) = \lg P_j(u_{j(l_j)})$. Таким образом, задача оптимального проектирования системы управления режимами энергосистемы по критерию надежности с учетом требуемого уровня кибербезопасности свелась к задаче вида (1), (2), (4).

В нашем случае под резервированием элементов подсистемы (при условии, что используемые ресурсы исчерпаны не полностью) понимается следующее. Если произведено резервирование в *j*-й подсистеме, и она содержит $\lambda_j + 1$ элементов (λ_j резервных и один основной), то выход ее из строя происходит при выходе из строя всех $\lambda_j + 1$ элементов – так называемое "параллельное резервирование".

На первом этапе решения поставленной задачи резервирования отсеиваются все типы элементов, которые учитывать в дальнейшем нет необходимости.

Основой предлагаемого подхода является процедура Z последовательного отсева значений $u_{j(l_j)} \in U_j$ $(j = 1, ..., n)$, т.е.

элементов решения задачи $v = (u_{1(l_1)}, ..., u_{j(l_j)}, ..., u_{n(l_n)}) \in V$. Основная процедура состоит из Q "элементарных" процедур $W_1^p (p = 1, ..., Q)$, каждая из которых заключается в отсеве по p-му ограничению элементов $u_j = u_{j(l_j)}$, $l_j \in J_j = \{1, ..., \xi_j\}$, $j = 1, ..., n$, удовлетворяющих неравенству

$$g_p(u_{1(l_1)}^{p(l_j)}, u_{2(l_2)}^{p(l_j)}, ..., u_{j-1(l_{j-1})}^{p(l_j)}, u_{j(l_j)}^{p(l_j)}, u_{j+1(l_{j+1})}^{p(l_j)}, ..., u_{n(l_n)}^{p(l_j)}) \geq g_p^*, \tag{5}$$

где при $p = 1, ..., q$

$$v^{p(l_j)} = (u_{1(l_1)}^{p(l_j)}, u_{2(l_2)}^{p(l_j)}, ..., u_{j-1(l_{j-1})}^{p(l_j)}, u_{j(l_1)}^{p(l_j)}, u_{j+1(l_{j+1})}^{p(l_j)}, ..., u_{n(l_n)}^{p(l_j)}) \equiv (v^{p(l_j)} \setminus U_j, u_{j(l_j)} = \arg\min_{v \in (V \setminus U_j) \cup (u_{j(l_j)})} g_p(v). \tag{6}$$

При $p = q+1, ..., Q$ справедливо неравенство

$$g_p(u_{1(l_1)}^{p(l_j)}, u_{2(l_2)}^{p(l_j)}, ..., u_{j-1(l_{j-1})}^{p(l_j)}, u_{j(l_j)}^{p(l_j)}, u_{j+1(l_{j+1})}^{p(l_j)}, ..., u_{n(l_n)}^{p(l_j)}) < g_p^*, \tag{7}$$

где

$$v^{p(l_j)} = (u_{1(l_1)}^{p(l_j)}, u_{2(l_2)}^{p(l_j)}, ..., u_{j-1(l_{j-1})}^{p(l_j)}, u_{j(l_1)}^{p(l_j)}, u_{j+1(l_{j+1})}^{p(l_j)}, ..., u_{n(l_n)}^{p(l_j)}) \equiv (v^{p(l_j)} \setminus U_j, u_{j(l_j)} = \arg\max_{v \in (V \setminus U_j) \cup (u_{j(l_j)})} g_p(v). \tag{8}$$

Перепишем условия (5) с учетом (6) и (7) и с учетом (8) в виде:

$$g_p(v^{p(l_j)} \setminus U_j, u_{j(l_j)}) > g_p^*, \quad p = 1, ..., q;$$
$$g_p(v^{p(l_j)} \setminus U_j, u_{j(l_j)}) < g_p^*, \quad p = q+1, ..., Q. \tag{9}$$

Перенумеруем оставшиеся элементы во множествах

U_j $(j=1,...,n)$ и после следующего отсева по ограничениям (2) и (4) получим

$$U'_j = \{u_{j(1)}, ..., u_{j(l_j)}, ..., u_{j(\xi'_j)}\}, \tag{10}$$

где $\xi'_j \le \xi_j$ $(j=1,...,n)$.

Для построения вариантов подсистем с резервированием определим максимальную $\lambda^*_{j(l_j)}$ и минимальную $\lambda^{**}_{j(l_j)}$ кратности резервирования (соответственно, максимальное и минимальное число резервных элементов) для l_j-го типа *j*-й подсистемы. При этом будем использовать вычисленные при реализации процедуры *Z* постоянные для каждой подсистемы величины

$$\begin{gathered}\Delta g_p^j = g_p^* - g_p(v^p_{V(l)} \setminus U_j); \\ (p=1,...,Q; \quad j=1,...,n),\end{gathered} \tag{11}$$

где $g_p(v^p_{V(l)} \setminus U_j)$ определяется (9).

Максимальная кратность резервирования $\lambda^*_{j(l_j)}$ для каждого элемента, вошедшего во множество U'_j, определяется по формуле

$$\lambda^*_{j(l_j)} = \min_{p=1,...,q} \left[\frac{\Delta g_p^j}{g_p(u_{j(l_j)})} - 1 \right], \tag{12}$$

где через $[a]$ обозначена целая часть *a*.

Действительно, если $\lambda_{j(l_j)} > \lambda^*_{j(l_j)}$, то справедливо соотношение (13) и хотя бы одно из ограничений (2) нарушается (здесь использовалось неравенство $[a+1] > a$, справедливое для любого *a*).

Аналогично, минимальная кратность резервирования $\lambda^{**}_{j(l_j)}$ для каждого элемента, вошедшего во множество U'_j, определяется соотношением (14).

Хотя всегда можно принять $\lambda^{**}_{j(l_j)} = 0$, но для уменьшения множества возможных вариантов системы с резервированием получим число различных кратностей резервирования $\left|\widetilde{\lambda}_{j(l_j)}\right| = \lambda^*_{j(l_j)} - \lambda^{**}_{j(l_j)} + 1$ как можно меньшим.

$$\sum_{k=1}^{n}(\lambda_{k(l_k)}+1)g_p(u_{k(l_k)})\geq$$

$$\geq(\lambda_{j(l_j)}+1)g_p(u_{j(l_j)}+\sum_{\substack{k=1\\k\neq j}}^{n}g_p(u_{k(l_k)})\geq$$

$$\geq(\lambda^*_{j(l_j)}+2)g_p(u_{j(l_j)}+\sum_{\substack{k=1\\k\neq j}}^{n}g_p(u_{k(l_k)})\geq \qquad (13)$$

$$\geq \min_{p=1,\ldots,q}\left[\frac{g^*_p-g_p(v^p_{V(l)}\setminus U_j)}{g_p(u_{j(l_j)})}+1\right]\times$$

$$\times g_p(u_{j(l_j)})+g_p(v^p_{V(l)}\setminus U_j)>$$

$$>\min_{p=1,\ldots,q}g^*_p,$$

$$\lambda^{**}_{j(l_j)}=\max_{p=q+1,\ldots,Q}\left[\frac{\Delta g^j_p}{g_p(u_{j(l_j)})}-1\right]. \qquad (14)$$

В случае, когда ограничения на минимально допустимые значения вероятности отсутствуют, то минимальную кратность резервирования можно определить следующим способом.

1. Прибавляют в *j*-й подсистеме по одному элементу того типа, который имеет максимальную надежность, до тех пор, пока, наконец, при добавлении очередного элемента не произойдет нарушение хотя бы одного из ограничений. Если же ограничения нарушаются сразу, то рассматривается следующий по надежности тип элементов.

2. Вычисляют значение надежности для построенной таким образом системы

$$P^*=\prod_{k=1}^{n}(1-(1-P_j(u_{k(l_k)})))^{\lambda_{k(l_k)}+1}, \qquad (15)$$

где $P_j(u_{k(l_k)})$, $(k\neq j)$ – максимально возможная надежность, которой обладает один из типов элементов, использующийся в *k*-й подсистеме; $P_j(u_{j(l_j)})$ – надежность элемента l_j-го типа, использующегося в *j*-й

подсистеме; $\lambda_{j(l_j)}$ – количество резервных элементов j-й подсистемы l_j-го типа.

3. Из выражения $P^* \le 1-(1-P_j(u_{j(l_j)})^{\lambda^{**}_{j(l_j)}+1}$ определяют $\lambda^{**}_{j(l_j)}$ – минимально возможное количество резервных элементов, необходимых для достижения надежности, равной P^* или более. Ясно, что максимум надежности будет достигаться для величин $\lambda_{j(l_j)}$, которые, по крайней мере, не меньше полученных величин $\lambda^{**}_{j(l_j)}$.

Если определенная таким образом или по формуле (14) минимальная кратность резервирования равна $\lambda^{**}_{j(l_j)}$ хотя бы для одного $j=1,...,n$, то максимальная кратность резервирования $\lambda^{*}_{j(l_j)}$, определяемая формулой (12), может быть уточнена выражением (16).

Легко видеть, что $\overline{\lambda}^{*}_{j(l_j)} < \lambda^{*}_{j(l_j)}$. Аналогично можно уточнить минимальную кратность резервирования, определяемую формулой (14), при помощи известной максимальной кратности резервирования $\lambda^{*}_{j(l_j)}$

$$\overline{\lambda}^{*}_{j(l_j)} = \min_{p=1,\,...,\,q}\left[\frac{g^{*}_{p}-\sum\limits_{k=1,\,k\ne j}^{n}(\lambda^{**}_{j(l_j)}+1)g_p(u_{k(l_k)})}{g_p(u_{k(l_k)})}-1\right]. \qquad (16)$$

Запишем теперь математическую модель задачи оптимального резервирования ("параллельного"):

$$P(v)=\prod_{j=1}^{n}P_j\left(u_{j(l_j)}^{\lambda_{j(l_j)}}\right)\to \max \qquad (17)$$

при наличии ограничений (18), где наличие в варианте системы по (19) переменной $u_{j(l_j)}^{\lambda_{j(l_j)}} \in U''_j$ означает, что в выбранном варианте системы в j-й подсистеме в качестве основного и резервных элементов выбраны элементы l_j-го типа и выбранная кратность резервирования равна

$\lambda_{j(l_j)}$, причем $\lambda^{**}_{j(l_j)} \le \lambda_{j(l_j)} \le \lambda^{*}_{j(l_j)}$,

$$g_p(v) = \sum_{j=1}^{n} g_p\left(u_{j(l_j)}^{\lambda_{j(l_j)}}\right) \le g_p^* \quad (p = 1, \ldots, q),$$

$$g_p(v) = \sum_{j=1}^{n} g_p\left(u_{j(l_j)}^{\lambda_{j(l_j)}}\right) \ge g_p^* \quad (p = q+1, \ldots, Q), \tag{18}$$

$$v \in V'' = \prod_{j=1}^{n} U''_j, \quad u_{j(l_j)}^{\lambda_{j(l_j)}} \in U''_j \quad (j = 1, \ldots, n),$$

$$v = \left(u_{1(l_1)}^{\lambda_{1(l_1)}}, \ldots, u_{j(l_j)}^{\lambda_{j(l_j)}}, \ldots, u_{n(l_n)}^{\lambda_{n(l_n)}}\right). \tag{19}$$

В ограничениях (18) слагаемые в левых частях, определяющие значение *p*-го ограничивающего фактора для *j*-й подсистемы (для основного и резервных элементов), перепишутся следующим образом

$$g_p\left(u_{j(l_j)}^{\lambda_{j(l_j)}}\right) = (\lambda_{j(l_j)} + 1) g_p(u_{j(l_j)}). \tag{20}$$

Вероятность безотказной работы *j*-й подсистемы в выражении (17) определяется в следующем виде

$$P_j\left(u_{j(l_j)}^{\lambda_{j(l_j)}}\right) = 1 - (1 - P_j(u_{j(l_j)}))^{\lambda_{j(l_j)}+1}. \tag{21}$$

Множество возможных вариантов технической реализации *j*-й подсистемы с резервированием имеет вид

$$U''_j = \left\{ \begin{matrix} u_{j(l_j)}^{\lambda_{j(l_j)}} \mid l_j = 1, \ldots, \xi'_j; \\ \lambda_{j(l_j)} = \lambda^{**}_{j(l_j)}, \ldots, \lambda^{*}_{j(l_j)} \end{matrix} \right\}; \tag{22}$$

$$(j = 1, \ldots, n);$$

число элементов в этом множестве

$$\left|U''_j\right| = \prod_{j=1}^{n} \sum_{l_j=1}^{\xi_j} (\lambda^{*}_{j(l_j)} - \lambda^{**}_{j(l_j)} + 2). \tag{23}$$

Задачу (17) – (18) перепишем следующим образом:
максимизировать

$$f(\overline{v}) = \sum_{j=1}^{n} f_j(\overline{u}_{j(t_j)}) \tag{24}$$

при условиях

$$\begin{gathered} g_p(\overline{v}) = \sum_{j=1}^{n} g_p(\overline{u}_{j(t_j)}) \le g_p^* \quad (p = 1, \ldots, q), \\ g_p(\overline{v}) = \sum_{j=1}^{n} g_p(\overline{u}_{j(t_j)}) \ge g_p^* \quad (p = q+1, \ldots, Q), \\ \overline{v} \in \overline{V} = \prod_{j=1}^{n} \overline{U}_j, \quad \overline{u}_{j(t_j)} \in \overline{U}_j \quad (j = 1, \ldots, n), \end{gathered} \tag{25}$$

где $f(v) = \lg P(v)$; $\overline{U}_j = \left\{ \overline{u}_{j(t_j)} \mid t_j = 1, \ldots, \sum_{l_j=1}^{\xi_j} \left(\left| \lambda_{j(l_j)} \right| + 1 \right) \right\}$ – множество возможных вариантов j-й подсистемы; $\left|\overline{U}_j\right| = \left|U_j''\right|$; $\left|\overline{V}\right| = \left|V''\right|$.

Эта задача эквивалентна задаче (17), (18), поскольку логарифм является монотонным преобразованием.

Введение множеств $\overline{U}_j$ является просто результатом замены переменной $u_{j(l_j)}^{\lambda_{j(l_j)}}$ на $\overline{u}_{j(t_j)}$ с соответствующим изменением множества значений.

Таким образом, были рассмотрены основные этапы алгоритма синтеза системы управления режимами энергосистемы по критерию надежности при требуемом уровне кибербезопасности для заданных экономических показателей. В процессе преобразований получены и уточнены соотношения для минимальной и максимальной кратности резервирования элементов.

Выводы. Сформулированы актуальные проблемы в области кибербезопасности электроэнергетических объектов, что становится важным в связи с появлением принципиально новых – цифровых подстанций. В свете дальнейшей реализации концепций SmartGrid и сетецентрического управления, значение обозначенных проблем существенно возрастает при появлении виртуальных электростанций.

Среди аппаратных решений, обеспечивающих киберзащиту

современных энергосистем, предложено для их инфраструктуры управления вводить резервирование ключевых элементов с целью повышения надежности и тем самым, обеспечения необходимого уровня кибербезопасности.

В качестве реализации указанных решений используется алгоритм синтеза системы управления режимами энергосистемы по критерию надежности при требуемом уровне кибербезопасности для заданных экономических показателей.

Основные результаты исследований показывают, что задача синтеза системы управления режимами энергосистемы по критерию надежности имеет экстремум, математическая модель задачи учитывает параллельное резервирование и эквивалентна задаче нахождения максимума логарифмической функции. Таким образом, может быть получен требуемый уровень кибербезопасности. Доказана справедливость предложенных соотношений для максимальной и минимальной кратности резервирования. Эти соотношения уточнены для случаев наличия и отсутствия ограничений на минимально допустимые значения вероятностей безотказной работы элементов энергосистемы. Также предложена процедура последовательного отсева элементов, которые учитывать в дальнейшем нет необходимости.

Список литературы: **1.** *Воропай Н.И.* Интегрированные интеллектуальные энергетические системы / *Н.И. Воропай, В.А. Стенников* // Известия РАН. Энергетика, 2014. – № 1. – С. 64-73. **2.** *Кобец Б.Б.* Инновационное развитие электроэнергетики на базе концепции Smart Grid / *Б.Б. Кобец, И.О. Волкова.* – М.: ИАЦ Энергия, 2010. – 208 с. **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.** *Осак А.Б.* Влияние человеческого фактора при обеспечении кибербезопасности на надежность объектов электроэнергетики и живучесть электроэнергетических систем / *А.Б. Осак, Е.Я. Бузина* // Институт систем энергетики им. Л. А. Мелентьева СО РАН. – 2015. – № 12-2. – С. 174-179. **5.** *Массель Л.В.* Киберопасность как одна из стратегических угроз энергетической безопасности России / *Л.В. Массель, Н.И. Воропай, С.М. Сендеров* // Вопросы кибербезопасности. – 2016. – № 4 (17). – С. 2-10. **6.** *Безкоровайный М.М.* Кибербезопасность – подходы к определению понятия / *М.М. Безкоровайный, А.Л. Татузов* // Вопросы кибербезопасности. – 2014. – № 1 (2). – С. 22-27. **7.** *Shvets S.V.* The development of the theory of instantaneous power of three-phase network in terms of network centrism / *Y.I. Sokol, O.G. Gryb, S.V. Shvets,* [et al.] // Electrical engineering & electromechanics. – 2017. – №. 4. – P. 61-65. **8.** *Shvets S.V.* Network-centric technologies for control of three-phase network operation modes / *Y.I. Sokol, O.G. Gryb, S.V. Shvets,* [et al.] // Electrical engineering & electromechanics. – 2017. – №. 3. – P. 67-71. **9.** *Швець С.В.* Мережецентричні аспекти використання безпілотних літальних апаратів / *С.В. Швець, В.Г. Воропай* // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Технічні науки. Випуск 176 "Проблеми енергозабезпечення та енергозбереження в АПК України". – Харків: ХНТУСГ, 2016. – С. 33-34. **10.** *Осак А.Б.* Кибербезопасность объектов электроэнергетики. Угрозы и возможные

последствия / *А.Б. Осак, Д.А. Панасецкий, Е.Я. Бузина* // Сборник докладов XXII конференции "Релейная защита и автоматика энергосистем". – Москва. – 2014. – С. 417-423.

References:

1. Voropaj, N.I., and Stennikov, V.A. (2014), "Integrated intelligent power systems", *Proceedings of the Russian Academy of Sciences. Power Engineering,* No. 1, pp.64-73.
2. Kobets, B.B., and Volkova, I.O. (2010), *Innovative development of electric power industry on the basis of the concept Smart Grid*, IAC Energy, Moscow, 208 p.
3. Markov, A.S., Rautkin, Yu.V., and Fadin, A.A. (2013), "Corporate information systems for managing information security events", *Proceedings of the XVIII Baikal All-Russian Conference,* Irkutsk, pp. 412-416.
4. Osak, A.B., and Buzina, E.Ya. (2015), "Influence of the human factor while ensuring cybersecurity on the reliability of electric power facilities and the survivability of electric power systems", *Institute of Power Systems. L. A. Melentieva, SB RAS*, No. 12-2, pp. 174-179.
5. Massel, L.V., Voropai, N.I., and Senderov, S.M., (2016), "Cyber security as one of the strategic threats to Russia's energy security", *Cybersecurity issues*, No.4 (17), pp. 2-10.
6. Bezkorovainiy, M.M., and Tatuzov, A.L., (2014), "Cybersecurity-approaches to the definition of the concept", *Cybersecurity issues*, No. 1 (2), pp. 22-27.
7. Shvets, S.V., Sokol, Y.I. , Gryb, O.G., Sirotin, Yu.O., Iierusalimova, T.S., and Gapon, D.A. (2017), "The development of the theory of instantaneous power of three-phase network in terms of network centrism", *Electrical engineering & electromechanics,* No. 4, pp. 61-65.
8. Shvets, S.V., Sokol, Y.I., Gryb, O.G., Sirotin, Yu.O., Iierusalimova, T.S., and Gapon D.A. (2017), "Network-centric technologies for control of three-phase network operation modes", *Electrical engineering & electromechanics*, No. 3, pp. 67-71.
9. Shvets, S.V., and Voropaj, V.G. (2016), "Network-centric aspects of the use of unmanned aerial vehicles", *Bulletin of the Kharkov National Technical University of Agriculture named after Petr Vasilenko. Technical sciences*, No.176 *"Problems of energy supply and energy saving in the agroindustrial complex of Ukraine"*, pp. 33-34.
10. Osak, A.B., Panasetsky, D.A., and Buzina, E.Ya. (2014), "Cybersecurity of electric power facilities. Threats and possible consequences", *Collection of reports of the XXII conference "Relay Protection and Automation of Power Systems"*, Moskow, 2014, pp. 417-423.

Статью представил д-р техн. наук, проф., профессор кафедры "Автоматизации и кибербезопасности энергосистем" НТУ "ХПИ" Сендерович Г.А.

Поступила (received) 28.11.2017

Gryb Oleg, Dr. Sci. Tech, Professor
National Technical University "Kharkiv Polytechnic Institute"
Str. Kirpicheva, 2, Kharkov, Ukraine, 61002
Tel.: (050) 139-24-39, e-mail: oleg47gryb@gmail.com
ORCID ID: 0000-0003-4758-8350

Shvets Sergey, Cand. Sci. Tech, Associate Professor
National Technical University "Kharkiv Polytechnic Institute"
Str. Kirpicheva, 2, Kharkov, Ukraine, 61002
Tel.: (067) 768-08-38, e-mail: se55sh32@gmail.com
ORCID ID: 0000-0002-3716-141X

Bortnikov Alexander, Postgraduate Student
National Technical University "Kharkiv Polytechnic Institute"
Str. Kirpicheva, 2, Kharkov, Ukraine, 61002
Tel.: (067)-900-76-48, e-mail: a42km@ya.ru
ORCID ID: 0000-0002-5235-499X

УДК 004.032

Синтез елементів енергосистеми за критерієм надійності в умовах кібербезпеки / Гриб О.Г., Швець С.В., Бортніков О.В. // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2017. – № 50 (1271). – С. 97 – 110.

Серед апаратних рішень кіберзахисту сучасних енергосистем запропоновано в їх інфраструктурі управління вводити резервування ключових елементів для підвищення надійності і тим самим, забезпечення необхідного рівня кібербезпеки. Отримані співвідношення кратності резервування елементів для випадків наявності і відсутності обмежень на мінімально допустимі значення ймовірностей їх безвідмовної роботи. Бібліогр.: 10 назв.

Ключові слова: енергосистема; резервування; надійність; кібербезпека; інфраструктура управління.

УДК 004.032

Синтез элементов энергосистемы по критерию надежности в условиях кибербезопасности / Гриб О.Г., Швец С.В., Бортников А.В. // Вестник НТУ "ХПИ". Серия: Информатика и моделирование. – Харьков: НТУ "ХПИ". – 2017. – № 50 (1271). – С. 97 – 110.

Среди аппаратных решений киберзащиты современных энергосистем предложено в их инфраструктуре управления вводить резервирование ключевых элементов для повышения надежности и тем самым, обеспечения необходимого уровня кибербезопасности. Получены соотношения кратности резервирования элементов для случаев наличия и отсутствия ограничений на минимально допустимые значения вероятностей их безотказной работы. Библиогр.: 10 назв.

Ключевые слова: энергосистема; резервирование; надежность; кибербезопасность; инфрастукрута управления.

UDC 004.032

Synthesis of power system elements by the criterion of reliability in conditions of cybersecurity / Gryb O.G. , Shvets S.V. , Bortnikov A.V. // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2017. – №. 50 (1271). – P. 97 – 110.

Among the hardware solutions for cybersecurity of modern power systems, it is proposed in their management infrastructure to introduce redundancy of key elements to increase reliability and thereby ensure the necessary level of cybersecurity. We have obtained the ratio of the multiplicity of the reservation of elements for the cases of presence and absence of restrictions on the minimum permissible values of the probabilities of their trouble-free operation. Refs.: 10 titles.

Keywords: power system; redundancy; reliability; cybersecurity; management infrastructure.