19. Listvin A.V., Listvin V.N., SHvyrkov D.V. *Opticheskie volokna dlya linij svyazi* [Optical fibers for communication lines]. Moscow, LESARart Publ., 2003. 288 p.

Received 20.10.2017

УДК 50.03.05

КОМПЛЕКСНАЯ ОЦЕНКА ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ И ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д.
Уфимский государственный авиационный технический университет, Уфа, РФ
E-mail: vasilyev@ugatu.ac.ru

Целью статьи является разработка формализованной методики комплексной оценки выполнения требований к обеспечению защиты информации в автоматизированной системе с применением метода нечеткого логического вывода и экспертных оценок. Предложена процедура определения уровня значимости (критичности) обрабатываемой информации на основе системы нечетких правил (продукций) с учетом степени возможного ущерба от нарушения целостности, доступности или конфиденциальности информации. Рассмотрен пример, иллюстрирующий особенности применения предложенной методики к построению защищенной автоматизированной системы управления.

Ключевые слова: автоматизированная система управления, защита информации, уровень значимости (критичности) информации, класс защищенности

Введение

Проблеме защиты информации в автоматизированных системах управления производственными и технологическими процессами (далее сокращенно АСУ ТП) в последние годы уделяется повышенное внимание на уровне общества, государственных и коммерческих структур, предприятий и организаций. Это в первую очередь относится к АСУ ТП, осуществляющим управление критически важными объектами, включающими в себя объекты топливно-энергетического комплекса, транспортной безопасности, использования атомной энергии, опасные производственные объекты, гидротехнические сооружения. Актуальность и острота проблемы обеспечения информационной безопасности (ИБ) АСУ ТП подчеркивается статистикой резкого роста числа инцидентов ИБ промышленных объектов и возрастанием тяжести последствий от реализации кибератак.

По результатам исследований, проведенных Центром ICS CERT при «Лаборатории Касперского» [1], в период с июля по декабрь 2016 года с вредоносным программным обеспечением (ПО) в России столкнулись 42% компьютеров, так или иначе относящихся к технологической сети предприятий. В 28% случаев вредоносное ПО попадало на компьютеры из Интернета, в 6% – при подключении переносных накопителей. В сетях промышленных предприятий обнаружено в общей сложности 20 тыс. модификаций вредоносного ПО.

В отчете «Лаборатории Касперского» также говорится, что ICS CERT обнаружил серию фишинговых атак, начавшихся не позднее июня 2016 года и продолжающихся до сих пор. Они направлены преимущественно на промышленные компании; в общей сложности во второй половине 2016 года атакам подверглись более 500 организаций из более чем 50 стран мира. Исследования показали, что из всех целевых атак, обнаруженных тогда «Лабораторией Касперского», каждая четвертая была направлена на предприятия. В системах промышленной автоматизации, в том числе на объектах критической инфраструктуры, обнаружено 75 незакрытых уязвимостей, включая 58 максимально критичных для безопасности предприятий. Из 75 обнаруженных в 2016 году уязвимостей к середине марта 2017 года производителями ПО было закрыто только 30.

Приведенные выше данные подтверждаются и результатами исследований компании Positive Technologies [2], согласно которым количество промышленных компаний, столкнувшихся с инцидентами ИБ в 2016 году, возросло почти в три раза по сравнению с 2015 годом. Как отмечают авторы [2], злоумышленники атаковали объекты критической инфраструктуры целенаправленно, причем атаки отличались тщательностью подготовки, нередко с использованием принципов социальной инжене-

рии (например путем внедрения вредоносного ПО через систему массовых спам-рассылок).

Последним примером масштабной кибератаки, поразившей множество компаний по всему миру (включая российские) в период с 12 мая по 15 мая 2017 года, является атака сетевого червя-шифровальщика WannaCry [3]. В числе жертв данной хорошо скоординированной акции – компании, занимающиеся различными видами производства, нефтеперерабатывающие заводы, объекты городской инфраструктуры и распределительные энергосети. В большинстве случаев системы промышленной автоматизации были атакованы вредоносным ПО WannaCry из локальной сети предприятия – при наличии прямого подключения между смежными сетями и при подключениях через VPN. Неудивительно, что международное сообщество и специалисты по ИБ озабочены поиском эффективных путей решения проблемы обеспечения ИБ промышленных объектов.

Европейской комиссией разработана глобальная стратегия по защите объектов критической инфраструктуры The European Programme for Critical Infrastructure Protection [4]. Предложен и эффективно используется в мировой практике ряд международных стандартов по защите информации в АСУ ТП: NERC Critical Infrastructure Protection [5], ISA/IEC 62443 Industrial Automation and Control Systems Security [6], NIST SP 800-82 Guide to Industrial Control Systems Security [7]. В России в качестве аналогичного нормативного документа выступает Приказ ФСТЭК России № 31 от 14.03.2014 [8], в значительной мере коррелирующий, а по ряду позиций превосходящий указанные выше зарубежные программы и стандарты [9].

Методика комплексной оценки выполнения требований ФСТЭК к защите информации в АСУ ТП

Приказ ФСТЭК № 31 представляет собой сбалансированный документ, отражающий современную точку зрения на проблему построения защищенных АСУ ТП в условиях наличия возможных угроз и уязвимостей на основе системного риск-ориентированного подхода. В основе данного подхода лежит формирование организационных и технических мер защиты на основании анализа и учета характерных для системы рисков. Предполагается, что рассматриваемая АСУ ТП имеет многоуровневую архитектуру, включающую в себя: уровень операторского (диспетчерского) управления (верхний уровень); уровень автоматического управления (средний уровень) и уровень ввода (вывода) данных и исполнительных устройств (нижний (полевой) уровень). Каждый из этих уровней может иметь различное число подсистем, к каждой из которых (с учетом ее специфики и характера обрабатываемой в ней информации) могут предъявляться различные требования по обеспечению защиты информации.

В качестве ключевых характеристик, определяющих требования к защите информации в АСУ ТП и ее подсистемах, выступают уровень значимости (критичности) обрабатываемой информации и класс защищенности системы (и ее подсистем). Всего в Приказе ФСТЭК № 31 выделены три уровня значимости (критичности) обрабатываемой информации: высокий (УЗ1), средний (УЗ2) и низкий (УЗ3) с учетом степени возможного ущерба от нарушения целостности (Х1), доступности (Х2) или конфиденциальности (Х3) информации.

Для определения уровня значимости (критичности) информации можно воспользоваться экспертной оценкой с использованием механизма нечеткого логического вывода [10]. Соответствующая система нечетких правил (продукций), на основе которых принимается решение об уровне значимости (критичности) информации (УЗ), принимает вид:

Правило 1: ЕСЛИ Х1 = Высокая, ИЛИ Х2 = Высокая, ИЛИ Х3 = Высокая, ТО УЗ = Высокий (УЗ1), ИНАЧЕ

Правило 2: ЕСЛИ Х1 = Средняя, ИЛИ Х2 = Средняя, ИЛИ Х3 = Средняя, ТО УЗ = Средний (УЗ2), ИНАЧЕ УЗ = Низкий (УЗ3).

Процедура нечеткого логического вывода в данном случае может быть реализована с помощью схемы, представленной на рис. 1.

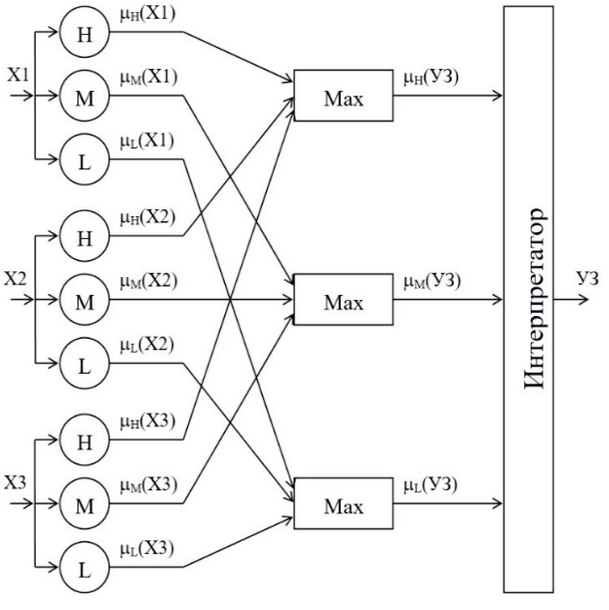

Рис. 1. Схема нечеткого алгоритма принятия решения

Здесь через H, M, L обозначены соответственно термы (нечеткие множества) для лингвистических переменных X1, X2, X3 («Степень ущерба» от нарушения одного из свойств ИБ); H – «Высокая» (High), M – «Средняя» (Middle), L – «Низкая» (Low); $\mu_H(Xi)$, $\mu_M(Xi)$, $\mu_L(Xi)$ – функции принадлежности значений *Xi* нечетким множествам H, M и L соответственно; $\mu_H(УЗ)$, $\mu_M(УЗ)$, $\mu_L(УЗ)$ – функции принадлежности значений УЗ нечетким множествам H, M, L.

Операция логического «ИЛИ» реализуется с помощью блоков вычисления максимума. Интерпретатор работает по следующему правилу:

$$УЗ = \begin{cases} УЗ1, если \mu_H(УЗ) \geq 0{,}5, иначе \\ УЗ2, если \mu_M(УЗ) \geq 0{,}5, иначе \\ УЗ3, если \mu_L(УЗ) \geq 0{,}5; \end{cases}$$

определяя таким образом искомый уровень значимости (критичности) информации. Нечеткие множества «Низкая(-ий)», «Средняя(-ий)», «Высокая(-ий)» для переменных X1, X2, X3, УЗ задаются с помощью функций принадлежности, форма и относительное расположение которых определяются экспертом (или группой экспертов) исходя из субъективных представлений о возможных последствиях (ущербе) от реализации угроз безопасности информации. На рис. 2 приведен пример построения нечетких множеств для переменной X1, приведенной к безразмерному виду (в относительных единицах) в диапазоне [0, 1].

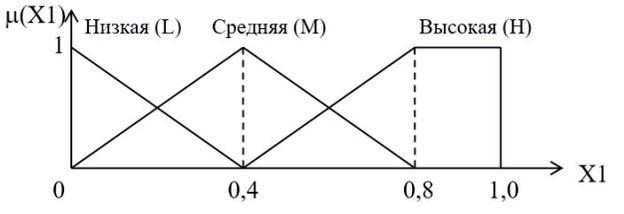

Рис. 2. Пример задания функций принадлежности

Класс защищенности системы (К1 – первый класс, К2 – второй класс, К3 – третий класс) определяется в зависимости от уровня значимости (критичности) обрабатываемой информации:

$$УЗ1 \rightarrow К1, УЗ2 \rightarrow К2, УЗ3 \rightarrow К3.$$

Следующим шагом после установления уровня значимости (критичности) информации и класса защищенности системы является определение обязательного (базового) набора организационных и технических мер защиты информации для соответствующего класса защищенности АСУ ТП согласно требованиям ФСТЭК и оценка соответствия реального состояния ИБ на объекте этим требования (аудит ИБ). Приказ ФСТЭК № 31 содержит 21 группу мер защиты информации (см. таблицу ниже), каждая из которых включает в себя различное количество (от 3 до 31) конкретных мер защиты. Обозначим через M_{ij} частный показатель полноты использования *j*-ой меры защиты (j =1,2,…, n_i) в *i*-ой группе мер (i = 1,2,…,21), где M_{ij} принимает значение 0, если соответствующая мера защиты не применяется, 0,5 – если данная мера защиты используется частично и 1 – если данная мера защиты используется в полном объеме; n_i – количество мер защиты в *i*-ой группе, рекомендованных для данного класса защищенности АСУ ТП. Тогда каждой *i*-ой группе мер защиты можно присвоить групповой показатель полноты использования EV_i мер защиты из базового набора мер защиты, выраженный в процентах, и абсолютный показатель количества N_i неиспользованных или частично использованных мер защиты из рекомендованного базового набора NE_i:

$$EV_i = \left(\frac{1}{n_i} \sum_{j=1}^{n_i} M_{ij} \right) \cdot 100\%;$$
$$NE_i = n_i - \sum_{j=1}^{n_i} unit(M_{ij}), \quad (1)$$

где функция $unit(M_{ij})$ равна 1, если M_{ij}=1, и 0, если M_{ij} = 0 или 0,5. Так, если некоторая группа (например, 1-ая) включает в себя 8 мер защиты, из которых на конкретном объекте выполнены в полном объеме 6 мер, частично – 1 и не выполнена 1 мера защиты, то имеем: n_i = 8, EV_i = 81,3%, NE_i = 2. Заполнив два последних столбца таблицы, эксперт (аудитор) получает полную картину для вынесения суждения (заключения) о соответствии рассматриваемой АСУ ТП требованиям Приказа ФСТЭК № 31 к обеспечению защиты информации. Помимо групповых оценок – показателей EV_i и NE_i, (i = 1; 2 … 21), можно вычислить также интегральные оценки выполнения (полностью или частично) требований по защите информации, характеризующие среднее значение групповых показателей (EV_{cp}) и разброс значений групповых показателей ($EV_{\min}$ и $EV_{\max}$):

$$EV_{cp} = \frac{1}{21} \sum_{i=1}^{21} EV_i; \quad EV_{\min} = \min_i \{EV_i\};$$
$$EV_{\max} = \max_i \{EV_i\}.$$

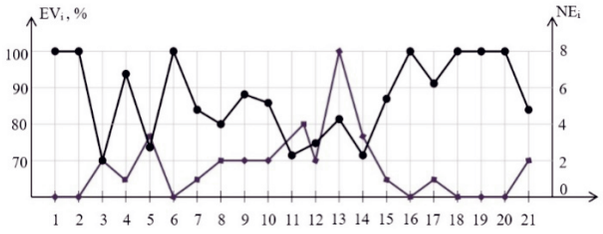

Рис. 3. Диаграмма групповых показателей использования мер защиты информации (EV_i ; NE_i)

На рис. 3 приведен пример диаграммы, показывающей значения всех 21 групповых показателей EV_i и NE_i для некоторой АСУ ТП.

Пример

Как видно из рис. 3, по ряду позиций (группы 1, 2, 6, 16, 18-20) имеет место выполнение (полное или частичное) требований по защите информации, наименьшие значения групповых показателей EV_i выполняются по третьей, пятой, восьмой, одиннадцатой, двенадцатой и четырнадцатой группам мер защиты. Наибольший «всплеск» абсолютных значений показателя EV_i достигается в тринадцатой группе мер ($NE_{13} = 8$), что в значительной степени объясняется большим количеством защитных мер ($n_{13} = 31$), предусмотренных в этой группе. Среднее значение групповых показателей EV_{cp} в данном случае принимает значение $EV_{cp} = 87{,}3\%$, что говорит о достаточно высоком уровне соответствия АСУ ТП требованиям ФСТЭК по защите информации.

Минимальное и максимальное значения групповых показателей использования защитных мер составляют, соответственно, $EV_{\min} = 70\%$ и $EV_{\max} = 100\%$. Для более полного выполнения требований ФСТЭК необходимо внедрение дополнительных мер защиты из базового набора (ранее не реализованных), обеспечивая в первую очередь увеличение тех групповых показателей, которые принимают наименьшие значения (то есть EV_3, EV_5, EV_8, EV_{11}, EV_{12}, EV_{14}). Очевидно, что выбор указанных дополнительных мер должен приводить к сокращению числа NE_i частных показателей M_{ij} внутри перечисленных групп, принимающих значения 0 и 0,5.

Заключение

Предложен подход к комплексной оценке выполнения системы требований по обеспечению защиты информации в АСУ ТП, установленных Приказом ФСТЭК России № 31 от 14.03.2014. Показано, что использование механизма логического вывода, а также частных и групповых показателей полноты использования базовых мер защиты информации позволяет формализовать процедуру экспертной оценки уровня значимости (критичности) обрабатываемой информации и класса защищенности АСУ ТП, выявить слабые места защиты, более обоснованно подойти к выбору состава организационных и технических мер защиты информации в соответствии с требованиями ФСТЭК России.

Литература

1. Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2016 г. URL: https://ics-cert.kaspersky.ru/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/ (д.о. 17.07.2017).
2. Зинина О. Анализ угроз информационной безопасности 2016-2017. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Analysis_information_security_threats_2016_2017 (д.о. 17.07.2017).
3. WannaCry в промышленных сетях: работа над ошибками. URL: https://ics-cert.kaspersky.ru/reports/2017/06/08/wannacry-in-industrial-networks/ (д.о. 17.07.2017).
4. European Programme for Critical Infrastructure Protection. URL: https://ec.europa.eu/energy / en/topics/infrastructure/protection_critical_infrastructure (д.о. 20.08.2017).
5. ICS456: Essentials for NERC Critical Infrastructure Protection. URL: https://www.sans.org/course/essentials-for-nerc-critical-infrastructure-protection (д.о. 20.08.2017).
6. ISA/IEC 62443 Industrial Automation and Control Systems Security. URL: https://www.isa.org/isa99 (д.о. 20.08.2017).
7. NIST SP 800-82 Guide to Industrial Control Systems Security. URL: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (д.о. 20.08.2017).
8. Об утверждении «Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды». Приказ ФСТЭК России №31 от 14.03.2014 // Российская газета, 2014.
9. Защита АСУ ТП в России: исследуем новые требования ФСТЭК / Сопоставление требований ФСТЭК от 14 марта 2014 г. №31 с

Таблица 1. Исследование мер защиты информации

Номер группы мер *i*	Группы мер защиты информации	Число мер защиты (n_i)	Показатель EV_i, %	Показатель NE_i
1	Идентификация и аутентификация субъектов доступа и объектов доступа	8		
2	Управление доступом субъектов доступа к объектам доступа	18		
3	Ограничение программной среды	5		
4	Защита машинных носителей информации	9		
5	Регистрация событий безопасности	9		
6	Антивирусная защита	3		
7	Обнаружение вторжений	3		
8	Контроль (анализ) защищенности информации	6		
9	Обеспечение целостности	9		
10	Обеспечение доступности	8		
11	Защита среды виртуализации	11		
12	Защита технических средств	6		
13	Защита автоматизированной системы и ее компонентов	31		
14	Обеспечение безопасной разработки программного обеспечения	7		
15	Управление обновлениями программного обеспечения	4		
16	Планирование мероприятий по обновлению защиты информации	4		
17	Обеспечение действий в нештатных (непредвиденных) ситуациях	6		
18	Информирование и обучение персонала	4		
19	Анализ угроз безопасности информации и рисков от их реализации	4		
20	Выявление инцидентов и реагирование на них	7		
21	Управление конфигурацией автоматизированной системы управления и ее системы защиты	6		

требованиями международных стандартов. URL: https://ptsecurity.com/upload/corporate / ru/download/FSTEC_N31_NERK_NIST_ISA_IEC.pdf (д.о. 17.07.2017).

10. Зак Ю.А. Принятие решений в условиях нечетких и размытых данных: Fuzzy-технологии. М.: Книжный дом «ЛИБРОКОМ», 2013. – 352 с.

Получено 24.07.2017

Васильев Владимир Иванович, д.т.н., профессор, заведующий Кафедрой вычислительной техники и защиты информации (ВТЗИ) Уфимского государственного авиационного технического университета (УГАТУ). Тел. 8-917-350-11-39. E-mail: vasilyev@ugatu.ac.ru

Вульфин Алексей Михайлович, к.т.н., доцент Кафедры ВТЗИ УГАТУ. Тел. 8-917-400-21-89. E-mail: vulfin.alexey@gmail.com

Гузаиров Мурат Бакеевич, д.т.н., профессор Кафедры ВТЗИ УГАТУ. Тел. 8-917-750-00-66. E-mail: guzairov@ugatu.su

Кириллова Анастасия Дмитриевна, программист Кафедры ВТиЗИ УГАТУ. Тел. 8-917-400-75-50. E-mail: kirillova.andm@gmail.com

INTEGRATED ASSESSMENT OF INFORMATION SECURITY REQUIREMENTS IMPLEMENTATION IN AUTOMATED CONTROL SYSTEMS INTENDED FOR PRODUCTION AND TECHNOLOGICAL PROCESSES

Vasilyev V.I., Vulfin A.M., Guzairov M.B., Kirillova A.D.
Ufa State Aviation Technical University, Ufa, Russian Federation
E-mail: vasilyev@ugatu.ac.ru

The goal of this paper is the further development of the mentioned approach in the form of engineering technique of evaluating the information security requirements fulfillment in automated systems using fuzzy logic methods and expert estimates. The procedure of determining the level of significance (criticality) of processed information on the basis of fuzzy rule set which accounts for possible detriments caused by violating the integrity, availability or confidentiality is proposed. After determining the information significance (criticality) level and the corresponding system security class, the evaluation of the real system security level compliance to the requirements established by the Federal Service of Technical and Export Control Order No. 31 is performed. These requirements determine the basic set of organizational and technical measures of information protection for each class of the system security. The local and group completeness indices are calculated using experts polling method according to the recommended measures of information protection. In addition to the obtained estimates of the group indices, the integral estimates of information security requirements fulfillment characterizing the average value and the spread in the values of the group indices are shown. The example illustrating the specifics of applying this technique to designing the secured automated control system is considered.

Keywords: automated control system, information security, Information importance (criticality) level, protection class

DOI: 10.18469/ikt.2017.15.4.02

Vasilyev Vladimir Ivanovich, Ufa State Aviation Technical University, 12 K. Marx St., Ufa, 450000, Russian Federation; the Head of Department of Computer Science and Information Security; Doctor of Technical Science, Professor. Tel.: +79173501139. E-mail: vasilyev@ugatu.ac.ru

Vulfin Aleksey Mikhailovich, Ufa State Aviation Technical University, 12 K. Marx St., Ufa, 450000, Russian Federation; Associated Professor of the Department of Computer Science and Information Security; PhD in Technical Science. Tel.: +79174002189. E-mail: vulfin.alexey@gmail.com

Guzairov Murat Bakeevich, Ufa State Aviation Technical University, 12 K. Marx St., Ufa, 450000, Russian Federation; Professor of the Department of Computer Science and Information Security; Doctor of Technical Science, Professor. Tel.: +7917750006. E-mail: guzairov@ugatu.su

Kirillova Anastasia Dmitrievna, Ufa State Aviation Technical University, 12 K. Marx St., Ufa, 450000, Russian Federation; programmer of the Department of Computer Science and Information Security. Tel.: +79174007550; E-mail: kirillova.andm@gmail.com

References

1. Threat landscape for industrial automation systems in the second half of 2016. Available at: https://ics-cert.kaspersky.ru/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/ (accessed 17.07.2017).
2. Zinenko O. Analiz ugroz informatsionnoy bezopasnosti 2016-2017 [Analysis of information security threats 2016-2017]. Available at: https://www.anti-malware.ru/analytics/Threats_Analysis/Analysis_information_security_threats_2016_2017 (accessed 17.07.2017).
3. WannaCry v promyishlennyih setyah: rabota nad oshibkami [WannaCry on industrial networks: error correction]. Available at: https://ics-cert.kaspersky.ru/reports/2017/06/08/wannacry-in-industrial-networks/ (accessed 17.07.2017).

4. European Programme for Critical Infrastructure Protection. Available at: https://ec.europa.eu/energy/en/topics/infrastructure/protection_critical_infrastructure (accessed 20.08.2017)
5. ICS456: Essentials for NERC Critical Infrastructure Protection. Available at: https://www.sans.org/course/essentials-for-nerc-critical-infrastructure-protection (accessed 20.08.2017)
6. ISA/IEC 62443 Industrial Automation and Control Systems Security. Available at: https://www.isa.org/isa99 (accessed 20.08.2017)
7. NIST SP 800-82 Guide to Industrial Control Systems Security. Available at: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (accessed 20.08.2017)
8. Ob utverzhdenii Trebovaniy k obespecheniyu zaschityi informatsii v avtomatizirovannyih sistemah upravleniya proizvodstvennyimi i tehnologicheskimi protsessami na kriticheski vazhnyih ob'ektah, predstavlyayuschih povyishennuyu opasnost dlya zhizni i zdorovya lyudey i dlya okruzhayuschey sredyi: Prikaz FSTEK Rossii No. 31 ot 14.03.2014 g. [On approving the Requirements to protection in automated production and technological processes control systems at the critically important objects, representing the enhanced danger for the people life and health and for the environment: The Order of Russia FSTEC № 31 of 14.03.2014]. The Russian news-paper, 2014.
9. Zaschita ASU TP v Rossii: issleduem novyie trebovaniya FSTEK / Sopostavlenie trebovaniy FSTEK ot 14 marta 2014 g. No. 31 s trebovaniyami mezhdunarodnyih standartov [Protection of APTCS in Russia: investigating the new FSTEC requirements / Comparison of FSTEC requirements of 14th March, 2014 No. 31 with the requirements of international standards]. Available at: https://ptsecurity.com/upload/corporate/ru-ru/download/FSTEC_N31_NERK_NIST_ISA_IEC.pdf (accessed 17.07.2017) (In Russ.)
10. Zak U.A. *Prinyatie resheniy v usloviyah nechetkih i razmyityih dannyih: Fuzzy-tehnologii.* [Decision-making in a fuzzy and indistinct data. Fuzzy technology]. Moscow, Librokom Publ., 2013. 352 p.

Received 24.07.2017

УДК 621.391

ПРИМЕНЕНИЕ МЕДИАННЫХ ФИЛЬТРОВ С ВЗВЕШЕННЫМ ЦЕНТРАЛЬНЫМ ЭЛЕМЕНТОМ ДЛЯ ОЧИСТКИ ИЗОБРАЖЕНИЙ ОТ ИМПУЛЬСНОГО ШУМА

Червяков Н.И., Ляхов П.А., Оразаев А.Р.
Северо-Кавказский федеральный университет, Ставрополь, РФ
E-mail: ljahov@mail.ru

В статье показано применение медианных фильтров с взвешенными центральными элементами для очистки изображений от импульсного шума. Показано влияние вероятности получения неискаженных пикселей и искажения функции распределения пикселей изображения на результат обработки. Продемонстрировано, что медианные фильтры с окном 3×3 позволяют получать более высокое качество очистки изображений от шума с небольшой вероятностью импульсного шума, а медианные фильтры с размерами окон 5×5 и 7×7 позволяют получать более высокое качество очистки изображений от шума с высокой вероятностью импульсного шума. Полученный результат может быть использован в медицинской обработке изображений и адаптивных системах фильтрации при обработке фото- и видеоданных.

Ключевые слова: цифровая обработка изображений, импульсный шум, медианный фильтр, цифровая обработка сигналов

Введение

В процессе передачи и преобразования посредством радиотехнических систем изображения подвергаются воздействию различных помех, что в ряде случаев приводит к ухудшению визуального качества и потере участков изображений. С широким внедрением цифровых систем связи увеличивается актуальность решения задач восстановления изображений, полученных с помощью фото- и видеокамер, с целью фильтрации изображений. На практике часто встречаются изображения, искаженные шумом, который появляется на этапах формирования и передачи его по каналу связи [1]. Линейные алгоритмы фильтрации применяются для реставрации и улучшения визуального качества изображений. Их можно применять для снижения уровня шума на изображениях. Однако, чтобы подавить шум и при этом