НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2023 Том 23 № 6 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2023 Vol. 23 No 6 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2023-23-6-1233-1241
УДК 001.8; 004.6

Методы бесконтактной регистрации информационных сигналов для аудита информационной безопасности систем и сетей электроснабжения

Алексей Юрьевич Гришенцев[1]✉, Сергей Аркадьевич Арустамов[2], Николай Сергеевич Кармановский[3], Вячеслав Александрович Горошков[4], Роман Ильич Чернов[5]

[1,2,3,4,5] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] AGrishentsev@yandex.ru✉, https://orcid.org/0000-0003-1373-0670
[2] sergey.arustamov@gmail.com, https://orcid.org/0000-0002-7520-8987
[3] karmanov50@mail.ru, https://orcid.org/0000-0002-0533-9893
[4] gorosvia@ya.ru, https://orcid.org/0000-0001-9950-5778
[5] aeijo@mail.ru, https://orcid.org/0000-0001-9361-1238

Аннотация

Введение. Известно, что в системах и сетях электроснабжения присутствует информационный сигнал. Наличие информационных сигналов в силовых элементах систем и сетей электроснабжения (электротехнического сигнала) в совокупности с другой информацией позволяет извлекать вторичную информацию из систем и сетей электроснабжения. В некоторых случаях информация такого рода является конфиденциальной, имеет высокий уровень значимости, а объекты электроснабжения могут относиться к объектам критической информационной инфраструктуры. Таким образом, аудит и обеспечение информационной безопасности систем и сетей электроснабжения представляются актуальными. В этой связи важными являются вопросы выявления ранее не учтенных каналов возможной утечки конфиденциальной информации, разработки методов бесконтактного мониторинга информационной безопасности объектов генерации, транспортировки, трансформации и потребления электроэнергии. **Метод.** Предложен метод решения обратной задачи вычисления токов многопроводных длинных линий на основании бесконтактного измерения магнитного поля токов с учетом принципа наложения. Для реализации метода в применении к Q-проводной линии требуется одновременное измерение магнитного поля в Q различных точках с известными координатами. Также требуется знание координат проводов длинной линии. Геометрические измерения предлагается реализовывать с помощью лазерных дальномеров или сканеров. При измерении магнитного поля длинной линии учитывается квазипостоянная составляющая магнитного поля Земли. Предложен метод определения направления и задержки отражения бегущих волн в длинной линии на основании информации с двух датчиков магнитного поля, размещенных на достаточном расстоянии друг от друга вдоль линии. **Основные результаты.** Предложены методы обеспечения аудита и мониторинга состояния систем и сетей электроснабжения, находящихся под воздействием угроз нарушения информационной безопасности. Выполнено математическое моделирование предложенного метода бесконтактного измерения тока в длинной линии и натурные эксперименты измерения тока в длинной линии и регистрации бегущих волн. Результаты экспериментов показали точность предлагаемых методов достаточную для решения поставленных задач. **Обсуждение.** Работа развивает представление о методах и средствах обеспечения аудита и мониторинга информационной безопасности электрических систем и сетей. Результаты работы позволяют выявлять новые, ранее не учтенные каналы утечки информации и разрабатывать новые бесконтактные методы регистрации информационных сигналов в линиях электропередачи.

Ключевые слова

информационная безопасность, электрические системы и сети, аудит информационной безопасности

Ссылка для цитирования: Гришенцев А.Ю., Арустамов С.А., Кармановский Н.С., Горошков В.А., Чернов Р.И. Методы бесконтактной регистрации информационных сигналов для аудита информационной безопасности систем и сетей электроснабжения // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23, № 6. С. 1233–1241. doi: 10.17586/2226-1494-2023-23-6-1233-1241

Methods of contactless registration of information signals for the audit of information security of power supply systems and networks

Alexey Yu. Grishentsev[1]✉, Sergey A. Arustamov[2], Nikolay S. Karmanovsky[3], Vyacheslav A. Goroshkov[4], Roman I. Chernov[5]

[1,2,3,4,5] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] AGrishentsev@yandex.ru✉, https://orcid.org/0000-0003-1373-0670
[2] sergey.arustamov@gmail.com, https://orcid.org/0000-0002-7520-8987
[3] karmanov50@mail.ru, https://orcid.org/0000-0002-0533-9893
[4] gorosvia@ya.ru, https://orcid.org/0000-0001-9950-5778
[5] aeijo@mail.ru, https://orcid.org/0000-0001-9361-1238

Abstract

It is known that there is an information signal in power supply systems and networks. The presence of information signals in the power elements of power supply systems and networks (electrical signal) in combination with other information allows extracting secondary information from power supply systems and networks. In some cases, this kind of information is confidential, has a high level of significance, and power supply facilities may belong to critical information infrastructure facilities. Thus, auditing and ensuring information security of power supply systems and networks seem relevant. In this regard, the issues of identifying previously unaccounted for channels of possible leakage of confidential information, developing methods for contactless monitoring of information security of generation, transportation, transformation and electricity consumption facilities are important. A contactless method for recording and calculating spurious emissions in established operating modes and during transients in long lines is proposed by solving the inverse problem of calculating the currents of multi-wire long lines based on measuring their magnetic field, taking into account the principle of superposition. To implement the method in application to a Q-wire line, simultaneous measurement of the magnetic field at Q different points with known coordinates is required. It also requires knowledge of the coordinates of the wires with the length of the line. Geometric measurements are proposed to be implemented using laser rangefinders or scanners. When measuring the magnetic field of a long line, the quasi-constant component of the Earth's magnetic field is taken into account. A method is proposed for determining the direction and delay of reflection of traveling waves in a long line, based on information from two magnetic field sensors located at a sufficient distance from each other along the line. Methods are proposed to ensure the audit and monitoring of the state of power supply systems and networks that are under the influence of threats to information security violations. Mathematical modeling of the proposed method of contactless current measurement in a long line and field experiments of current measurement in a long line and registration of traveling waves are performed. The experimental results show the accuracy of the proposed methods sufficient to solve the tasks. The work develops an idea of methods and means of ensuring audit and monitoring of information security of electrical systems and networks. The results of the work make it possible to identify new, previously unaccounted for channels of information leakage and to develop new contactless methods for registering information signals in power transmission lines.

Keywords

information security, electrical systems and networks, information security audit

For citation: Grishentsev A.Yu., Arustamov S.A., Karmanovsky N.S., Goroshkov V.A., Chernov R.I. Methods of contactless registration of information signals for the audit of information security of power supply systems and networks. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2023, vol. 23, no. 6, pp. 1233–1241 (in Russian). doi: 10.17586/2226-1494-2023-23-6-1233-1241

Введение

В ряде исследований [1, 2] показано, что в системах и сетях электроснабжения присутствует информационный сигнал, названный низкоэнтропийным. Низкоэнтропийный сигнал определяется как сигнал, зависящий от времени и имеющий малое значение статистического показателя — коэффициента вариабельности [1]. Источником низкоэнтропийного сигнала являются генераторы электрических мощностей. Кроме низкоэнтропийного сигнала, характерного для устоявшихся режимов работы электрических систем и сетей, в них периодически присутствуют сигналы с высокой энтропией, свойственные переходным процессам, в результате собственных (коммутации в электросети) и внешних (в виде молниевых разрядов в элементы электросети) воздействий. Наведенные токи и соответствующие им сигналы также могут вызывать магнитные бури [3]. Совокупность всех информационных сигналов, присутствующих в электрических сетях, предлагается называть электротехническими сигналами [1].

Наличие информационных сигналов в силовых элементах систем и сетей электроснабжения дает право уточнить название таких энергетических сетей, называя их энергоинформационными.

Электротехнический сигнал является источником следующей информации, которую будем называть первичной:

— качество и соответствие требованиям стандартов сети по частоте, амплитуде и форме (числу и распределению гармонических компонент в составе спектра сигнала), разности фаз тока и напряжения, разности фаз в фазных проводниках;
— передаваемые и потребляемые мощности;
— расписание и энергетические режимы работы систем генерации, передачи, трансформации и потребления электрических мощностей;
— наличие неоднородностей длинных линий, обусловленных несогласованностью волновых, нагрузоч-

ных сопротивлений и сопротивлений генерирующих источников;
— направление распространения бегущих волн, коэффициенты затухания и фазы, удаленность от места измерения точек отражения и переотражения бегущих волн.

Анализ электротехнического сигнала в совокупности с информацией о виде и назначении промышленных потребителей, типе электрических станций, подстанций трансформации и пр., позволяет извлекать вторичную информацию из систем и сетей электроснабжения, например, о режимах работы, генерируемых, потребляемых, трансформируемых и/или передаваемых мощностях, значимости тех или иных элементов и узлов систем электроснабжения для хозяйственной деятельности и обороноспособности. В некоторых случаях информация такого рода является конфиденциальной, имеет высокий уровень значимости, а объекты, с электроснабжением которых связан электротехнический сигнал, могут относиться к объектам критической информационной инфраструктуры[1] (КИИ).

Вследствие того, что в силовых узлах систем и сетей электроснабжения циркулируют значительные токи при высоких уровнях напряжений, часть перечисленной информации можно извлечь бесконтактно, на удаленном расстоянии от силовых токоведущих элементов за счет возбуждаемого электромагнитного поля. Значительные масштабы распределенных систем и сетей электроснабжения способствуют их демаскировке и позволяют получать информацию визуально. Так, например, в случае использования воздушных линий электропередачи (ЛЭП) напряжение передаваемой электроэнергии можно достаточно точно определить по типу и числу изоляторов в гирлянде, типу используемой линейной арматуры, наличию и числу жил в расщепленном проводе, типу опор, расстоянию между фазными проводами [4]. Картирование ЛЭП позволяет делать обоснованные предположения и выводы о территориальном расположении потребителей и источников электроэнергии, наличии резервирования питания и пр. Подобная информация может иметь особенное значение в период вероятного физического воздействия на элементы и узлы систем и сетей электроснабжения, например, в критических ситуациях, связанных с их целенаправленным выводом из строя.

В результате анализа работ [5–7] можно сделать вывод о значимости мониторинга, аудита и обеспечения информационной безопасности (ИБ) электрических систем и сетей.

В настоящей работе рассмотрены вопросы разработки методов бесконтактного мониторинга и выявления ранее не учтенных каналов возможной утечки конфиденциальной информации для повышения ИБ объектов генерации, транспортировки, трансформации и потребления электроэнергии как элементов и узлов электрических систем и сетей.

[1] Методические рекомендации по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса. М.: ФСТЭК России и Минэнерго России, 2019. 39 с.

Этапы аудита и мониторинга информационной безопасности систем и сетей электроснабжения

На сегодняшний день существует несколько определений термина аудит в контексте ИБ. Например, в работе [8] выполнен сравнительный анализ четырех[2] определений [9–10], на основании которого отдано обоснованное предпочтение следующему определению (ИСО 19011-2011): «*Аудит информационной безопасности* — систематический, независимый и документируемый процесс получения оценок состояния ИБ объекта аудита и объективного их оценивания с целью установления степени соответствия критериям аудита». В новой редакции стандарта[3] определение понятия аудит следующее: «*Аудит* — систематический, независимый и документированный процесс установления объективного свидетельства и его объективного оценивания для получения степени соответствия критериям аудита».

Современные системы и сети электроснабжения имеют развитую распределенную структуру и управляются административными субъектами генерации, транспорта, трансформации и поставки электроэнергии конечному потребителю. Мониторинг и управление электрическими сетями проводится за счет слаботочных проводных сетей и радиоканалов информационно-управляющих сетей. Значительная часть управляющих воздействий в электросетях осуществляется техническим персоналом.

Аудит и мониторинг ИБ производятся на основании технического задания. Предлагаемая последовательность аудита ИБ систем и сетей электроснабжения приведена на рис. 1.

С учетом рассмотренных потенциальных каналов утечки информации из сильноточных цепей систем электроснабжения определим базовые группы потенциальных объектов атак и потенциальных каналов утечки информации.

После сбора данных первичного анализа результатов аудита ИБ систем и сетей электроснабжения производится их интегральная обработка и систематизация. Далее производится оценка ущерба в результате физических и информационных атак на объекты инфраструктуры электрических систем и выработка мер противодействия угрозам вероятных атак и на объекты инфраструктуры электрических систем и сетей. На заключительном этапе аудита формируется перечень предписаний и рекомендаций, направленных на повышение ИБ и снижение вероятности реализации угроз. При необходимости осуществляется мониторинг реализации предписаний и рекомендаций, направленных на повышение ИБ и снижение вероятности реализации угроз.

[2] Астахов А. Введение в аудит информационной безопасности. Global Trust Solutions [Электронный ресурс]. Режим доступа: https://globaltrust.ru/category/prezentaczii/page/7/, свободный. Яз. рус. (дата обращения: 10.10.2023).

[3] ГОСТ Р ИСО 19011-2021. Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента. Введен 07.01.2021. М.: Стандартинформ, 2021. 49 с.

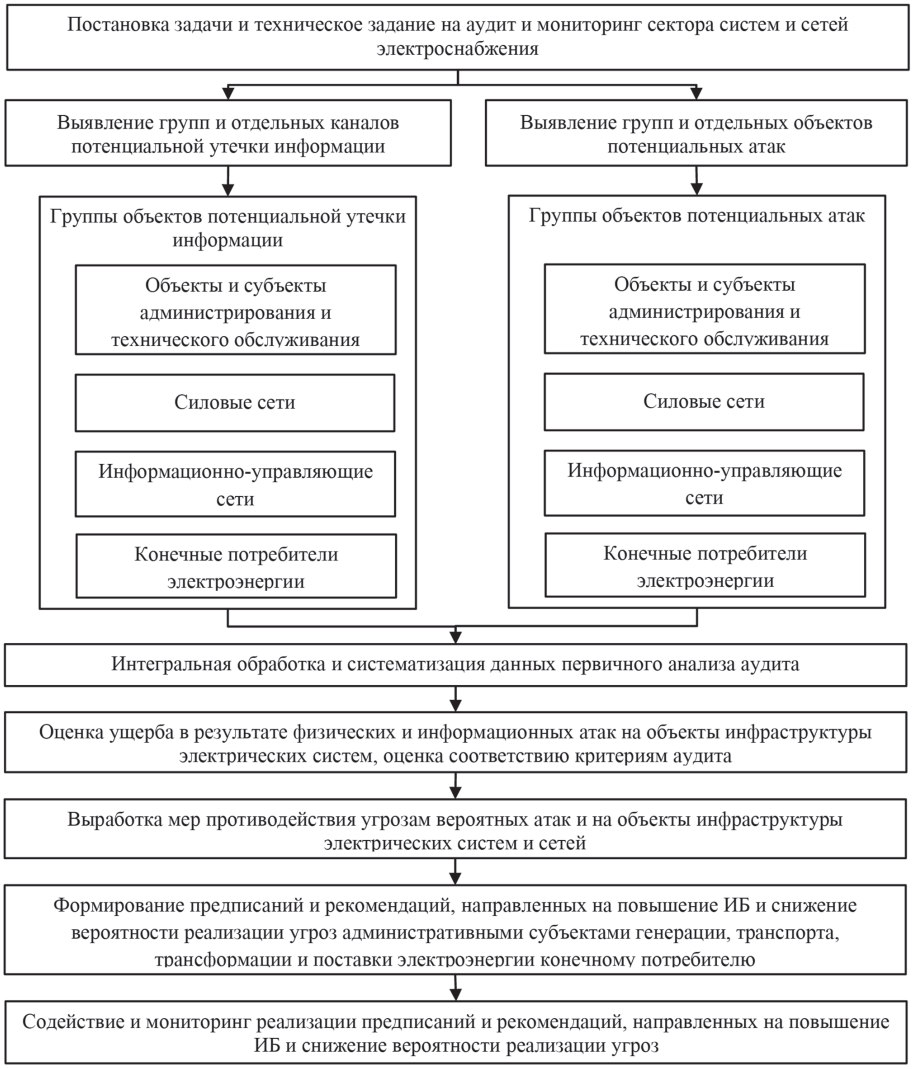

Рис. 1. Общая последовательность аудита информационной безопасности систем и сетей электроснабжения

Fig. 1. The general sequence of the audit of information security systems and power supply networks

Отметим, что технология аудита и мониторинга [11] информационно-управляющих сетей, действующих в составе систем и сетей электроснабжения мало чем отличается от аудита и мониторинга прочих информационно-управляющих сетей. Подобные задачи хорошо проработаны[1] и регламентированы[2], имеется достаточное число методов и средств подобного аудита [12–14]. Изучены вопросы аудита объектов и субъектов администрирования [9, 10] и технического обслуживания. Анализ уязвимостей ИБ высокочастотных сигналов, передающихся по силовым высоковольтным ЛЭП [15] и используемым для передачи сообщений телеметрии и диспетчерского управления электрическими системами и сетями также требует отдельного анализа, как с точки зрения ИБ, так и с учетом электромагнитной совместимости [16]. При этом низкочастотной электротехнический сигнал, имеющий значительную амплитуду, хорошо отделим от высокочастотного сигнала, имеющего обычно существенно меньшую амплитуду. В аспекте ИБ отдельного рассмотрения, выходящего за рамки настоящей работы, заслуживает внимания технология интеграции волоконно-оптического кабеля в проводники ЛЭП[3], обычно в грозозащитный провод.

Анализ проблемы ИБ показал, что еще недостаточно проработан вопрос обеспечения аудита и мониторинга силовых систем и сетей электроснабжения, действующих как под управлением энергетических предприятий и поставщиков электроэнергии, так и под управлением конечного потребителя. Остановимся далее на вопросе обеспечения и поддержке аудита и мониторинга силовых систем и сетей электроснабжения.

[1] Методический документ. Меры защиты информации в государственных информационных системах. М.: ФСТЭК России, 2014. 176 с.

[2] ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. Введен 01.01.2007. М.: Стандартинформ, 2006. 62 с.

[3] ВОЛС на воздушных линиях электропередачи [Электронный ресурс]. Режим доступа: https://www.ruscable.ru/article/vols_na_vozdushnykh_liniyakh_elektropere, свободный. Яз. рус. (дата обращения: 10.10.2023).

Методы детектирования электротехнического сигнала

Контактные методы регистрации электротехнического сигнала основаны на физическом подключении к силовым сетям. Применение контактных методов требует непосредственного доступа к элементам и узлам электрических систем и сетей, что является ограничивающим фактором, например, при необходимости проведения скрытого мониторинга и аудита. Для контактного мониторинга вполне применимы приборы, используемые при техническом мониторинге и обслуживании электрических сетей. После проверки корректности подключения и адекватности показаний для аудиторского мониторинга можно использовать штатные приборы, установленные в электрических системах и сетях.

Вместе с тем контактным методам измерений свойственны определенные недостатки. Существует необходимость доступа к силовым элементам и узлам электрических систем и сетей. Необходимо согласование выполнения измерений с административными и техническими службами электрических систем и сетей. Отсутствует возможность скрытых приборных измерений.

Бесконтактные методы основаны на существующей возможности удаленных измерений электротехнического сигнала, а значит, предоставляют возможности, недоступные контактным методам. К ним относится возможность проводить независимый аудит без согласования с административными и техническими службами электрических систем и сетей. Бесконтактные методы позволяют производить измерения на значительном удалении от силовых токоведущих элементов электрических систем и сетей.

Отметим, что большинство технических средств ИБ являются средствами двойного назначения. Они могут применяться для аудита и мониторинга ИБ, но также использоваться как средства информационной атаки для получения доступа к информации.

Бесконтактный дистанционный метод измерений токов в устоявшихся режимах работы и при переходных процессах. Вектор магнитной индукции от времени $\mathbf{B}_{q,p}(t)$ в точке с координатами (x_p, y_p) для уединенного провода с током $i_q(t)$ и координатами осевой линии (x_q, y_q) вычислим с помощью выражения [17]:

$$\mathbf{B}_{q,p}(t) = \mathbf{x}B_{q,p,x}(t) + \mathbf{y}B_{q,p,y}(t) = \\ = \mu i_q(t)\frac{\mathbf{x}\cos\theta_{q,p} + \mathbf{y}\sin\theta_{q,p}}{2\pi\left(\sqrt{(x_p - x_q)^2 + (y_p - y_q)^2}\right)}, \quad (1)$$

где $\mu = \mu_1\mu_0$ — абсолютная магнитная проницаемость среды; μ_1 — относительная магнитная проницаемость среды; μ_0 — магнитная постоянная; $q, p = 1, \ldots, Q$ — целочисленные индексы; $\theta_{q,p}$ — полярный угол, характеризующий положение (x_p, y_p) относительно (x_q, y_q), причем (x_q, y_q) принимается за точку, через которую проходит полярная ось; **x** и **y** — направляющие векторы по осям *Ox* и *Oy*.

Используя принцип наложения (суперпозиции), в случае *Q*-проводной ЛЭП, учитывая (1), получим выражение:

$$\mathbf{B}_p(t) = \sum_{q=1}^{Q} \mathbf{B}_{q,p}(t). \quad (2)$$

Используя выражение (2), предлагается метод решения следующей обратной задачи: при известном значении магнитной индукции $\mathbf{B}_p(t)$ в p — точках ($p, q = 1, \ldots, Q$), можно вычислить токи $i_q(t)$ в отдельных проводниках *Q*-проводной ЛЭП. Для решения обратной задачи запишем систему линейных алгебраических уравнений (СЛАУ) в матричном виде:

$$\mathbf{AI} = \mathbf{B}, \quad (3)$$

где $\mathbf{A} = (a_{q,p}) = \mu\dfrac{\mathbf{x}\cos\theta_{q,p} + \mathbf{y}\sin\theta_{q,p}}{2\pi\left(\sqrt{(x_p - x_q)^2 + (y_p - y_q)^2}\right)}$ — матрица коэффициентов СЛАУ; $\mathbf{B} = \mathbf{B}_p(t)$ — вектор магнитной индукции; $\mathbf{I} = i_q(t)$ — вектор токов в отдельных проводниках *Q*-проводной ЛЭП. Решением СЛАУ (3) будет: $\mathbf{I} = \mathbf{A}^{-1}\mathbf{B}$.

Для решения СЛАУ (3) и вычисления значений токов $i_q(t)$ в отдельных проводниках *Q*-проводной ЛЭП измерим вектора магнитной индукции $\mathbf{B}_p(t)$ в *Q* различных точках (x_p, y_p). Для вычисления элементов матрицы **A** измерим координату *Q* точек (x_p, y_p) и координату точек (x_q, y_q), через которые проходят *Q* проводники с токами $i_q(t)$. Произвести подобные измерения с достаточно высокой точностью возможно с помощью лазерного дальномера или системы лазерного сканирования. Определить напряжение в воздушной длинной линии можно по наличию и конфигурации расщепленного провода, по типу и числу изоляторов в гирлянде.

Следует отметить, что наличие магнитных неоднородностей среды, например расположение ЛЭП над поверхностью земли или воды, может значительно повлиять на форму магнитного поля, а значит, и на точность измерений. В таком случае необходимо внести поправки в значения магнитной индукции, которые можно определить с помощью моделирования картины поля, используя уравнения Лапласа. Дополнительно повысить точность измерения токов $i_q(t)$ в *Q* линиях проводников можно за счет учета квазистационарного вектора магнитной индукции магнитного поля Земли. При переменном электротехническом сигнале компонента магнитного поля Земли легко обнаружима как постоянная составляющая.

Предлагаемый метод эффективно применим в условиях, когда сигнал, за счет которого регистрируется магнитное поле ЛЭП, хорошо различим на фоне сигналов, генерируемых магнитным полем других источников. Для оценки дистанций, на которых применим метод, построены графики зависимости затухания магнитной индукции уединенного протяжного проводника с током от расстояния (r) для значений токов 10 А, 100 А, 1кА, 5 кА, 10 кА (рис. 2).

Бесконтактный дистанционный метод регистрации бегущих волн в длинной линии. Метод бесконтактного извлечения информации позволяет получить

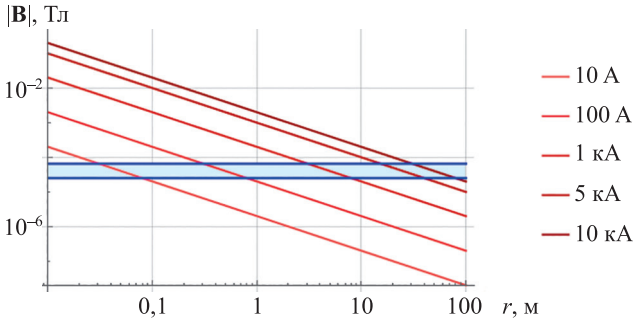

Рис. 2. Зависимость модуля индукции магнитного поля от расстояния для уединенного проводника круглого сечения с током. Синим цветом отмечена средняя интенсивность магнитного поля Земли, которая колеблется от 25 до 65 мкТл[1]

Fig. 2. The dependence of the magnetic field induction modulus on the distance for a solitary conductor of circular cross-section with a current. The average intensity of the Earth's magnetic field is marked in blue, which ranges from 25 to 65 μT[1]

сведения о направлении движения, скорости и амплитуде бегущей прямой и отраженной волн. Для определения абсолютных значений токов бегущих волн можно использовать метод, предложенный в подразделе «Бесконтактный дистанционный метод измерений токов в устоявшихся режимах работы и при переходных процессах». Метод основан на размещении двух датчиков *1*, *2* магнитного поля вдоль длинной линии, подключенных к общему самописцу *3* (рис. 3). В качестве датчиков предлагается использовать магнитные антенны, которые имеют достаточно высокую чувствительность и быстродействие.

Известно, что скорость волны в неискажающей однородной длинной линии $v = 1/\sqrt{LC}$, где L — погонная индуктивность длинной линии; C — погонная емкость длинной линии. При необходимости скорость распространения волны можно уточнить, зная расстояние между датчиками (рис. 3) или по справочникам первичных и вторичных характеристик длинной линии, предоставляемым с контактными рефлектометрами.

Распространение бегущих волн при переходных процессах происходит волновым пакетом, в результате которого датчики позволяют измерить групповую скорость волнового пакета. По направлению распространения падающей волны определяется направление к источнику волнового пакета. При регистрации отраженной волны по длительности задержки оценивается время распространения волны до места отражения. Источниками волновых пакетов могут быть коммутационные устройства и грозовые разряды.

Значительные габариты и пространственные масштабы систем и сетей электроснабжения позволяют извлекать дополнительную информацию с помощью непосредственного визуального наблюдения объектов электрических сетей и картирования с помощью

[1] Geomagnetism Frequently Asked Questions. National Centers for Environmental Information (NCEI). [Электронный ресурс]. Режим доступа: https://www.ncei.noaa.gov/products/geomagnetism-frequently-asked-questions, свободный. Яз. англ. (дата обращения: 08.10.2023).

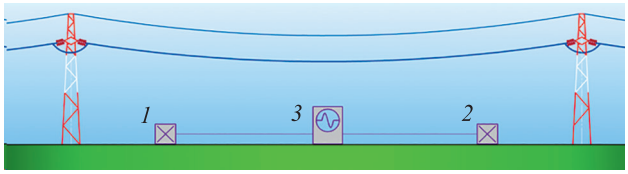

Рис. 3. Схема измерения бегущих волн в длинной линии: *1*, *2* — датчики магнитного поля; *3* — самописец

Fig. 3. Measuring circuit of traveling waves in a long line: *1*, *2* — magnetic field sensors, *3* — recorder

картографических сервисов, например, Google Maps[2], Яндекс карт[3] и пр. Особенно уязвимы к такому виду извлечения информации воздушные ЛЭП, открытые распределительные устройства и трансформаторные подстанции, крупные электростанции и потребители электроэнергии.

Результаты экспериментов

Численное моделирование и решения обратной задачи вычисления токов в длинной линии. Для проверки разработанных методов выполнено численное моделирование в программном пакете Wolfram Mathematica. Расчеты сопоставлены с результатами натурного эксперимента.

Расположение трех фаз проводников с токами $i_1(t)$, $i_2(t)$, $i_3(t)$ воздушной ЛЭП 110 кВ и датчиков D_1, D_2 и D_3 индукции магнитного поля показано на рис. 4. Шаг сетки на рисунке соответствует 1 метру. Каждый датчик регистрирует две компоненты магнитной индукции от времени — $B_x(t)$ и $B_y(t)$.

Моделирование выполнено в следующем порядке. Фазные токи приняты равными $i_1(t) = A_0\cos(2\pi ft)$, $i_2(t) = A_0\cos(2\pi ft + 2\pi/3)$, $i_3(t) = A_0\cos(2\pi ft + 4\pi/3)$, где $A_0 = 75$ А — амплитуда тока; $f = 50$ Гц — частота напряжения. В точках размещения датчиков в соответствии с (2) произведен расчет суммарного вектора магнитной индукции (от тока каждой фазы). К каждой компоненте вектора данных магнитной индукции $B_x(t)$ и $B_y(t)$ полученной с датчиков, добавлен случайный гауссов шум с

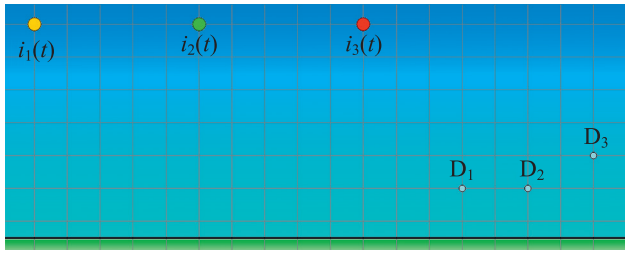

Рис. 4. Схема расположения трех фаз проводников воздушной линии электропередачи и датчиков индукции магнитного поля

Fig. 4. The location of the three phases of the air transmission line conductors and magnetic field induction sensors

[2] https://www.google.com/
[3] https://yandex.ru/maps

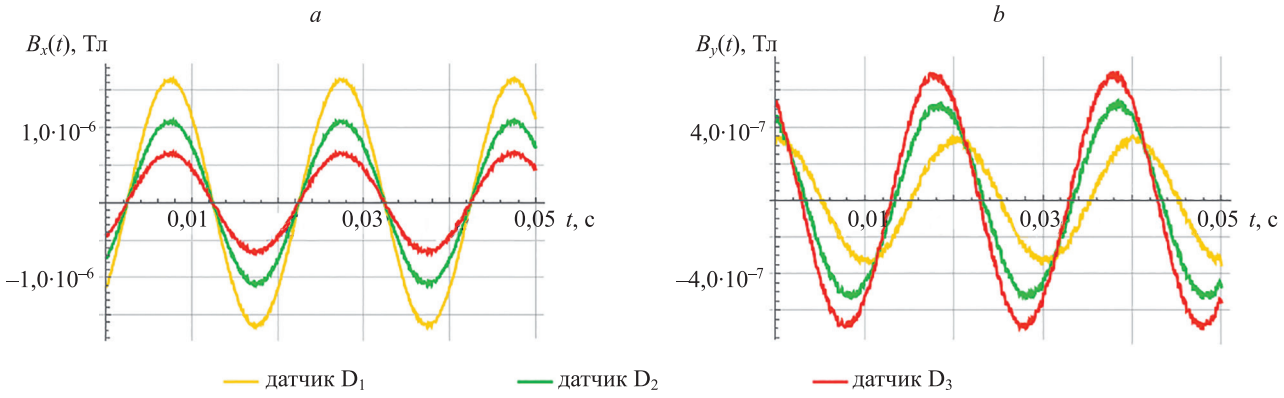

Рис. 5. Значения компонентов магнитной индукции $B_x(t)$ (*a*) и $B_y(t)$ (*b*) в точках расположения датчиков D_1, D_2 и D_3

Fig. 5. Values of magnetic induction components $B_x(t)$ (*a*) and $B_y(t)$ (*b*) at the locations of sensors D_1, D_2 and D_3

нулевым средним значением и спектральной плотностью шума $N_0 = 2\sigma^2 = 1{,}62\cdot10^{-9}$ Тл^2/Гц, σ — среднеквадратичное отклонение распределения гауссова шума. Полученные данные использованы для вычисления токов в фазных проводниках.

Расчетные значения магнитной индукции в точках расположения датчиков D_1, D_2 и D_3 приведены на рис. 5.

Решая системы уравнений (3) с использованием полученных данных, получим значения токов $i_1(t)$, $i_2(t)$, $i_3(t)$ в фазных проводниках воздушной ЛЭП (рис. 6).

По графикам (рис. 6) заметно, что фазовый ток $i_3(t)$ наименее зашумлен, так как датчики к нему расположены ближе, чем к другим проводникам. Наиболее зашумлен фазовый ток $i_1(t)$, так как датчики от проводника расположены на наибольшем удалении.

Измерение токов в длинной двухпроводной линии. На рис. 7 приведена схема двухпроводной линии с указанием расположения проводников с током $i_1(t) = -i_2(t) = i_л(t)$ и датчика Холла (D). Плоскость датчика Холла располагалась перпендикулярно вектору магнитной индукции. На практике положение, перпендикулярное вектору магнитной индукции, можно определить по максимуму амплитудных значений переменной компоненты показаний датчика.

Амплитудное значение сигнала с датчика Холла ($U_{дХ}$) составляет 2,75 В при постоянной составляющей на датчике, обусловленной индукцией магнитного поля Земли 1,49 В. Таким образом, амплитуда сигнала, обусловленная током в линии, составляет $U_{дХ}$ = 1,26 В, что соответствует модулю вектора магнитной индукции $|\mathbf{B}| \approx 0{,}2016$ мТл.

Учитывая (2), и что датчики расположены на одной оси вдоль двухпроводной линии, запишем выражение для мгновенного значения тока в линии

$$i_л(t) = 2\frac{\pi|\mathbf{B}|}{\mu_0}\left(\frac{\cos\theta_1}{\sqrt{\Delta x_1^2 + \Delta y_1^2}} + \frac{\cos\theta_2}{\sqrt{\Delta x_2^2 + \Delta y_2^2}}\right)^{-1}.$$

При заданных в эксперименте геометрических параметрах (рис. 7) $\Delta x_1 = \Delta x_2 = 1{,}5\cdot10^{-3}$ м, $\Delta y = 5\cdot10^{-3}$ м и $\theta_1 = \theta_2 \approx 0{,}287$ рад, получим значение действующего тока $I_д \approx 6{,}474$ А. При действующем значении напряжения в сети 220 В получим значение мощности $p \approx 1{,}42$ кВт. При этом фактическая мощность нагрузки составила 1,5 кВт. Таким образом, погрешность моделирования по данным экспериментальных измерений не превышает 5,3 %.

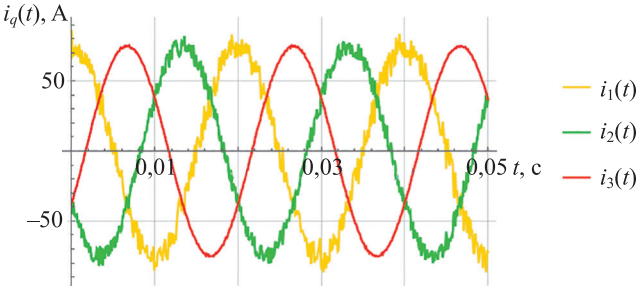

Рис. 6. Графики значений фазных токов в проводниках

Fig. 6. Graphs of current values in phase conductors

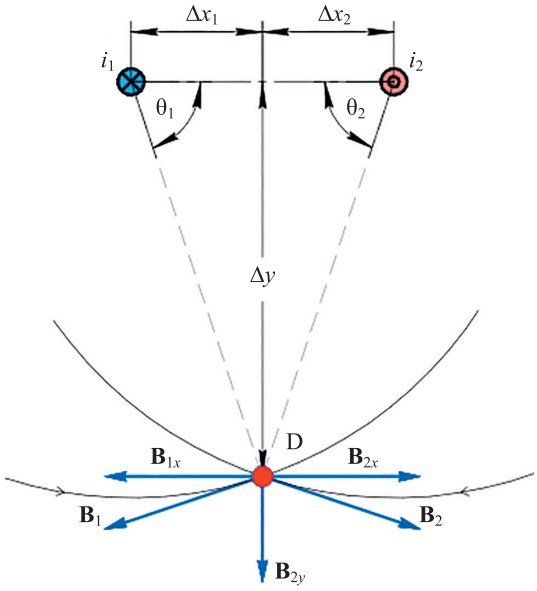

Рис. 7. Расположение точки измерений и конфигурации проводников длинной линии

Fig. 7. Location of the measurement point and configuration of line length conductors

Бесконтактная регистрация бегущих волн в длинной линии. В качестве регистратора использован осциллограф АКИП-4115/4А. В нагруженную активным сопротивлением 0,05 Ом линию подавался единичный импульс с амплитудой 15 В. Фактическая длина линии составила 33,2 м и была выполнена из двухпроводного кабеля ПВС. На рис. 8 приведена осциллограмма бегущих волн в длинной линии, полученная с помощью непосредственного (контрольного) измерения напряжения $u_{л}(t)$ и регистрации магнитной компоненты электромагнитного поля с помощью магнитной антенны $u_{ма}(t)$. Хорошо видно, что на осциллограмме напряжения $u_{л}(t)$ присутствуют первая прямая волна и две отраженные волны с измененными фазами на стороне приемника.

На осциллограмме $u_{ма}(t)$ видно, что инверсия сигнала на стороне приемника отсутствует, что характерно при включении нагрузки с малым сопротивлением и близко к режиму «короткого замыкания». Первичные и вторичные характеристики длинной линии можно вычислить, используя известные выражения [17, 18]. Скорость распространения фронта электромагнитной волны в линии составляет $v \approx 0{,}1526 \cdot 10^9$ м/с. Расчетная длина линии (в данном случае — расстояние от источника до нагрузки) при общем времени распространения прямой и обратной волны $T = 0{,}433 \cdot 10^{-6}$ с (по началу фронта волн), составляет $l_{лин} \approx 33{,}04$ м. Таким образом, ошибка оценки длины линии не превысила 0,5 %.

Предложенный метод регистрации бегущих волн в длинной линии с помощью двух разнесенных датчиков позволил измерить с высокой точностью скорость распространения волнового пакета, а значит, оценить значения запаздывания отраженных волн даже в случае, если свойства линии не известны, например, если проложен подземный кабель или кабель внутри зданий и сооружений, информация о типе которого неизвестна.

Результаты моделирования и натурных экспериментов показали, что предложенные методы бесконтактных измерений дают возможность достичь необходимую точность решения поставленной задачи приборного аудита и мониторинга ИБ силовых элементов и узлов электрических сетей.

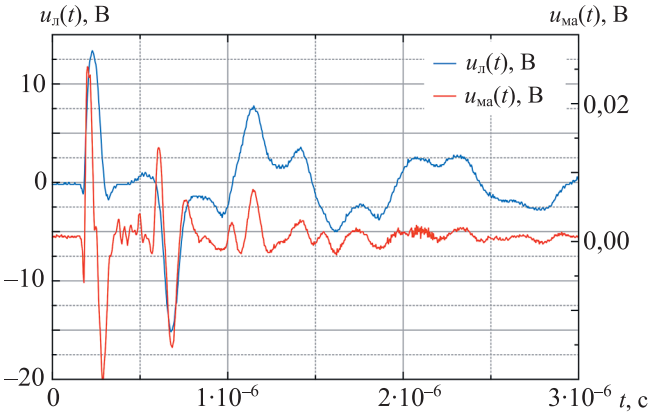

Рис. 8. Фактическое напряжение $u_{л}(t)$ в длинной линии и напряжение $u_{ма}(t)$ с датчика — магнитная антенна

Fig. 8. The actual voltage $u_{л}(t)$ in the long line and the voltage $u_{ма}(t)$ from the sensor — magnetic antenna

Заключение

Разработан бесконтактный метод измерений токов в устоявшихся режимах работы и при переходных процессах в длинных линиях за счет решения обратной задачи вычисления токов многопроводных длинных линий на основании измерения их магнитного поля с учетом принципа суперпозиции. Предложен бесконтактный метод измерения направления и задержки отражения бегущих волн в длинной линии. Показаны ранее не учтенные каналы утечки информации из электрических систем и сетей, а также способы их регистрации.

Литература

1. Коровкин Н.В., Грицутенко С.С. Введение понятия «низкоэнтропийный сигнал» // Электричество. 2020. № 10. С. 33–43. https://doi.org/10.24160/0013-5380-2020-10-33-43
2. Коровкин Н.В., Грицутенко С.С. О применимости быстрого преобразования Фурье для гармонического анализа несинусоидальных токов и напряжений // Известия Российской академии наук. Энергетика. 2017. № 2. С. 73–86.
3. Gaunt C.T. Reducing uncertainty — responses for electricity utilities to severe solar storms // Journal of Space Weather and Space Climate. 2014. V. 4. P. A01. https://doi.org/10.1051/swsc/2013058
4. Идельчик В.И. Электрические системы и сети. М.: Энергоатомиздат, 1989. 594 с.
5. Бурлов В.Г., Маньков В.Д., Полюхович М.А. Теоретические аспекты синтеза модели управления безопасностью электрических сетей с применением ГИС // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция. Материалы конференции. Ч. 2. СПб., 2020. С. 229–230.
6. Рушечников Я.И., Яновский А.В., Третьяков И.А. Программно-аппаратное обеспечение исследования электромагнитных излучений, создаваемых вычислительной техникой, в бытовой электрической сети // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2023. № 2. С. 75–84. https://doi.org/10.24143/2072-9502-2023-2-75-84

References

1. Korovkin N.V., Gritsutenko S.S. Introduction of the low-entropy signal concept. *Elektrichestvo*, 2020, no. 10, pp. 33–43. (in Russian). https://doi.org/10.24160/0013-5380-2020-10-33-43
2. Korovkin N.V., Gritsutenko S.S. About applicability of the fast fourier transform for a harmonic analisys of non sinusoidal currents and voltages. *Izvestija Rossijskoj akademii nauk. Jenergetika*, 2017, no. 2, pp. 73–86. (in Russian)
3. Gaunt C.T. Reducing uncertainty — responses for electricity utilities to severe solar storms. *Journal of Space Weather and Space Climate*, 2014, vol. 4, pp. A01. https://doi.org/10.1051/swsc/2013058
4. Idelchik V.I. *Electrical Systems and Networks*. Moscow, Jenergoatomizdat Publ., 1989, 594 p. (in Russian)
5. Burlov V., Mankov V., Polyukhovich M. Theoretical aspects of synthesis of the electric power networks safety management model using GIS. *Regional informatics (RI-2020). XVII St. Petersburg Internatonal Conference. Proceedings of the Conference. Part 2*. 2020, pp. 229–230. (in Russian)
6. Rushechnikov I.I., Ianovskii A.V., Tretiakov I.A. Software and hardware for studying electromagnetic radiation generated by computing equipment in household electric network. *Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics*, 2023, no. 2, pp. 75–84. (in Russian). https://doi.org/10.24143/2072-9502-2023-2-75-84

7. Осак А.Б., Бузина Е.Я. Анализ влияния киберуязвимостей систем релейной защиты, противоаварийной и режимной автоматики на надежность электро-снабжения потребителей в условиях цифровой трансформации электроэнергетики // Методические вопросы исследования надежности больших систем энергетики. Материалы 93-го заседания семинара. В 2-х кн. Книга 2. Иркутск, 2021. С. 310–319.
8. Макаренко С.И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1–29. https://doi.org/10.24411/2410-9916-2018-10101
9. Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Рудановский М.В. Аудит информационной безопасности органов исполнительной власти / 3-е изд., стереотип. М.: ООО «ФЛИНТА», 2011. 100 с.
10. Хомяков В.А. Аудит как метод модернизации системы обеспечения информационной безопасности // Экономический вестник Ярославского университета. 2013. № 29. С. 48–52.
11. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями: монография. СПб.: Наукоемкие технологии, 2018. 122 с.
12. Бойко А.А., Обущенко Е.Ю., Щеглов А.В. Особенности синтеза полного множества тестовых способов удаленного информационно-технического воздействия на пространственно распределенные системы информационно-технических средств // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2017. № 2. С. 33–45.
13. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. СПб: Университет ИТМО, 2018. 45 с.
14. Нырков А.П., Рудакова С.А. Методика аудита объектов информатизации по требованиям информационной безопасности // Журнал Университета водных коммуникаций. 2012. № 3. С. 146–149.
15. Аксенов И.И., Мба Э.К. Разработка системы мониторинга воздушных линий электропередачи 110 кВ // Энергоэффективность и энергосбережение в современном производстве и обществе: материалы международной научно-практической конференции. Ч. 1. 2022. С. 51–64.
16. Комаров С. Беда пришла, откуда не ждали... // Broadcasting. Телевидение и радиовещание. 2005. № 7. С. 71–72 [Электронный ресурс]. URL: http://lib.broadcasting.ru/articles2/Oborandteh/grief_came, свободный, Яз. рус. (дата обращения: 10.10.2023).
17. Демирчян К.С., Нейман Л.Р., Коровкин Н.В., Чечурин В.Л. Теоретические основы электротехники Т. 3 / 4-е изд. СПб.: Питер, 2006. 377 с.
18. Калантаров П.Л., Цейтлин Л.А. Расчёт индуктивностей: справочная книга / 3-е изд., перераб. и доп. Л.: Энергоатомиздат, 1986. 488 с.

7. Osak A.B., Buzina E.Y. Analysis of the cyber vulnerabilities impact of relay protection systems, emergency and regime automation on the reliability of consumers power supply in the context of the power industry digital transformation. *Methodological issues in researching the reliability of the large energy systems. Materials from the 93th seminar meeting*. Irkutsk, 2021, pp. 310–319. (in Russian)
8. Makarenko S.I. Audit of information security — the main stages, conceptual framework, classification of types. *Systems of Control, Communication and Security*, 2018, no. 1, pp. 1–29. (in Russian). https://doi.org/10.24411/2410-9916-2018-10101
9. Averchenkov V.I., Rytov M.Iu., Kuvyklin A.V., Rudanovskii M.V. *Information Security Audit of the Executive Authorities*. Moscow, FLINTA Publ., 2011, 100 p. (in Russian)
10. Homyakov V.A. Audit is as a method of modernization in provision system of information security. *Jekonomicheskij vestnik Jaroslavskogo universiteta*, 2013, no. 29, pp. 48–52. (in Russian)
11. Makarenko S.I. *Security Audit of the Critical Infrastructure Using Special Information Influences*. St. Petersburg, Naukoemkie tehnologii Publ., 2018, 122 p. (in Russian)
12. Boyko A.A., Obushenko E.Y., Shcheglov A.V. About synthesis of a full set of test methods of remote information-technical impacts on spatially distributed systems of information-technical tools. *Proceedings of Voronezh State University. Series: Systems Analysis and Information Technologies*, 2017, no. 2, pp. 33–45. (in Russian)
13. Begaev A.N., Begaev S.N., Fedotov V.A. *Penetration Testing*. St. Petersburg, ITMO University, 2018, 45 p. (in Russian)
14. Nyrkov A.P., Rudakova S.A. The technique of audit of information objects for information security requirements. *Zhurnal Universiteta vodnyh kommunikacij*, 2012, no. 3, pp. 146–149. (in Russian)
15. Aksenov I.I., Mbah E.Ch. Development of a 110 kV overhead transmission line monitoring system. *Energy efficiency and energy saving in the modern production and society: materials of the International Scientific and Practical Conference. Part. 1*, 2022, pp. 51–64. (in Russian)
16. Komarov S. The trouble has come from where it was not expected ... *Broadcasting*, 2005, no. 7, pp. 71–72. Available at: http://lib.broadcasting.ru/articles2/Oborandteh/grief_came. (accessed: 10.10.2023). (in Russian)
17. Demirchian K.S., Neiman L.R., Korovkin N.V., Chechurin V.L. *Theoretical Basics of Electrical Engineering. V. 3*. St. Petersburg, Piter Publ., 2006, 337 p. (in Russian)
18. Kalantarov P.L., Tceitlin L.A. *Inductance Calculation. Reference Book*. Leningrad, Jenergoatomizdat Publ., 1986, 488 p. (in Russian)

Авторы

Гришенцев Алексей Юрьевич — доктор технических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sc 56321138400, https://orcid.org/0000-0003-1373-0670, AGrishentsev@yandex.ru

Арустамов Сергей Аркадьевич — доктор технических наук, профессор, профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sc 59695216400, https://orcid.org/0000-0002-7520-8987, sergey.arustamov@gmail.com

Кармановский Николай Сергеевич — кандидат технических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sc 57192385103, https://orcid.org/0000-0002-0533-9893, karmanov50@mail.ru

Горошков Вячеслав Александрович — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0001-9950-5778, gorosvia@ya.ru

Чернов Роман Ильич — инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0001-9361-1238, aeijo@mail.ru

Authors

Alexey Yu. Grishentsev — D.Sc., Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, sc 56321138400, https://orcid.org/0000-0003-1373-0670, AGrishentsev@yandex.ru

Sergey A. Arustamov — D.Sc., Full Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, sc 59695216400, https://orcid.org/0000-0002-7520-8987, sergey.arustamov@gmail.com

Nikolay S. Karmanovsky — PhD, Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, sc 57192385103, https://orcid.org/0000-0002-0533-9893, karmanov50@mail.ru

Vyacheslav A. Goroshkov — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0001-9950-5778, gorosvia@ya.ru

Roman I. Chernov — Engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0001-9361-1238, aeijo@mail.ru

Статья поступила в редакцию 10.10.2023
Одобрена после рецензирования 06.11.2023
Принята к печати 25.11.2023

Received 10.10.2023
Approved after reviewing 06.11.2023
Accepted 25.11.2023