3. *Kutuzov O., Cekhanovskij V., Tatarnikova T*. Infokommunikacionnye sistemy i seti. SPb.: Lan', 2020.
4. *Odom U.* Cisco. Oficial'noe rukovodstvo po podgotovke k ekzamenam CCNA, ICND2 200-101. Marshrutizaciya i kommunikaciya. M.: Vil'yams, 2016.
5. *Olifer V.G., Olifer N.A*. Komp'yuternye seti. Principy, tekhnologii, protokoly. 5-e izd. SPb.: Piter, 2016.
6. *Robachevskij A*. Internet iznutri. Ekosistema global'noj seti. 2-e izd. M.: Al'pina Pablisher, 2017.
7. *Sergeev A.N.* Osnovy lokal'nyh komp'yuternyh setej. SPb.: Lan', 2016.
8. *Tengajkin E.* Organizaciya setevogo administrirovaniya. Setevye operacionnye sistemy, servery, sluzhby i protokoly. 3-e izd. SPb.: Lan', 2020.
9. *Tengajkin E.* Proektirovanie setevoj infrastruktury. Organizaciya, principy postroeniya i funkcionirovaniya. 3-e izd. SPb.: Lan', 2020.
10. *Hant K*. TCP/IP. Setevoe administrirovanie. 3-e izd. SPb.: Simvol-plyus, 2008.

DOI: 10.25586/RNU.V9187.20.04.P.113 УДК 004.7

Т.Е. Черницкая, С.И. Макаренко, Д.В. Растягаев

АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ОЦЕНКИ ИНТЕРОПЕРАБЕЛЬНОСТИ СЕТЕЦЕНТРИЧЕСКИХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ*

В условиях перехода информационно-управляющих систем к сетецентрической архитектуре и созданию сетецентрических информационно-управляющих систем (СЦИУС) возрастает актуальность обеспечения интероперабельности в таких системах. Предложен подход к оценке аспектов информационной безопасности в рамках разработки модели технической интероперабельности СЦИУС на основе ГОСТ Р 55062–2012. Показано, что аспекты технической интероперабельности в части информационной безопасности включают в себя параметры конфиденциальности, целостности, доступности, а также некоторые другие дополнительные параметры.
Ключевые слова: интероперабельность, сетецентрическая система управления, информационная система, информационная безопасность, аспекты, параметры.

T.E. Chernitskaya, S.I. Makarenko, D.V. Rastyagaev

ASPECTS OF INFORMATION ASSURANCE WITHIN NET-CENTRIC INFORMATION AND CONTROL SYSTEMS INTEROPERABILITY EVALUATION

In the situation of transition from information and control systems to a network-centric architecture and development of net-centric information and control system, the relevance of interoperability assurance in such systems is increasing. An approach to the assessment of information assurance capability is proposed as a part of developing a model of technical interoperability of network-centric information

* Данное исследование проводится в рамках проекта РФФИ № 19-07-00774.

and control system based on Russia's state standard no. 55062-2012. It is shown that capabilities of information assurance within technical interoperability include confidentiality, integrity and availability dimensions as well other minor dimensions.
Keywords: interoperability, net-centric control system, control system, automation, information assurance, capabilities, dimensions.

Введение

Особенностью развития систем управления организационными и техническими системами является переход их к сетецентрическим информационно-управляющим системам (СЦИУС). Ключевым принципом построения СЦИУС является интероперабельность. По определению, данному организациями по стандартизации [7; 17], «интероперабельность – способность двух или более информационных систем или компонентов к обмену информацией и к использованию информации, полученной в результате обмена».

В отечественной литературе большое число публикаций посвящено обсуждению принципов формирования СЦИУС, например работа [10], однако исследований по проблеме интероперабельности в СЦИУС несравнимо меньше. К основным работам по этой тематике стоит отнести работы [1; 2; 8; 11; 12; 13; 15]. При этом глубокое теоретическое исследование влияния аспектов информационной безопасности (ИБ) в рамках оценки технической интероперабельности СЦИУС в отечественной науке не проводилось.

В работе [2] обоснован вариант декомпозиции параметров интероперабельности в соответствии с ГОСТ Р 55062–2012 [7] на основании модели Systems, Capabilities, Operations, Programs, and Enterprises Model for Interoperability Assessment (SCOPE-модели) [22] с учетом ее адаптации к отечественному подходу оценки интероперабельности, представленному в стандарте. Это исследование продолжает и развивает ранее опубликованные работы авторов [1; 2; 8; 11; 12; 13; 15].

Далее рассмотрим параметры оценки аспектов ИБ, применимые к СЦИУС, более подробно.

Анализ существующих подходов и стандартов по категорированию параметров ИБ

Впервые категорирование инцидентов нарушения ИБ было предложено J.H. Saltzer и M.D. Schroeder в 1975 г. в работе [21]. В работе инциденты нарушения ИБ были разделены на три основных категории:

- несанкционированное раскрытие информации;
- несанкционированное изменение информации;
- отказ в доступе к информации.

Позднее эти категории нарушения отдельных свойств ИБ получили краткие наименования и стандартизированные определения, а также стали использоваться как основные параметры, характеризующие состояние ИБ [3; 14]:

- конфиденциальность (confidentiality) – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на это право;
- целостность (integrity) – состояние информации, при котором обеспечиваются ее достоверность и полнота. При этом под полнотой понимается состав и объем информа-

ции, достаточный для правильного понимания какого-либо явления или принятия решения, а под достоверностью – истинность и точность информации в описании какого-либо факта, события или явления;

• доступность (availability) – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа к информации, могут реализовывать их беспрепятственно.

В 1992 г. Организация экономического сотрудничества и развития предложила свою собственную модель ИБ [19], состоящую из девяти принципов обеспечения ИБ:

• осведомленность (awareness) – знание пользователя системы об имеющихся рисках нарушения безопасности и способах защиты информации в системе;

• ответственность (responsibility) – знание пользователя о разрешенных способах работы с информацией в системе и с последствиями нарушения разрешенных способов работы;

• противодействие (response) – оперативный сбор информации о случаях нарушения безопасности в системе и передача ее ответственным лицам для принятия адекватных мер защиты;

• этика (ethics) – понимание последствий любых действий, направленных на обработку информации в системе, в частности их степени влияния на работу других пользователей;

• демократия (democracy) – свойство политики безопасности системы, учитывающее право пользователя на свободу публикации информации и обмен ею с другими пользователями;

• оценка риска (risk assessment) – качественная и количественная оценка рисков нарушения безопасности, включающая в себя технический, физический и человеческий фактор;

• разработка и внедрение систем безопасности (security design and implementation) – разработка, внедрение и эксплуатация систем и сетей должна учитывать требования к информационной безопасности;

• управление безопасностью (security management) – управление безопасностью системы должно базироваться на анализе наиболее вероятных рисков, обладать свойствами гибкости и масштабируемости;

• пересмотр (reassessment) – своевременный учет новых угроз безопасности для формирования актуальных моделей угроз безопасности системы.

В 1998 г. в национальном стандарте США NIST SP 800-160 [18] общепризнанные основные параметры ИБ – конфиденциальность, целостность, доступность – были дополнены еще тремя параметрами:

• владение или контроль (possession or control) – свойство информации, состоящее в фактической реализации возможности пользователя распоряжаться и пользоваться информацией, а также проводить над ней санкционированные политикой безопасности операции;

• подлинность (authenticity) – достоверность утверждения происхождения или авторства информации;

• полезность (availability) – свойство информации быть использованной в интересах решения задач пользователя.

Эта модель получила название паркеровской гексады и до сих пор является предметом дискуссий среди специалистов по ИБ.

В 2011 г. международным консорциумом The Open Group опубликован стандарт управления ИБ O-ISM3, в котором сформирован выборочный подход к определению составляющих ИБ, основанный на классической триаде свойств «конфиденциальность – целостность – доступность». Согласно стандарту O-ISM3 для каждой организации можно идентифицировать индивидуальный набор целей ИБ, относящихся к одной из пяти категорий [20]:

- приоритетные цели безопасности;
- долгосрочные цели безопасности;
- цели качества информации;
- цели контроля доступа;
- технические цели безопасности.

В 2013 г. экспертами J. Hughes и G. Cybenko была предложена модель ИБ «Количественные показатели ИБ и оценка рисков. Три основополагающих принципа компьютерной безопасности» [16], которая в дополнение к вышеуказанным параметрам ИБ вводила следующие категории:

- подверженность системы риску (system susceptibility) – свойство, определяющее уязвимость системы и степень ее подверженности атакам;
- доступность уязвимости (threat accessibility) – свойство, определяющее возможность получения информации о наличии уязвимостей системы злоумышленником, а также доступа его к этим уязвимостям за счет непосредственного физического взаимодействия с системой либо удаленно – по сети;
- способность эксплуатировать уязвимость (threat capability) – свойство, определяющее способность злоумышленника использовать имеющиеся знания о системе и ее уязвимостях для реализации успешной атаки на нее.

Наиболее признанной и распространенной в руководящих документах общемирового и государственного уровня остается триада «конфиденциальность – целостность – доступность», которая в некоторой литературе сокращается как «КЦД». Именно такая модель ИБ используется в государственных стандартах. Тем не менее профессиональное сообщество настаивает на том, что данная модель устарела и более не удовлетворяет современным требованиям. Так, в стандарте ГОСТ Р ИСО/МЭК 27000–2012 [4] утверждены следующие дополнительные требования, предъявляемые к свойствам ИБ:

- аутентифицированность (authentication) – свойство, гарантирующее, что заявленные характеристики объекта являются подлинными;
- подлинность (authenticity) – свойство, гарантирующее, что субъект или ресурс идентичны заявленному;
- подотчетность (accountability) – ответственность субъекта за его действия и решения;
- невозможность отказа (non-repudiation) – способность информации удостоверять имевшее место событие или действие и их субъектов так, чтобы это событие или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение;
- достоверность (reliability) – свойство соответствия предусмотренному поведению и результатам.

Разобщенность взглядов на состав свойств, параметров и категорий ИБ привела к отсутствию утвержденных стандартов категорирования, качественного и количественного оценивания свойств ИБ. Между тем разработка единых требований по оцениваемым свойства ИБ, а также их показателям и критериям оценки в составе отечественной модели интероперабельности является одной из ключевых задач формирования соответствующих руководящих документов.

Предложения по составу параметров, определяющих аспекты информационной безопасности в рамках оценки интероперабельности сетецентрических информационно-управляющих систем

Для количественной оценки аспектов ИБ в рамках оценки технической интероперабельности СЦИУС предлагается следующее множество параметров.

Основные параметры ИБ:

- безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность [6];
- конфиденциальность информации – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на это право [14];
- доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа к информации, могут реализовывать их беспрепятственно [14];
- целостность информации – состояние информации, при котором обеспечиваются ее достоверность и полнота [3].

Дополнительные параметры ИБ:

- полнота информации – состав и объем информации, достаточный для правильного понимания какого-либо явления или принятия решения [9];
- достоверность информации – истинность и точность информации в описании какого-либо факта, события или явления [9];
- подлинность информации – достоверность утверждения о происхождении или авторстве информации;
- полезность информации – свойство информации быть использованной в интересах решения задач пользователя;
- контроль информации – свойство информации, состоящее в фактической реализации возможности пользователя распоряжаться и пользоваться информацией, а также проводить над ней санкционированные политикой безопасности операции [18];
- учетность действий пользователей – свойство информации, обеспечивающее однозначное отслеживание собственных действий любого пользователя (субъекта) при доступе к информации и ее обработке [5].

Заключение

На основании вышеизложенного можно сделать следующие выводы.

1. Одной из основных составляющих технической интероперабельности СЦИУС является ИБ.

2. Для количественной оценки аспектов ИБ в рамках оценки технической интероперабельности СЦИУС предлагается использовать следующие основные параметры: без-

опасность информации, целостность информации, конфиденциальность информации, доступность информации.

3. Для более «тонкой» оценки аспектов ИБ в рамках оценки технической интероперабельности СЦИУС предлагается использовать следующие дополнительные параметры: полнота информации, достоверность информации, подлинность информации, полезность информации, контроль информации, учетность пользователей.

4. Предлагаемые параметры оценки аспектов ИБ предполагается в дальнейшем использовать при разработке итогового документа «Модели для построения и оценки интероперабельности сетецентрических управляющих систем» как одного из основных результатов проекта РФФИ № 19-07-00774 «Исследование проблемы интероперабельности при реализации принципов сетецентрических информационно-управляющих систем».

Авторы выражают благодарность А.Я. Олейникову
за его ценные замечания при подготовке статьи

Литература

1. *Башлыкова А.А., Зацаринный А.А., Каменщиков А.А., Козлов С.В., Олейников А.Я., Чусов И.И.* Интероперабельность как научно-методическая и нормативная основа бесшовной интеграции информационно-телекоммуникационных систем // Системы и средства информатики. 2018. Т. 28, № 4. С. 61–72. DOI: 10.14357/08696527180407.
2. *Башлыкова А.А., Козлов С.В., Макаренко С.И., Олейников А.Я., Фомин И.А.* Подход к обеспечению интероперабельности в сетецентрических системах управления // Журнал радиоэлектроники. 2020. № 6. С. 15. DOI: 10.30898/1684-1719.2020.6.13.
3. ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Практические правила управления информационной безопасностью. М.: Стандартинформ, 2006. С. 4–15.
4. ГОСТ Р ИСО/МЭК 27000–2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. М.: Стандартинформ, 2019.
5. ГОСТ Р ИСО/МЭК 7498–2000. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. М.: Изд-во стандартов, 1999. Ч. 2. Архитектура защиты информации. С. 3.
6. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. М.: Стандартинформ, 2008. С. 3–12.
7. ГОСТ Р 55062–2012. Информационные технологии (ИТ). Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения. М.: Стандартинформ, 2014. 12 с.
8. *Козлов С.В., Макаренко С.И., Олейников А.Я., Растягаев Д.В., Черницкая Т.Е.* Проблема интероперабельности в сетецентрических системах управления // Журнал радиоэлектроники. 2019. № 12. С. 16. DOI: 10.30898/1684-1719.2019.12.4.
9. *Макаренко С.И.* Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки: монография. СПб.: Наукоемкие технологии, 2020. 337 с.
10. *Макаренко С.И., Иванов М.С.* Сетецентрическая война: принципы, технологии, примеры и перспективы: монография. СПб.: Наукоемкие технологии, 2018. 898 с.

11. *Макаренко С.И., Олейников А.Я., Черницкая Т.Е.* Модели интероперабельности информационных систем // Системы управления, связи и безопасности. 2019. № 4. С. 215–245. DOI: 10.24411/2410-9916-2019-10408.
12. *Макаренко С.И., Черницкая Т.Е.* Аспекты совместимости сетевых протоколов, интерфейсов и требований по качеству обслуживания в рамках оценки интероперабельности сетецентрических информационно-управляющих систем // Журнал радиоэлектроники. 2020. № 10. DOI: 10.30898/1684-1719.2020.10.4.
13. *Олейников А.Я., Растягаев Д.В., Фомин И.А.* Основные положения концепции обеспечения интероперабельности сетецентрических информационно-управляющих систем // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2020. Вып. 3. С. 122–131. DOI: 10.25586/RNU.V9187.20.03.P.122.
14. Рекомендации по стандартизации Р 50.1.053–2005. Информационные технологии. Основные термины и определения в области технической защиты информации. М.: Стандартинформ, 2006. 11 с.
15. *Черницкая Т.Е., Макаренко С.И., Растягаев Д.В.* Аспекты автоматизации функций управления, принятия решений и сетевого взаимодействия в рамках оценки интероперабельности сетецентрических информационно-управляющих систем // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2020. Вып. 3. С. 138–145. DOI: 10.25586/RNU.V9187.20.03.P.138.
16. *Hughes J., Cybenko G.* Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity // Technology Innovation Management Review, 2013, pp. 15–24. URL: https://timreview.ca/sites/default/files/article_PDF/HughesCybenko_TIMReview_August2013.pdf (дата обращения: 22.10.2020).
17. ISO/IEC/IEEE 24765:2017. Systems and Software Engineering. Vocabulary. ISO, 2017, 522 p.
18. NIST Special Publication 800-160: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems // National Institute of Standards and Technology, 2016, vol. 1, 260 p.
19. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. OECD Publications, 2002, 30 c. URL: https://www.oecd.org/sti/ieconomy/15582260.pdf (date of the application: 22.10.2020).
20. Open Group Standard Open Information Security Management Maturity Model (O-ISM3), Version 2.0. The Open Group, 2017, 130 p.
21. *Saltzer J.H., Schroeder M.D.* The Protection of Information in Computer Systems // Proceedings of the IEEE, 1975, vol. 63, no. 9, pp. 1278–1308.
22. Systems, Capabilities, Operations, Programs, and Enterprises (SCOPE) Model for Interoperability Assessment, Version 1.0, NCOIC, 2008, 154 p.

Literatura

1. *Bashlykova A.A., Zacarinnyj A.A., Kamenshchikov A.A., Kozlov S.V., Olejnikov A.Ya., Chusov I.I.* Interoperabel'nost' kak nauchno-metodicheskaya i normativnaya osnova besshovnoj integracii informacionno-telekommunikacionnyh sistem // Sistemy i sredstva informatiki. 2018. T. 28, № 4. S. 61–72. DOI: 10.14357/08696527180407.
2. *Bashlykova A.A., Kozlov S.V., Makarenko S.I., Olejnikov A.Ya., Fomin I.A.* Podhod k obespecheniyu interoperabel'nosti v setecentricheskih sistemah upravleniya // Zhurnal radioelektroniki. 2020. № 6. S. 15. DOI: 10.30898/1684-1719.2020.6.13.
3. GOST R ISO/MEK 17799–2005. Informacionnaya tekhnologiya. Prakticheskie pravila upravleniya informacionnoj bezopasnost'yu. M.: Standartinform, 2006. S. 4–15.

4. GOST R ISO/MEK 27000–2012. Informacionnaya tekhnologiya (IT). Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informacionnoj bezopasnosti. Obshchij obzor i terminologiya. M.: Standartinform, 2019.
5. GOST R ISO/MEK 7498–2000. Informacionnaya tekhnologiya. Vzaimosvyaz' otkrytyh sistem. Bazovaya etalonnaya model'. M.: Izd-vo standartov, 1999. Ch. 2. Arhitektura zashchity informacii. S. 3.
6. GOST R 50922–2006. Zashchita informacii. Osnovnye terminy i opredeleniya. M.: Standartinform, 2008. S. 3–12.
7. GOST R 55062–2012. Informacionnye tekhnologii (IT). Sistemy promyshlennoj avtomatizacii i ih integraciya. Interoperabel'nost'. Osnovnye polozheniya. M.: Standartinform, 2014. 12 s.
8. *Kozlov S.V., Makarenko S.I., Olejnikov A.Ya., Rastyagaev D.V., Chernickaya T.E.* Problema interoperabel'nosti v setecentricheskih sistemah upravleniya // Zhurnal radioelektroniki. 2019. № 12. S. 16. DOI: 10.30898/1684-1719.2019.12.4.
9. *Makarenko S.I.* Modeli sistemy svyazi v usloviyah prednamerennyh destabiliziruyushchih vozdejstvij i vedeniya razvedki: monografiya. SPb.: Naukoemkie tekhnologii, 2020. 337 s.
10. *Makarenko S.I., Ivanov M.S.* Setecentricheskaya vojna: principy, tekhnologii, primery i perspektivy: monografiya. SPb.: Naukoemkie tekhnologii, 2018. 898 s.
11. *Makarenko S.I., Olejnikov A.Ya., Chernickaya T.E.* Modeli interoperabel'nosti informacionnyh sistem // Sistemy upravleniya, svyazi i bezopasnosti. 2019. № 4. S. 215–245. DOI: 10.24411/2410-9916-2019-10408.
12. *Makarenko S.I., Chernickaya T.E.* Aspekty sovmestimosti setevyh protokolov, interfejsov i trebovanij po kachestvu obsluzhivaniya v ramkah ocenki interoperabel'nosti setecentricheskih informacionno-upravlyayushchih sistem // Zhurnal radioelektroniki. 2020. № 10. DOI: 10.30898/1684-1719.2020.10.4.
13. *Olejnikov A.Ya., Rastyagaev D.V., Fomin I.A.* Osnovnye polozheniya koncepcii obespecheniya interoperabel'nosti setecentricheskih informacionno-upravlyayushchih sistem // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2020. Vyp. 3. S. 122–131. DOI: 10.25586/RNU.V9187.20.03.P.122.
14. Rekomendacii po standartizacii R 50.1.053–2005. Informacionnye tekhnologii. Osnovnye terminy i opredeleniya v oblasti tekhnicheskoj zashchity informacii. M.: Standartinform, 2006. 11 s.
15. *Chernickaya T.E., Makarenko S.I., Rastyagaev D.V.* Aspekty avtomatizacii funkcij upravleniya, prinyatiya reshenij i setevogo vzaimodejstviya v ramkah ocenki interoperabel'nosti setecentricheskih informacionno-upravlyayushchih sistem // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2020. Vyp. 3. S. 138–145. DOI: 10.25586/RNU.V9187.20.03.P.138.
16. *Hughes J., Cybenko G.* Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity // Technology Innovation Management Review, 2013, pp. 15–24. URL: https://timreview.ca/sites/default/files/article_PDF/HughesCybenko_TIMReview_August2013.pdf (дата обращения: 22.10.2020).
17. ISO/IEC/IEEE 24765:2017. Systems and Software Engineering. Vocabulary. ISO, 2017, 522 p.
18. NIST Special Publication 800-160: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems // National Institute of Standards and Technology, 2016, vol. 1, 260 p.

19. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. OECD Publications, 2002, 30 c. URL: https://www.oecd.org/sti/ieconomy/15582260.pdf (date of the application: 22.10.2020).
20. Open Group Standard Open Information Security Management Maturity Model (O-ISM3). Version 2.0. The Open Group, 2017, 130 p.
21. *Saltzer J.H., Schroeder M.D.* The Protection of Information in Computer Systems // Proceedings of the IEEE, 1975, vol. 63, no. 9, pp. 1278–1308.
22. Systems, Capabilities, Operations, Programs, and Enterprises (SCOPE) Model for Interoperability Assessment, Version 1.0, NCOIC, 2008, 154 p.

DOI: 10.25586/RNU.V9187.20.04.P.121 УДК 004.93.1

Н.А. Ворожцова, С.В. Вологдин

ПОДГОТОВКА НАБОРА ДАННЫХ ДЛЯ РАСПОЗНАВАНИЯ ПОКАЗАНИЙ С ФОТОГРАФИЙ ЛИЦЕВЫХ ПАНЕЛЕЙ ПРИБОРОВ УЧЕТА ЭЛЕКТРОЭНЕРГИИ

В рамках исследования, проводимого с целью разработки программного обеспечения, которое позволит повысить точность расчетов потребления электроэнергии за счет автоматизации процесса распознавания данных с фотографий лицевых панелей приборов учета, необходимо разработать алгоритм распознавания символов на изображении. На данный момент существует множество методов и алгоритмов распознавания объектов на изображении. В связи с этим возникает необходимость выбора методов и алгоритмов, соответствующих особенностям объекта распознавания. Результатом применения разработанного алгоритма будет являться распределение всех классов распознавания по степени сходства распознаваемого объекта с ними. Разрабатываемое программное обеспечение должно устранить проблемы, возникающие при ручном вводе данных показаний приборов учета электроэнергии, а именно: отсутствие доверия к полученным данным и невозможность их оперативной проверки; ошибки при вводе данных; многоэтапность процесса обработки данных для отправки поставщику. Предложен алгоритм подготовки набора данных для распознавания фотографий лицевых панелей приборов учета электроэнергии. На первом этапе происходит сбор графических данных, примеры которых отображены в таблице, необходимых для решения поставленной задачи. Затем из полученных изображений необходимо выбрать те, которые обладают лучшим качеством. Выбранные изображения будут являться эталонными, и к эталонному виду в дальнейшем будут приводиться все получаемые изображения объектов исследования. Далее производится выбор подходящего инструмента для разметки изображений, разметка и аннотирование изображений. Финальным этапом является выгрузка полученного набора данных в формате JSON и загрузка в нейронную сеть для ее тренировки.

Ключевые слова: интеллектуальная информационная мобильная система, мобильный энергоучет, распознавание образов, сверточная нейронная сеть, информационно-аналитический комплекс.