Учредитель

ФГБОУ ВО «Новосибирский государственный технический университет»

Редакционный совет

Председатель редакционного совета

Вострецов Алексей Геннадьевич, д-р техн. наук, проф., засл. деятель науки РФ, НГТУ, г. Новосибирск

Заместители председателя

Белим Сергей Викторович, д-р физ.-мат. наук, проф., ОмГТУ, г. Омск
Белов Виктор Матвеевич, д-р техн. наук, проф., НГТУ, г. Новосибирск
Котенко Игорь Витальевич, д-р техн. наук, проф., СПИИРАН, г. Санкт-Петербург

Члены редакционного совета

Авдеенко Татьяна Владимировна, д-р техн. наук, проф., НГТУ, г. Новосибирск
Аверченков Владимир Иванович, д-р техн. наук, проф., Брянский ГТУ, г. Брянск
Алгулиев Расим Магомед оглу, д-р техн. наук, проф., академик НАН Республики Азербайджан, ИИТ НАН Республики Азербайджан, г. Баку
Аникин Игорь Вячеславович, д-р техн. наук, доцент, КНИТУ-КАИ, г. Казань
Арутюнян Мариам Евгеньевна, д-р физ.-мат. наук, проф., ИИиАП НАН Республики Армения, г. Ереван
Баранкова Инна Ильинична, д-р техн. наук, доцент, МГТУ им. Г.И. Носова, г. Магнитогорск
Беззатеев Сергей Валентинович, д-р техн. наук, доцент, СПбГУАП, г. Санкт-Петербург
Боранбаев Сейлхан Нарбутинович, д-р техн. наук, проф., Евразийский национальный университет им. Л.Н. Гумилева, г. Нур-Султан, Республика Казахстан
Васильев Владимир Иванович, д-р техн. наук, проф., УГАТУ, г. Уфа
Воевода Александр Александрович, д-р техн. наук, проф., НГТУ, г. Новосибирск
Гатчин Юрий Арменакович, д-р техн. наук, проф., ИТМО, г. Санкт-Петербург
Громов Юрий Юрьевич, д-р техн. наук, проф., Тамбовский ГТУ, г. Тамбов
Иващук Ольга Александровна, д-р техн. наук, проф., НИУ «БелГУ», г. Белгород
Киселёва Тамара Васильевна, д-р техн. наук, проф., СибГИУ, г. Новокузнецк
Кулаков Станислав Матвеевич, д-р техн. наук, проф., СибГИУ, г. Новокузнецк
Кульба Владимир Васильевич, д-р техн. наук, проф., ИПУ РАН, г. Москва
Кытманов Алексей Александрович, д-р физ.-мат. наук, доцент, СФУ, г. Красноярск
Лавлинский Сергей Михайлович, д-р техн. наук, доцент, Институт математики им. С.Л. Соболева СО РАН, г. Новосибирск
Ленский Артем, PhD, ст. науч. сотр., Австралийский национальный университет, г. Канберра
Магазев Алексей Анатольевич, д-р физ.-мат. наук, проф., ОмГТУ, г. Омск
Макарова Елена Анатольевна, д-р техн. наук, проф., УГАТУ, г. Уфа
Митрохин Валерий Евгеньевич, д-р техн. наук, проф., ОмГУПС, г. Омск
Мышляев Леонид Павлович, д-р техн. наук, проф., СибГИУ, г. Новокузнецк
Пагано Микеле, д-р, проф., Пизанский университет, г. Пиза, Италия

Пиотровский Дмитрий Леонидович, д-р техн. наук, проф., Средиземноморский Карпасский университет, Турецкая Республика Северного Кипра
Петрунин Юрий Юрьевич, д-р филос. наук, проф., МГУ им. М.В. Ломоносова, г. Москва
Тузиков Александр Васильевич, д-р физ.-мат. наук, проф., чл.-корр. НАН Республики Беларусь, ОИПИ НАН Республики Беларусь, г. Минск
Харин Юрий Семенович, д-р физ.-мат. наук, проф., чл.-корр. НАН Республики Беларусь, БГУ, г. Минск
Ходашинский Илья Александрович, д-р техн. наук, проф., ТУСУР, г. Томск
Шарипов Бахыт Жапарович, д-р пед. наук, проф., Международный университет информационных технологий, г. Алматы, Республика Казахстан
Ячиков Игорь Михайлович, д-р техн. наук, проф., МГТУ им. Г.И. Носова, г. Магнитогорск

Редакция

Главный редактор

Вострецов Алексей Геннадьевич, д-р техн. наук, проф., засл. деятель науки РФ, НГТУ, г. Новосибирск

Заместитель главного редактора

Белов Виктор Матвеевич, д-р техн. наук, проф., НГТУ, г. Новосибирск

Журнал зарегистрирован 01.03.2021 Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Свидетельство о регистрации ПИ № ФС 77-80320

Адрес издателя и редакции: 630073, г. Новосибирск, пр. К. Маркса, 20.
E-mail: office@publish.nstu.ru и digital-tech-security@mail.ru
Web site: http://publish.nstu.ru и http://journals.nstu.ru/digital-tech-security/

Publisher and editorial office adress: 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Fe-deration

До номера 1 (100) 2021 г. включительно журнал выходил под названием «Сборник научных трудов НГТУ» (ISSN 2307-6879)

16+

© Коллектив авторов, 2023
© Новосибирский государственный технический университет, 2023

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ

ISSN 2782-2230

№ 1 (108) **2023**

СОДЕРЖАНИЕ

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

Бабичев М.М., Григорьев Д.А. Формирование ступенчатого сигнала с минимальными уровнями третьей гармоники 9

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

Аникин А.Д., Бирюков К.А., Архипова А.Б. Анализ протоколов безопасности на базе системы распространения лицензируемого контента 26

Бочарникова М.Е., Пестунова Т.М., Селифанов В.В. Вопросы личной информационной безопасности в условиях цифровой трансформации экономики, управления и общественных коммуникаций 36

Воевода А.А., Шипагин В.И. Модальный синтез регуляторов полиномиальным методом для систем автоматического управления с избыточной размерностью вектора управления 53

Селифанов В.В., Аникеева В.В., Огнев И.А. Вопросы оценки доверия к системе управления рисками 69

Правила для авторов 83

Выпускающий редактор *И.П. Брованова*
Корректор *Л.Н. Киншт*
Компьютерная верстка *С.И. Ткачева*

Лицензия № ИД 04303 от 20.03.01. Подписано в печать 22.03.2023. Выход в свет 29.03.2023
Формат 60×84/16. Бумага офсетная. Тираж 300 экз. Уч.-изд. л. 5,11
Печ. л. 5,5. Изд. № 57. Заказ № 104. Цена свободная

Отпечатано в типографии
Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20

Editorial board

Novosibirsk State Technical University

Editorial council

Chairman of the editorial council

Vostretsov A.G., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF

Deputy chairman

Belim S.V., Dr. Sc. (Phys. & Math.), Omsk State Technical University, Omsk, RF
Belov V.M., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF
Kotenko I.V., Dr. Sc. (Eng.), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, RF

The members of the editorial council

Avdeenko T.V., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF
Averchenkov V.I., Dr. Sc. (Eng.), Bryansk State Technical University, Bryansk, RF
Alguliyev R.M.o., Dr. Sc. (Eng.), Azerbaijan National Academy of Sciences, Institute of Information Technology, Baku, AZE
Anikin I.V., Dr. Sc. (Eng.), Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, RF
Haroutunian M.E., Dr. Sc. (Phys. & Math.), Institute for Informatics and Automation Problems of NAS RA, Yerevan, ARM
Barankova I.I., Dr. Sc. (Eng.), Nosov Magnitogorsk State Technical University, Magnitogorsk, RF
Bezzateev S.V., Dr. Sc. (Eng.), Saint Petersburg State University of Aerospace Instrumentation, St. Petersburg, RF
Boranbaev S.N., Dr. Sc. (Eng.), L.N. Gumilyov Eurasian National University, Nur-Sultan, KZ
Vasil'ev V.I., Dr. Sc. (Eng.), Ufa State Aviation Technical University, UFA, RF
Voevoda A.A., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF
Gatchin Yu.A., Dr. Sc. (Eng.), National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, RF
Gromov Yu.Yu., Dr. Sc. (Eng.), Tambov State Technical University, Tambov, RF
Ivashhuk O.A., Dr. Sc. (Eng.), Belgorod State National Research University, Belgorod, RF
Kiseljova T.V., Dr. Sc. (Eng.), Siberian State Industrial University, Novokuznetsk, RF
Kulakov S.M., Dr. Sc. (Eng.), Siberian State Industrial University, Novokuznetsk, RF
Kul'ba V.V., Dr. Sc. (Eng.), V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, RF
Kytmanov A.A., Dr. Sc. (Phys. & Math.), Siberian Federal University, Krasnoyarsk, RF
Lavlinskij S.M., Dr. Sc. (Eng.), Sobolev Institute of Mathematics of Russian Academy of Sciences, Novosibirsk, RF
Lenskij A., PhD, Australian National University, Canberra, AUS
Magazev A.A., Dr. Sc. (Phys. & Math.), Omsk State Technical University, Omsk, RF
Makarova E.A., Dr. Sc. (Eng.), Ufa State Aviation Technical University, Ufa, RF

Mitrokhin V.E., Dr. Sc. (Eng.), Omsk State Transport University, Omsk, RF
Myshljaev L.P., Dr. Sc. (Eng.), Siberian State Industrial University, Novokuznetsk, RF
Pagano M., Dr. Sc., University of Pisa, Pisa, IT
Piotrovskij D.L., Dr. Sc. (Eng.), University of Mediterranean Karpasia, Turkish Republic of Northern Cyprus, CYP
Petrunin Yu.Yu., Dr. Sc. (Philos.), Lomonosov Moscow State University, Moscow, RF
Tuzikov A.V., Corresponding Member, National Academy of Sciences of Republic Belarus, Dr. Sc. (Phys. & Math.), United Institute of Informatics Problems, Minsk, BLR
Harin Yu.S., Corresponding Member, National Academy of Sciences of Republic Belarus, Dr. Sc. (Phys. & Math.), Belarusian State University, Minsk, BLR
Hodashinskij I.A., Dr. Sc. (Eng.), Tomsk State University of Control Systems and Radioelectronics, Tomsk, RF
Sharipov B.Zh., Dr. Sc. (Ped.), International University of Information Technology, Almaty, KZ
Jachikov I.M., Dr. Sc. (Eng.), Nosov Magnitogorsk State Technical University, Magnitogorsk, RF

Editorial office

Chief editor

Vostretsov A.G., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF

Deputy chief editor

Belov V.M., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF

Publisher and editorial adress: 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation
E-mail: office@publish.nstu.ru, digital-tech-security@mail.ru
Web site: http://publish.nstu.ru, http://journals.nstu.ru/digital-tech-security/

© Authors, 2023
© Novosibirsk State Technical University, 2023

DIGITAL TECHNOLOGY SECURITY

ISSN 2782-2230

№ 1 (108) **2023**

CONTENTS

ELECTRONICS, PHOTONICS, INSTRUMENTATION AND THE CONNECTION

Babichev M.M., Grigoriev D.A. Formation of a stepped signal with minimum levels of the third harmonic 9

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Anikin A.D., Biryukov K.A., Arkhipova A.B. Analysis of security protocols based on the licensed content distribution system 26

Bocharnikova M.E., Pestunova T.M., Selifanov V.V. Personal information security issues in the context of digital transformation of the economy, management and public communications 36

Voevoda A.A., Shipagin V.I. Modal synthesis of controllers by a polynomial method for automatic control systems with excessive dimension of the control vector 53

Selifanov V.V., Anikeeva V.V., Ognev I.A. Issues of assessing the credibility of the risk management system 69

Rules for authors 83

Editor *L.N. Kinsht*
Publishing Editor *I.P. Brovanova*
Computer imposition *S.I. Tkacheva*

License № ID 04303 from 20.03.01. Signed in print March 22, 2023
Date of publication March 29, 2023. Format 60 × 84 1/16
Offset Paper. Circulation is 300 copies. Educational-ed. liter. 5,11. printed pages 5,5
Publishing number 57. Order number 104

It is printed in printing house of Novosibirsk State Technical University
630073, Novosibirsk, 20 K. Marx Prospekt

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 1 (108). – 9–25

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

УДК 51-74:621.382.2/.3 DOI: 10.17212/2782-2230-2023-1-9-25

ФОРМИРОВАНИЕ СТУПЕНЧАТОГО СИГНАЛА С МИНИМАЛЬНЫМИ УРОВНЯМИ ТРЕТЬЕЙ ГАРМОНИКИ*

М.М. БАБИЧЕВ[1], Д.А. ГРИГОРЬЕВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: babichev@corp.nstu.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: grighoriev_daniil@mail.ru*

Одна из важных задач электронного приборостроения – создание мощных измерительных генераторов синусоидального сигнала, в частности, генераторов фиктивной мощности для испытания и поверки счетчиков электроэнергии. Такие генераторы обычно имеют цифровое управление. Широтно-импульсная модуляция (ШИМ) позволяет получить высокий коэффициент полезного действия (КПД). Однако при построении устройства на основе ШИМ возникает потребность в подавлении гармоник высших порядков. Для упрощения фильтрации сигнала повышают частоту переключения ключей в генераторе, что снижает его КПД. В работе представлен новый способ получения синусоидального сигнала с помощью сложения трех прямоугольных импульсных сигналов, имеющих частоту формируемой синусоиды, что позволяет подавить третью гармонику и фильтровать гармоники, начиная с пятой. Такой способ позволяет при высоком КПД и простом выходном фильтре формировать синусоиду с частотой не только 50 Гц, но и существенно более высокой.

Ключевые слова: генератор, синусоида, ШИМ, спектр, гармоника, фильтр, Electronics Workbench, моделирование

* Статья получена 17 февраля 2023 г.

ВВЕДЕНИЕ

В настоящее время в ряде задач, например при регулировке и поверке счетчиков электрической энергии используются мощные генераторы низкочастотных синусоидальных сигналов [21].

Для генерирования синусоидального сигнала с помощью цифровой управляющей схемы [1, 3, 11], формирователя сигнала ШИМ [12] и усилителя класса D с минимальным числом ключей и минимальным числом импульсов на период следует выбрать длительность импульсов и их размещение на периоде синусоидального сигнала так, чтобы:

1) была полностью подавлена третья гармоника;
2) значения пятой и седьмой гармоник были минимальными;
3) число импульсов на периоде синусоиды было минимальным.

Основное внимание уделяется минимизации третьей гармоники [20] по той причине, что ее сложнее фильтровать, чем гармоники более высоких порядков – 5, 7 и т. д. На выходе усилителя класса D ставится *LC*-фильтр [4] 2-го или более высокого порядка, что значит, что третья и более высокие гармоники подавляются в 4 и более раз, в то время как пятая гармоника – в 16 раз и более. Также разработчики стараются минимизировать коэффициент гармоник.

Выбирать большое число импульсов на период нецелесообразно, так как с ростом частоты переключения электронных ключей возрастают потери энергии [18]. С другой стороны, повышение частоты следования импульсов упрощает фильтрацию высших гармоник, что улучшает соотношение сигнал–шум [19].

1. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ЗАДАЧИ

Для решения поставленной задачи найдем значение нижеприведенного сигнала.

$$\int\limits_{\frac{\pi}{2}-\alpha_1}^{\frac{\pi}{2}+\alpha_1} \sin(nx)\,dx = -\frac{1}{n}\cos(nx)\Bigg|_{\frac{\pi}{2}-\alpha_1}^{\frac{\pi}{2}+\alpha_1} = -\frac{1}{n}\left[\cos\left(\frac{\pi}{2}+\alpha_1\right)-\sin\left(\frac{\pi}{2}-\alpha_1\right)\right] =$$

$$= -\frac{1}{n}(-2)\left[\sin\frac{1}{2}\left(n\frac{\pi}{2}+n\alpha_1+n\frac{\pi}{2}-n\alpha_1\right)\sin\frac{1}{2}\left(n\frac{\pi}{2}+n\alpha_1-n\frac{\pi}{2}+n\alpha_1\right)\right] =$$

$$= \frac{2}{n}\sin\left(n\frac{\pi}{2}\right)\sin(n\alpha_1)\,. \qquad (1)$$

Этот интеграл характеризует спектральный состав прямоугольного импульса, нечетно симметричного относительно полупериода, имеющего координаты центра π/2 и ширину импульса, равную $2\alpha_1$. Номер гармонической составляющей – *n*.

Далее можно найти некоторые пропорциональные составляющие спектра такого ШИМ-сигнала.

При *n* = 1

$$A_1 = 2\sin\left(\frac{\pi}{2}\right)\sin(\alpha_1) = 2\sin\alpha_1 . \tag{2}$$

При *n* = 2 и аналогично для всех четных

$$A_2 = \sin(\pi)\sin(2\alpha_1) = 0 . \tag{3}$$

При *n* = 3

$$A_3 = \frac{2}{3}\sin\left(\frac{3\pi}{2}\right)\sin(3\alpha_1) = -\frac{2}{3}\sin 3\alpha_1 . \tag{4}$$

При *n* = 5

$$A_5 = \frac{2}{5}\sin\left(\frac{5\pi}{2}\right)\sin(5\alpha_1) = \frac{2}{5}\sin 5\alpha_1 . \tag{5}$$

При *n* = 7

$$A_7 = \frac{2}{7}\sin\left(\frac{7\pi}{2}\right)\sin(7\alpha_1) = -\frac{2}{7}\sin 7\alpha_1 . \tag{6}$$

При *n* = 9

$$A_9 = \frac{2}{9}\sin\left(\frac{9\pi}{2}\right)\sin(9\alpha_1) = \frac{2}{9}\sin 9\alpha_1 , \tag{7}$$

где A_i $(i = 1\ldots9)$ – величина, пропорциональная соответствующей гармонике. Рассмотрим следующие углы α_{1i}, которые либо в единичном варианте, либо в комбинации углов дают полное подавление третьей гармоники:

$$\alpha_{11} = \frac{\pi}{3}; \quad \alpha_{12} = \frac{\pi}{2}; \quad \alpha_{13} = \frac{\pi}{6} . \tag{8}$$

Подставляя последовательно (8) в выражения (2) – (7), получим:

1) для угла $\alpha_{11} = \frac{\pi}{3}$

$$A_{11} = 2\sin\frac{\pi}{3} = \sqrt{3}; \quad A_{21} = 0;$$

$$A_{31} = -\frac{2\sin\pi}{3} = 0; \quad A_{51} = \frac{2\sin\frac{5\pi}{3}}{5} = \frac{-2\sin\frac{\pi}{3}}{5} = -\frac{\sqrt{3}}{5}; \tag{9}$$

$$A_{71} = -\frac{2\sin\frac{7\pi}{3}}{7} = -\frac{2\sin\frac{\pi}{3}}{7} = -\frac{\sqrt{3}}{7};$$

$$A_{91} = \frac{2}{9}\sin\frac{9\pi}{3} = 0;$$

2) для угла $\alpha_{12} = \frac{\pi}{2}$

$$A_{12} = 2\sin\frac{\pi}{2} = 2; \quad A_{22} = 0; \quad A_{32} = -\frac{2\sin\frac{3\pi}{2}}{3} = \frac{2}{3};$$

$$A_{52} = \frac{2}{5}\sin\frac{5\pi}{2} = \frac{2}{5}; \quad A_{72} = -\frac{2}{7}\sin\frac{7\pi}{2} = \frac{2}{7}; \tag{10}$$

$$A_{92} = \frac{2}{9}\sin\frac{9\pi}{2} = \frac{2}{9};$$

3) для угла $\alpha_{13} = \frac{\pi}{6}$

$$A_{13} = 2\sin\frac{\pi}{6} = 1; \quad A_{23} = 0; \quad A_{33} = -\frac{2\sin\frac{3\pi}{6}}{3} = -\frac{2}{3};$$

$$A_{53} = \frac{2}{5}\sin\frac{5\pi}{6} = \frac{1}{5}; \tag{11}$$

$$A_{73} = -\frac{2}{7}\sin\frac{7\pi}{6} = \frac{1}{7}; \quad A_{93} = \frac{2}{9}\sin\frac{9\pi}{6} = -\frac{2}{9}.$$

Далее рассмотрим три варианта формирования синусоидального сигнала и оценим влияние гармоник 5, 7 и 9. Формирование ШИМ-сигнала U_1 в соответствии с (9):

$$U_1 = \sqrt{3} - \frac{\sqrt{3}}{5} - \frac{\sqrt{3}}{7} = \sqrt{3}\left(1 - \frac{1}{5} - \frac{1}{7}\right). \tag{12}$$

Формирование ШИМ-сигнала U_2 как суммирование (10) и (11):

$$U_2 = \left(2 + \frac{2}{3} + \frac{2}{5} + \frac{2}{7} + \frac{2}{9}\right) + \left(1 - \frac{2}{3} + \frac{1}{5} + \frac{1}{7} - \frac{2}{9}\right) = 3 + \frac{3}{5} + \frac{3}{7}. \tag{13}$$

Формирование ШИМ-сигнала U_3 в виде суммы (9), (10) и (11):

$$U_3 = U_1 + U_2 = \sqrt{3} - \frac{\sqrt{3}}{5} - \frac{\sqrt{3}}{7} + 3 + \frac{3}{5} + \frac{3}{7} =$$

$$= 3\sqrt{3}\left(1 + \frac{3 - \sqrt{3}}{5 \cdot 3\sqrt{3}} + \frac{3 - \sqrt{3}}{7 \cdot 3\sqrt{3}}\right). \tag{14}$$

Для U_1 и U_2 коэффициент нелинейных искажений ($КНИ_1, КНИ_2$) одинаков и равен (для первых девяти гармоник) 24 %, для U_3 равен 6 %. Отношение $КНИ_{1,2}$ к $КНИ_3$ после фильтра первого порядка следующее:

$$\frac{КНИ_1}{КНИ_3} = 15; \qquad \frac{КНИ_2}{КНИ_3} = 7{,}5.$$

На рис. 1 приведены эпюры прямоугольных сигналов с углами α_{11}, α_{21}, α_{13} и их суммы. U_1 соответствует графику α_{11}; U_2 – графику α_{12+13}; U_3 – графику $\alpha_{11+12+13}$. Такие сигналы позволяют использовать минимально возможную частоту переключения электронных ключей, равную частоте формируемой синусоиды. Функциональная схема генератора синусоиды, использующего сигнал U_3, показана на рис. 2.

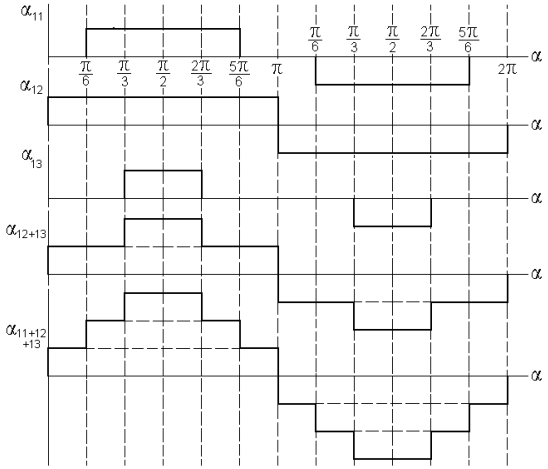


Рис. 1. Эпюры ступенчатых сигналов

Fig. 1. Plots of step signals

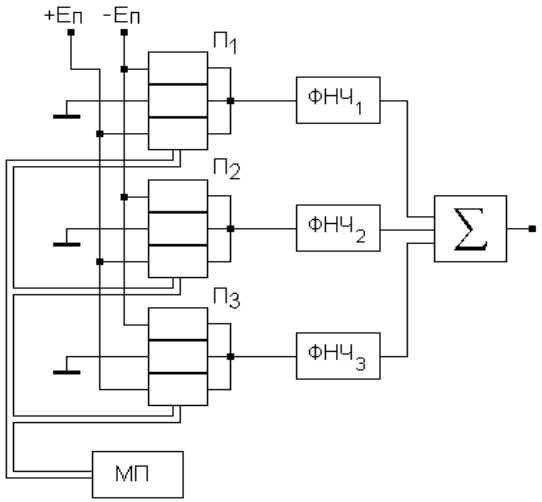


Рис. 2. Функциональная схема генератора синусоиды на основе шестиуровневого ступенчатого сигнала

Fig. 2. Functional diagram of a sine wave generator based on a 6-level step signal

Обозначения на рис. 2: $П_i$ – переключатели; $ФНЧ_i$ – фильтры низкой частоты; Σ – сумматор; МП – микропроцессор.

Микропроцессор управляет переключателями в соответствии с эпюрами рис. 1. Фильтры низкой частоты выполняются на *LC*-элементах. Сумматор может быть выполнен на трансформаторе.

При исполнении данной схемы может быть использован один двухканальный источник питания.

Выводы из математической модели:

1) первый и второй варианты, т. е. (12) и (13), имеют одинаковые КНИ. В силу простоты первый вариант предпочтительнее, однако уступает второму в $\sqrt{3}$ раз по величине первой гармоники;

2) третий вариант (14) без учета амплитуд имеет меньший КНИ (примерно в 5 раз), чем первый и второй вариант, а также имеет бóльшую величину амплитуды первой гармоники в 3 раза, чем первый вариант, и в $\sqrt{3}$ раз большую, чем второй вариант. Это позволяет увеличить выходную мощность усилителя класса D параллельного типа.

2. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

2.1. ФОРМИРОВАНИЕ СТУПЕНЧАТОГО СИГНАЛА

На первом этапе исследования было выбрано устройство, которое способно генерировать шестиуровневый ступенчатый сигнал. Возможностью формировать сигнал произвольной формы обладает двухканальный виртуальный осциллограф АКИП-72204А со встроенным генератором сигналов. Данный осциллограф работает под управлением приложения PicoScope v6, интерфейс представлен на рис. 3.

Сформируем с помощью инструмента «генератор произвольных сигналов» шестиступенчатый сигнал (на рис. 1 $\alpha_{11+12+13}$), задавшись 1024 отчетами на период сигнала. Для этого запишем отсчеты одного периода сигнала в CSV-файл. Период состоит из двух полупериодов, в каждом 6 интервалов времени, итого 12. Один интервал равен 1024 / 12 = 85,3 отсчетов. Пусть каждая ступень сигнала имеет по уровню 0,25 В. В таблице приведено описание формируемого сигнала.

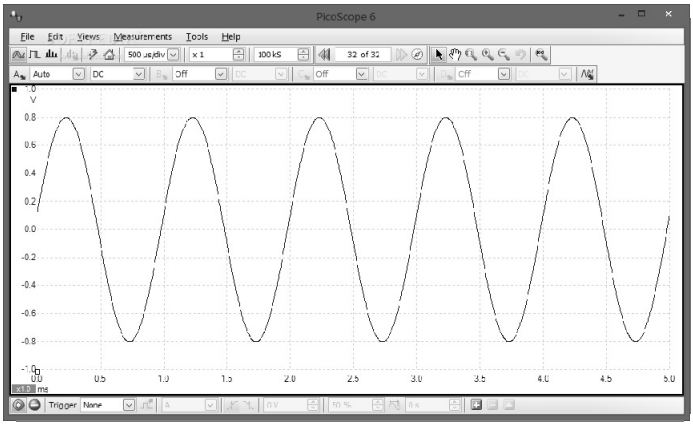


Рис. 3. Интерфейс программы PicoScope v6

Fig. 3. PicoScope v6 interface

Значения для формирования ступенчатого сигнала

Номера отсчетов	Уровень напряжения, В
0…85	0,25
86...171	0,5
172…341	0,75
342…426	0,5
427…512	0,25
513…597	–0,25
598…682	–0,5
683…853	–0,75
854…939	–0,5
940…1024	–0.25

На рис. 4 показан ступенчатый сигнал с частотой 1 кГц (такая частота была выбрана для удобства первоначального исследования), который в дальнейшем будет использоваться для гармонического анализа.

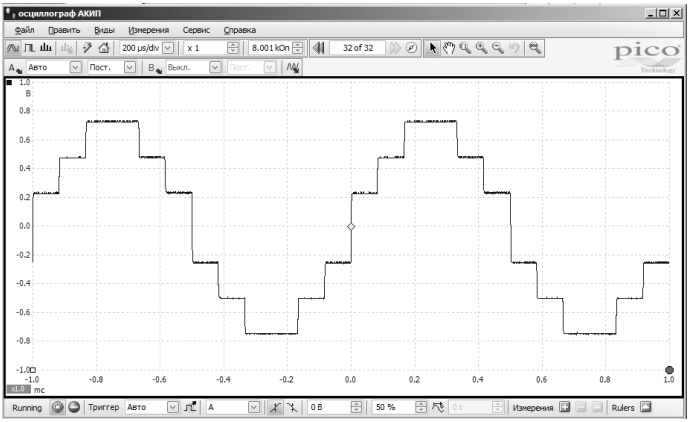


Рис. 4. Осциллограмма ступенчатого шестиуровневого сигнала

Fig. 4. Stepped 6-level Waveform

Если выбрать режим быстрого преобразования Фурье в программе PicoScope, в спектре помимо основной гармоники видны пятая, седьмая и последующие нечетные гармоники, не кратные трем. Как видно на рис. 5, на частоте 1 кГц выражена основная гармоника, затем на частоте 3 кГц – существенно подавленная третья гармоника, на частоте 5 кГц – пятая гармоника, и так далее; четные гармоники также подавлены.

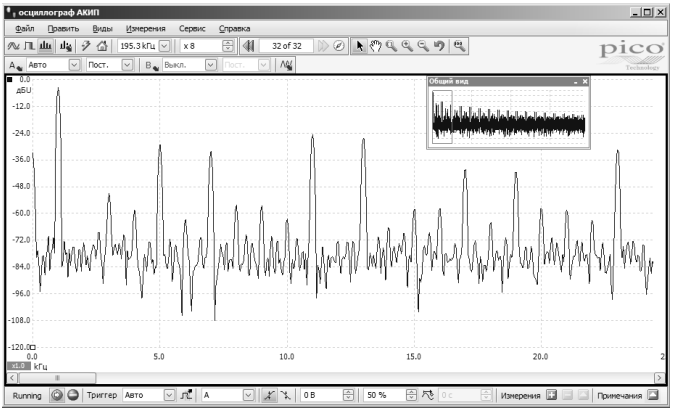


Рис. 5. Спектр ступенчатого сигнала

Fig. 5. Step signal spectrum

2.2. ОЦЕНКИ ЭФФЕКТИВНОСТИ ФНЧ ДЛЯ ПОДАВЛЕНИЯ ВЫСШИХ ГАРМОНИК

Исходя из рис. 5, в полученном сигнале требуется подавлять пятую гармонику и гармоники более высокого порядка. Для этого был использован ФНЧ второго порядка на основе емкости и индуктивности.

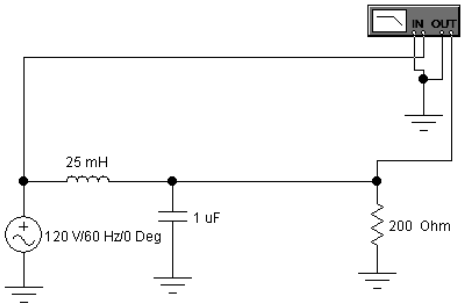


Рис. 6. Модель для оценки эффективности ФНЧ

Fig. 6. Model for evaluating the effectiveness of LPF

На рис. 6 показана модель данного фильтра, созданная в Electronics Workbench. Фильтр имеет частоту среза 1 кГц. С нагрузкой 200 Ом он имеет на частоте среза незначительное резонансное усиление. К нагрузке подключен виртуальный инструмент Bode Plotter – характериограф, отображающий АЧХ схемы.

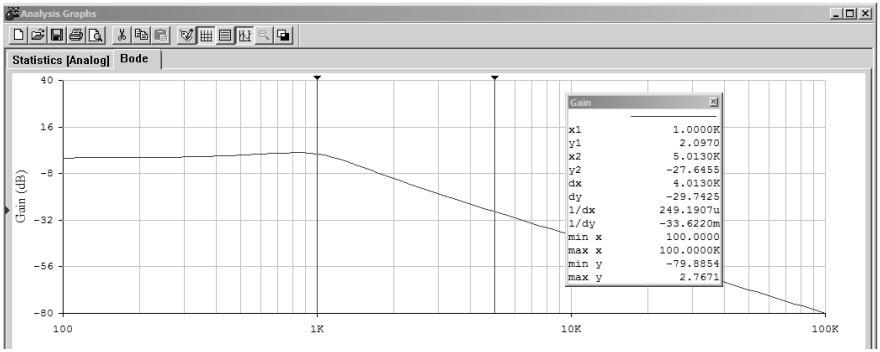


Рис. 7. Ослабление пятой гармоники

Fig. 7. Attenuation of the 5th harmonic

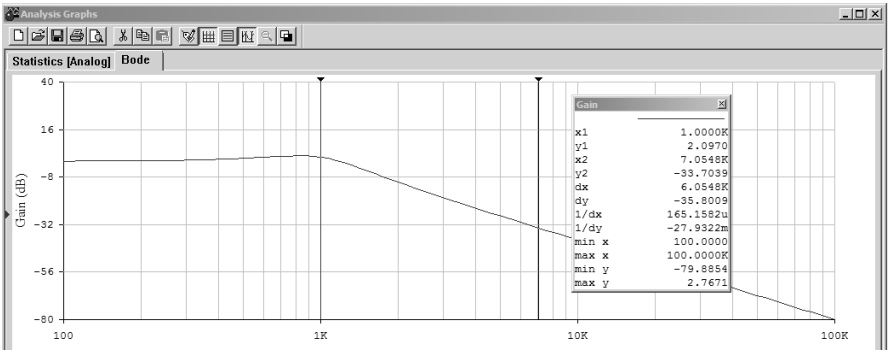


Рис. 8. Ослабление седьмой гармоники

Fig. 8. Attenuation of the 7th harmonic

Из рис. 7 и 8 видно, что третья, пятая и седьмая гармоники подавляются фильтром на частотах –22, –29 и –35 дБ соответственно. Согласно рис. 5 основная гармоника имеет уровень –3 дБ, третья существенно подавлена: уровень –50 дБ; пятая и седьмая: уровень –30 и –33 дБ соответственно. Пройдя через фильтр, высшие гармоники дополнительно уменьшатся. Разница между первой и третьей гармониками достигнет 72 дБ, между первой и пятой – 59 дБ, между первой и седьмой – 68 дБ. Девятая гармоника подавлена; следующая большая гармоника, одиннадцатая, имеет уровень –25 дБ, но фильтр подавит ее уже на уровне 43 дБ, что на 68 дБ меньше основной гармоники.

ЗАКЛЮЧЕНИЕ

Формирование шестиуровневого ступенчатого сигнала путем сложения трех прямоугольных сигналов с одинаковыми амплитудами, с длительностями и фазовыми сдвигами, указанными в настоящей статье, позволяет получить ступенчатую псевдосинусоиду с частотой, равной частоте прямоугольных сигналов. Было подтверждено, что у данного ступенчатого сигнала существенно подавлены гармоники, кратные трем, а также отсутствуют четные гармоники, что позволяет при помощи *LC*-фильтра низких частот 1-го или 2-го порядка получить синусоиду с коэффициентом гармоник существенно менее 6 %.

Предложенный способ формирования синусоидального сигнала отличается от традиционного ШИМ, формируемого при помощи пилообразного сигнала [17] тем, что частота переключения ключей равна частоте формируемой синусоиды, а не превышает ее во много раз. Это позволяет снизить потери энергии в электронных ключах.

Благодаря распределению мощности потерь в ключах на три однотипные мостовые схемы возможно получить достаточно большую выходную мощность генератора сигнала при относительно маломощных ключах.

В дальнейшем предполагается решить вопросы, связанные с практической реализацией задачи суммирования трех мощных прямоугольных сигналов для получения синусоиды на основе шестиуровневого ступенчатого сигнала.

БЛАГОДАРНОСТЬ

Авторы выражают глубокую благодарность своему наставнику доктору технических наук, профессору, заслуженному изобретателю РФ Ю.А. Пасынкову (1939–2017), чьи идеи легли в основу настоящей статьи. Всегда будем Вас помнить, Юрий Алексеевич!

СПИСОК ЛИТЕРАТУРЫ

1. Direct Digital Synthesis / K. Harrison, W. Fletcher, S. Le Roux, R. Song. – University of Cape Town Publ., 2017.

2. *Fomichev Yu.M., Silushkin S.V., Larioshina I.A.* Investigation converter circuit «Voltage-Current» for power calibrator // Journal of Physics: Conference Series. – 2015. – Vol. 671. – P. 012053.

3. *Rospawan A., Simatupang J.W., Purnama I.* A simple, cheap and precise microcontroller based DDS function generator // Journal of Electrical and Electronics Engineering. – 2019. – Vol. 3, iss. 2. – P. 118–121.

4. Harmonic current suppression strategy for grid-connected PWM converters with LCL filters / R. Zhao, Q. Li, H. Xu, Y. Wang, J.M. Guerrero // IEEE Access. – 2019. – Vol. 7. – P. 16264–16273.

5. *Ponjavic M., Milic S.* Switched capacitor compensation of supply distortion in class-D amplifiers // Electronics. – 2020. – Vol. 9, iss. 12. – P. 2197–2213.

6. Hybrid UP-PWM scheme for HERIC inverter to improve power quality and efficiency / Z. Tang, M. Su, Y. Sun, B. Cheng, Y. Yang, F. Blaabjerg, L. Wang // IEEE Transactions on Power Electronics. – 2019. – Vol. 34, iss. 5. – P. 4292–4303.

7. DC-Link current harmonic mitigation via phase-shifting of carrier waves in paralleled inverter systems / S. Baburajan, H. Wang, D. Kumar, Q. Wang, F. Blaabjerg // Energies. – 2021. – Vol. 14. – P. 4229–4244.

8. Cascaded multilevel PV inverter with improved harmonic performance during power imbalance between power cells / A. Lashab, D. Sera, F. Hahn, L. Camurca, Y. Terriche, M. Liserre, J.M. Guerrero // IEEE Transactions on Industry Application. – 2020. – Vol. 56, iss. 3. – P. 2788–2798.

9. Устройство подавления высших гармоник тока / Н.Н. Вихорев, А.И. Чивенков, Д.А. Алешин, Е.А. Чернов // Инженерный вестник Дона. – 2018. – Т. 51, вып. 4. – С. 56–65.

10. Влияние нагрузочного импеданса на третьей гармонике и выходной емкости транзистора на КПД усилителя класса F_3 / А.П. Ефимович, М.Л. Павлов, Г.В. Мазаев, В.В. Данилов, В.А. Ступак // Донецкие чтения 2017: Русский мир как цивилизационная основа научно-образовательного и культурного развития Донбасса. – Донецк, 2017. – Т. 1. – С. 193–195.

11. *Мендеров А.* Сравнение функциональных генераторов и генераторов сигналов произвольной формы // Электроника: наука, технология, бизнес. – 2021. – № 9 (210). – С. 122–125.

12. *Мишенин А.А., Лихолетов И.А.* ШИМ-сигнал и ШИМ-контроллер, их назначение // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова. – Белгород: БГТУ, 2021. – С. 3373–3375.

13. *Семенова Е.Ю., Климаш В.С.* Исследование однофазных и трехфазных инверторов напряжения с ШИМ в среде MATLAB // Научно-техническое творчество аспирантов и студентов. – Комсомольск-на-Амуре, 2018 – Т. 1. – С. 438–440.

14. *Бабичев М.М.* Реализация метода адаптивного квантования в измерительных генераторах с цифровым управлением // Системы анализа и обработки данных. – 2021. – № 2 (82). – С. 121–134. – DOI: 10.17212/2782-2001-2021-2-121-134.

15. *Максимов С.А., Пашнев В.В.* Использование техники переноса спектра сигнала для селективного подавления блокирующих сигналов // Высокопроизводительные вычислительные системы и технологии. – 2018. – № 1 (8). – С. 35–39.

16. *Зюзин А.М.* Способ построения управляемого функционального генератора // Символ науки. – 2016. – № 6-1. – С. 55–60.

17. *Бабичев М.М., Пасынков Ю.А.* Особенности ШИМ-сигнала на основе пилообразного напряжения // Актуальные проблемы электронного приборостроения (АПЭП-2016): труды 13 Международной научно-технической конференции, Новосибирск, 3–6 окт. 2016 г.: в 12 т. – Новосибирск, 2016. – Т. 1, ч. 1. – С. 291–293.

18. Седьмое поколение IGBT от IR: снизим потери при переключении / АО «КОМПЭЛ». – 2011. – 21 декабря. – URL: https://www.compel.ru/lib/54725 (дата обращения: 10.03.2023).

19. *Разуваев Ю.Ю.* Математическое моделирование усилителя мощности D-класса на основе широтно-импульсной модуляции // Вестник Воронежского государственного университета. Серия: Физика. Математика. – 2017. – № 2. – С. 46–53.

20. Способ уменьшения амплитуд высших гармоник в выходном напряжении частотного преобразователя / А.В. Стариков, С.Л. Лисин, О.С. Беляева, В.А. Кирдяшев // Вестник Самарского государственного технического университета. Серия: Технические науки. – 2021. – Т. 29, № 1. – С. 120–132.

21. *Пасынков Ю.А., Савиных М.А.* Технологический контроль метрологических характеристик счетчиков электроэнергии на производстве // Научный вестник НГТУ. – 2018. – № 1 (70). – С. 177–188. – DOI: 10.17212/1814-1196-2018-1-177-188.

Бабичев Михаил Михайлович, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – измерения интегральных характеристик периодических сигналов, измерения в электроэнергетике, способы уменьшения погрешности дискретности в генераторах фиктивной мощности, аналоговая схемотехника. E-mail: babichev@corp.nstu.ru

Григорьев Даниил Андреевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – схемотехника, встраиваемые системы. E-mail: grighoriev_daniil@mail.ru

DOI: 10.17212/2782-2230-2023-1-9-25

Formation of a stepped signal with minimum levels of the third harmonic*

M.M. Babichev[1], D.A. Grigoriev[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, senior lecturer of the Department of Information Security. E-mail: babichev@corp.nstu.ru*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: grighoriev_daniil@mail.ru*

One of the important tasks of electronic instrumentation is the creation of powerful measuring generators of a sinusoidal signal, in particular, fictitious power generators for testing and verifying electricity meters. Such generators are usually digitally controlled. Get a high efficiency allows pulse-width modulation (PWM). However, when building a device based on PWM,

* *Received 17 February 2023.*

there is a need to suppress higher-order harmonics. To simplify signal filtering, the switching frequency of the keys in the generator is increased, which reduces its efficiency. The paper presents a new method for obtaining a sinusoidal signal by adding three rectangular pulse signals having the frequency of the generated sinusoid, which makes it possible to suppress the 3rd harmonic and filter the harmonics starting from the 5th. This method allows, with high efficiency and a simple output filter, to form a sinusoid with a frequency of not only 50 Hz, but also significantly higher. The authors express deep respect to their mentor, Honored Inventor of the Russian Federation, Professor Yu.A. Pasynkov (1939-2017), whose ideas formed the basis of this article. We will always remember you, Yuri Alekseevich!

Keywords: generator, sine wave, PWM, spectrum, harmonic, filter, Electronics Workbench, simulation

REFERENCES

1. Harrison K., Fletcher W., Le Roux S., Song R. *Direct Digital Synthesis*. University of Cape Town Publ., 2017.

2. Fomichev Yu.M., Silushkin S.V., Larioshina I.A. Investigation converter circuit «Voltage-Current» for power calibrator. *Journal of Physics: Conference Series*, 2015, vol. 671, p. 012053.

3. Rospawan A., Simatupang J.W., Purnama I. A simple, cheap and precise microcontroller based DDS function generator. *Journal of Electrical and Electronics Engineering*, 2019, vol. 3, iss. 2, pp. 118–121.

4. Zhao R., Li Q., Xu H., Wang Y., Guerrero J.M. Harmonic current suppression strategy for grid-connected PWM converters with LCL filters. *IEEE Access*, 2019, vol. 7, pp. 16264–16273.

5. Ponjavic M., Milic S. Switched capacitor compensation of supply distortion in class-D amplifiers. *Electronics*, 2020, vol. 9, iss. 12, pp. 2197–2213.

6. Tang Z., Su M., Sun Y., Cheng B., Yang Y., Blaabjerg F., Wang L. Hybrid UP-PWM scheme for HERIC inverter to improve power quality and efficiency. *IEEE Transactions on Power Electronics*, 2019, vol. 34, iss. 5, pp. 4292–4303.

7. Baburajan S., Wang H., Kumar D., Wang Q., Blaabjerg F. DC-Link current harmonic mitigation via phase-shifting of carrier waves in paralleled inverter systems. *Energies*, 2021, vol. 14, pp. 4229–4244.

8. Lashab A., Sera D., Hahn F., Camurca L., Terriche Y., Liserre M., Guerrero J.M. Cascaded multilevel PV inverter with improved harmonic performance during power imbalance between power cells. *IEEE Transactionson Industry Application*, 2020, vol. 56, iss. 3, pp. 2788–2798.

9. Vikhorev N.N., Chivenkov A.I., Aleshin D.A., Chernov E.A. Ustroistvo podavleniya vysshikh garmonik toka [Harmonic current suppression device]. *Inzhenernyi vestnik Dona = Engineering Journal of Don*, 2018, vol. 51, iss. 4, pp. 56–65.

10. Efimovich A.P., Pavlov M.L., Mazaev G.V., Danilov V.V., Stupak V.A. [The influence of the load impedance at the third harmonic and the output capacitance of the transistor on the efficiency of the class F_3 amplifier]. *Donetskie chteniya 2017: Russkii mir kak tsivilizatsionnaya osnova nauchno-obrazovatel'nogo i kul'turnogo razvitiya Donbassa* [Donetsk readings 2017: Russian world as the civilizational basis for scientific, educational and cultural development of Donbass]. Donetsk, 2017, vol. 1, pp. 193–195. (In Russian).

11. Menderov A. Sravnenie funktsional'nykh generatorov i generatorov signalov proizvol'noi formy [Comparison of function and arbitrary waveform generators]. *Elektronika: nauka, tekhnologiya, biznes = Electronics: Science, Technology, Business*, 2021, no. 9 (210), pp. 122–125.

12. Mishenin A.A., Likholetov I.A. [PWM signal AND PWM controller, their purpose]. *Mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya molodykh uchenykh BGTU im. V.G. Shukhova* [International scientific and technical conference of young scientists of the Belarusian State Technical University V.G. Shukhov], Belgorod, 2021, pp. 3373–3375. (In Russian).

13. Semenova E.Yu., Klimash V.S. [Study of single-phase and three-phase voltage inverters with PWM in the MATLAB environment]. *Nauchno-tekhnicheskoe tvorchestvo aspirantov i studentov* [Scientific and technical creativity of graduate students and students], Komsomolsk-on-Amur, 2018, vol. 1, pp. 438–440. (In Russian).

14. Babichev M.M. Realizatsiya metoda adaptivnogo kvantovaniya v izmeritel'nykh generatorakh s tsifrovym upravleniem [Implementation of the adaptive quantization method in digitally controlled measuring generators]. *Sistemy analiza i obrabotki dannykh = Analysis and Data Processing Systems*, 2021, no. 2 (82), pp. 121–134. DOI: 10.17212/2782-2001-2021-2-121-134.

15. Maksimov S.A., Pashnev V.V. Ispol'zovanie tekhniki perenosa spektra signala dlya selektivnogo podavleniya blokiruyushchikh signalov [Using signal spectrum transfer technique to selectively suppress blocking signals]. *Vysokoproizvoditel'nye vychislitel'nye sistemy i tehnologii = High-performance computing systems and technologies*, 2018, no. 1 (8), pp. 35–39.

16. Zyuzin A.M. Sposob postroeniya upravlyaemogo funktsional'nogo generatora [A method for constructing a controlled functional generator]. *Simvol nauki = Symbol of science*, 2016, no. 6-1, pp. 55–60.

17. Babichev M.M., Pasynkov Yu.A. [Specific characteristics of a PWM signal based on sawtooth voltage]. *Aktual'nye problemy elektronnogo priborostroeniya*: *trudy 13 Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii (APEP-2016)* [13th International Scientific-Technical Conference on Actual problems of Electronic Instrument Engineering (APEIE-2016): proceedings]. Novosibirsk, 2016, vol. 1, pt. 1, pp. 291–293. (In Russian).

18. JSC "KOMPEL". *Sed'moe pokolenie IGBT ot IR: snizim poteri pri pereklyuchenii* [7th generation of IGBT from IR: reduce switching losses]. 2001, 21 December. Available at: https://www.compel.ru/lib/54725 (accessed 10.03.2023).

19. Razuvaev Yu.Yu. Matematicheskoe modelirovanie usilitelya moshchnosti D-klassa na osnove shirotno-impul'snoi modulyatsii [Mathematical simulation of D-class power amplifier on basis of pulse width modulation]. *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Fizika. Matematika = Proceedings of Voronezh State University. Series: Physics. Mathematics*, 2017, no. 2, pp. 46–53.

20. Starikov A.V., Lisin S.L., Belyaeva O.S., Kirdyashev V.A. Sposob umen'sheniya amplitud vysshikh garmonik v vykhodnom napryazhenii chastotnogo preobrazovatelya [Method for reducing the amplitudes of higher harmonics in the output voltage of the frequency converter]. *Vestnik Samarskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Tekhnicheskie nauki = Vestnik of Samara State Technical University. Technical Sciences Series*, 2021, vol. 29, no. 1, pp. 120–132.

21. Pasinkov Y.A., Savinykh M.A. Tekhnologicheskii kontrol' metrologicheskikh kharakteristik schetchikov elektroenergii na proizvodstve [Technological control of metrological characteristics of electricity meters during production]. *Nauchnyi vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta = Science bulletin of the Novosibirsk state technical university*, 2018, no.1 (70), pp. 177–188. DOI: 10.17212/1814-1196-2018-1-177-188.

Для цитирования:

Бабичев М.М., Григорьев Д.А. Формирование ступенчатого сигнала с минимальными уровнями третьей гармоники // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 9–25. – DOI: 10.17212/2782-2230-2023-1-9-25.

For citation:

Babichev M.M., Grigoriev D.A. Formirovanie stupenchatogo signala s minimal'nymi urovnyami tret'ei garmoniki [Formation of a stepped signal with minimum levels of the third harmonic]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 1 (108), pp. 9–25. DOI: 10.17212/2782-2230-2023-1-9-25.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 1 (108). – 26–35

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 004.056.5 DOI: 10.17212/2782-2230-2023-1-26-35

АНАЛИЗ ПРОТОКОЛОВ БЕЗОПАСНОСТИ НА БАЗЕ СИСТЕМЫ РАСПРОСТРАНЕНИЯ ЛИЦЕНЗИРУЕМОГО КОНТЕНТА*

А.Д. АНИКИН[1], К.А. БИРЮКОВ[2], А.Б. АРХИПОВА[3]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: anikin.2020@stud.nstu.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: k.biryukov.2020@stud.nstu.ru*
[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, доцент кафедры защиты информации. E-mail: arhipova@corp.nstu.ru*

В последние годы число кибератак значительно выросло. Большинство предприятий нуждается в надежной защите внутрикорпоративной сети. Системы предотвращения вторжений позволяют своевременно автоматически реагировать на угрозы различного рода, которые не могут быть идентифицированы с помощью файрволлов, антивирусов и других систем безопасности. На рынке представлено много компаний, предоставляющих свои сигнатуры правил для внедрения в системы предотвращения вторжений, разработанные производителями сетевого оборудования или персонального обеспечения. Существует необходимость сохранения конфиденциальности данных правил с реализацией возможности применения на устройствах коммерческих пользователей. Для этого разрабатываются системы распространения лицензионного контента на устройства потребителей. Однако необходимо обеспечивать высокий уровень безопасности подобных систем во избежание утечек секретных данных, предоставленных сторонними вендорами.

Ключевые слова: система обнаружения вторжений, система предотвращения вторжений, Eltex Distribution Manager, безопасность, шифрование, система, правила, угрозы, конфиденциальность, ключ шифрования, проверка подлинности, контроль доступа, сигнатуры.

* Статья получена 16 февраля 2023 г.

ВВЕДЕНИЕ

Надежные системы обнаружения и предотвращения вторжений (Intrusion Detection System (IDS), Intrusion Prevention System (IPS)) становятся необходимостью, учитывая экспоненциально растущее число кибератак [1]. Системы обнаружения и предотвращения вторжений анализируют трафик на основе набора правил и реагируют согласно настроенным параметрам на сетевые атаки или аномалии [2].

Компании, специализирующиеся на кибербезопасности, создают инновационные технологии потокового сканирования и системы правил, предназначенные для обнаружения наиболее опасных и широко распространенных угроз. Positive Technologies на основе продукта Positive Technologies Expert Security Center и Лаборатория Касперского на базе инфраструктуры безопасности Kaspersky Security Network с поддержкой Kaspersky SafeStream II предоставляют наборы сигнатур, позволяющие обнаруживать вредоносное программное обеспечение во всех типах трафика [3, 4].

Работа системы IPS / IDS на маршрутизаторах ESR производства компании Eltex основана на сигнатурном анализе трафика. Наборы правил можно получать из открытых источников, таких как Suricata – системы обнаружения сетевых вторжений, которая использует наборы правил для отслеживания сетевого трафика и создает оповещения при обнаружении подозрительных событий [5]. Но более надежным источником сигнатур для систем IPS / IDS являются коммерческие поставщики. Для работы системы предотвращения вторжений на маршрутизаторе необходимо лицензировать устройство и получить правила коммерческих вендоров посредством настройки взаимодействия с централизованной системой распространения лицензируемого контента Eltex Distribution Manager (EDM).

1. ПОСТАНОВКА ЗАДАЧИ

- Рассмотреть алгоритмы взаимодействия системы EDM с пользовательским устройством.
- Провести анализ мер безопасности в случае реализации угроз в системе EDM.

2. СОСТАВ СИСТЕМЫ

Рассмотрим базовый состав компонентов системы.

- EDM Root – корневой сервис EDM, работающий на стороне компании Eltex. В его задачи входит взаимодействие с клиентскими устройствами и

пользовательскими сервисами EDM и передача на них запрошенного в рамках лицензий контента, предоставленного коммерческими вендорами [6].

- Клиентское устройство (маршрутизатор) является потребителем распространяемого EDM контента – правил лицензионных вендоров с использованием полученных сигнатур в работе системы IPS / IDS [6].

3. АЛГОРИТМЫ РАБОТЫ

I. Проверка подлинности

При подключении маршрутизатора к EDM необходимо провести его аутентификацию для подтверждения подлинности клиентского устройства и идентификации его в базе лицензионного менеджера. Алгоритм идентификации компонентов системы состоит из двух этапов: проверка подлинности Root-сервера и проверка подлинности клиентского устройства. Рассмотрим данные алгоритмы подтверждения оригинальности компонентов системы.

Проверка подлинности Root-сервера:

1) ESR генерирует уникальный код и шифрует его своим секретным ключом, получая соответствующую подпись устройства;
2) подпись передается Root-серверу в запросе аутентификации;
3) Root проверяет валидность данных ESR и действительность его лицензии;
4) Root расшифровывает специальным ключом и отправляет обратно уникальный код устройства;
5) ESR проверяет код, убеждаясь в подлинности Root-сервера.

В результате происходит подтверждение подлинности Root-сервера, что позволяет избежать такой угрозы, как подмена Root-сервера, и дальнейшей компрометации данных лицензий.

Проверка подлинности клиентского устройства:

1) Root-сервер генерирует уникальный код и шифрует его сгенерированным ключом, получая специальную подпись;
2) подпись передается в ответ на запрос аутентификации в ESR;
3) ESR расшифровывает подпись своим ключом и отправляет полученное значение;
4) Root-сервер проверяет данные, убеждаясь в подлинности ESR.

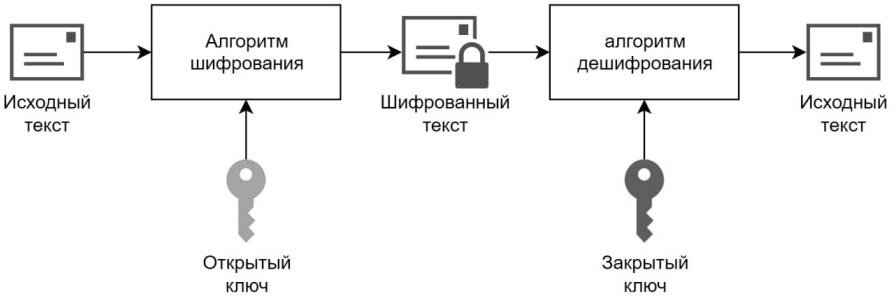
Ключи шифрования генерируются на основе уникальных параметров устройства с помощью алгоритма, разработанного компанией-производителем, благодаря чему обеспечивается уникальность данных значений и снижается вероятность компрометации ключей в результате попытки их генерации путем подделки данного алгоритма.

Таким образом, проверка подлинности каждого компонента системы позволяет свести к минимуму возможность фальсификации каких-либо компонентов системы и обеспечить сохранность правил, предоставленных вендорами.

II. Замена компонента системы

Однако возможна ситуация, когда компонент системы со стороны заказчика был заменен на новый, вследствие чего возникала необходимость актуализации ключей шифрования. Рассмотрим алгоритм работы системы в случае замены устройства.

Перед запросом клиентского устройства менеджером лицензий на получение правил производится проверка актуальности ключей для расшифровки получаемых данных. Проверяется актуальность ключа шифрования. В случае изменения ключа или вовсе его отсутствия в первую очередь выполняется обновление соответствующих данных, иначе клиентское устройство не сможет расшифровать полученные от Root правила. Так как используются симметричные алгоритмы шифрования для обмена ключами, которые уязвимы для модификации данных в канале связи, в том числе для атаки «Man-in-the-middle» (человек посередине), используются дополнительные методы односторонней или двусторонней аутентификации [7].



Алгоритм симметричного шифрования

Symmetric cryptographic algorithm

4. УГРОЗЫ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ В EDM

I. Перехват или подмена правил при передаче – реализация вышеупомянутой атаки «Man-in-the-middle» [8]

Методы предотвращения

1. Использование криптографического протокола обмена ключами при передаче контента.

2. Использование дополнительных методов односторонней или двусторонней аутентификации.

II. Компрометация алгоритмов генерации ключей ESR

Методы предотвращения

1. Реализация алгоритмов с учетом математической сложности декомпиляции данных. Сложность декомпиляции данных вызвана следующими особенностями [9].

1.1. Согласно архитектуре фон Неймана, данные и инструкции в памяти представляются в одинаковом виде. Следовательно, рассмотрев случайную последовательность байт из бинарного файла, будет невозможно однозначно прийти к выводу, что данный набор правил является инструкцией или данными. В случае, если процессор поддерживает разделение сегментов кода и данных, какая-то часть данных (например, таблицы ветвлений типа case) может всё равно остаться в сегменте кода.

1.2. Самомодифицирующийся код. Иногда программы могут использовать одни и те же адреса памяти для хранения исполняемого кода и данных, например, для экономии памяти, шифрования кода [10].

1.3. Идиомы. Идиома – это последовательность инструкций, которая формирует логическую единицу, действие, которое не является просто использованием первичного назначения используемых инструкций [11].

2. Осуществление контроля доступа к документации и исходникам прошивок.

3. Запрет удаленного доступа к критически важным системам.

III. Разведка – различные попытки определить алгоритм шифрования и авторизации [12]

Методы предотвращения

1. На Root-сервере IP-адрес автоматически блокируется в случае фиксации с этого IP-адреса большого количества обращений за отведенный интервал времени, в которых указаны неизвестный серийный номер или мак-адрес.

2. Блокировка IP-адреса в случае обнаружения попыток перебора.

IV. Расшифровка полученных правил на устройстве с легальной подпиской

Методы предотвращения

1. Шифрование правил для их дальнейшего хранения с использованием оптимальных с точки зрения криптостойкости и затратности по памяти и времени алгоритмов [13].

2. Запрет Root-доступа на устройство [14].

3. Защита прошивки цифровой подписью, что затрудняет установку неофициальных прошивок с возможностью компрометирования алгоритмов шифрования [15].

V. Подделка подписки – существует одно устройство с легальной подпиской, остальные устройства пытаются имитировать легальное

Методы предотвращения

1. Для генерации ключа используются уникальные параметры устройства.

2. Ограничение числа IP-адресов, с которых возможна авторизация для одного конкретного устройства. Если для устройства, успешно проходящего аутентификацию, фиксируется превышение лимита изменения IP-адресов за отведенное время, то эта персональная лицензия автоматически отзывается.

5. ИНСТРУКЦИИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Несмотря на весьма исчерпывающий набор протоколов противодействия различным видам угроз, нельзя исключать возможность компрометации алгоритма генерации ключей. На этот случай компанией была разработана следующая инструкция реагирования на данный инцидент.

1. Разрабатывается версия EDM с поддержкой нового и старого протокола.

2. Разрабатываются прошивки ESR с поддержкой нового протокола.

3. Проходит стандартная процедура тестирования версии EDM.

4. Обновляется продукт на стороне компании.

5. Производится информационная рассылка клиентам о необходимости обновления прошивок на устройствах.

6. Выпускаются новые версии прошивок ESR и EDM.

7. Отключается поддержка старого (скомпрометированного) протокола на ESR.

ЗАКЛЮЧЕНИЕ

Система передачи лицензируемого контента имеет широкий спектр протоколов безопасности на случай реализации различных угроз. Рассмотренные алгоритмы аутентификации компонентов системы распространения лицензируемого контента реализованы на высоком уровне безопасности. Протоколы передачи данных спроектированы с учетом возможности противодействия большинству самых распространенных видов атак. А в случае компрометации алгоритмов шифрования у компании имеется инструкция реагирования на данный инцидент.

СПИСОК ЛИТЕРАТУРЫ

1. *Chaudhuri A.* For the public sector, cyber resilience has never been more important / World Economic Forum. – 2022. – 18 July. – 13 p.

2. *Abdelkarim A.A., Nasereddin H.H.O.* Intrusion prevention system // International Journal of Academic Research. – 2011. – Vol. 3, N 1. – P. 432–433.

3. Positive Technologies: web-сайт. – URL: https://www.ptsecurity.com/ru-ru/services/ (дата обращения: 10.03.2023).

4. Kaspersky: web-сайт. – URL: https://www.kaspersky.ru/safestream2 (дата обращения: 10.03.2023).

5. Suricata: website. – URL: https://suricata.readthedocs.io/en/latest/what-is-suricata.html (accessed: 10.03.2023).

6. Eltex Distribution Manager (EDM). Руководство по эксплуатации. Версия ПО 1.1.

7. *Alenezi M.N., Alabdulrazzaq H.K., Mohammad N.Q.* Symmetric encryption algorithms: review and evaluation study // International Journal of Communication Networks and Information Security. – 2020. – Vol. 12, N 2. – P. 256–272.

8. Revisiting man-in-the-middle attacks against HTTPS / V. Kampourakis, G. Kambourakis, E. Chatzoglou, C. Zaroliagis // Network Security. – 2022. – Vol. 2022, N 3. – DOI: 10.12968/S1353-4858(22)70028-1.

9. *Щеглов К.Е.* Обзор алгоритмов декомпиляции // Исследовано в России. – 2001. – Ст. 116. – С. 1143–1158.

10. *Аветисян К.Р., Аидру А.В.* Применение принципов динамического полиморфизма при компиляции приложения с целью повышения его криптостойкости // Вестник Московского университета МВД России. – 2016. – № 2. – С. 213–215.

11. *Khanna T.* Rule-based pre-processing of idioms and non-compositional constructions to simplify them and improve black-box machine translation: Thesis / International Institute of Information Technology. – Hyderabad, 2021. – 62 p.

12. *Авдошин С.М., Савельева А.А.* Криптоанализ: современное состояние и перспективы развития // Информационные технологии. – 2007. – № S3. – С. 1–32.

13. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish / P. Patila, P. Narayankarb, D.G. Narayan, S.M. Meena // Procedia Computer Science – 2016. – Vol. 78. – P. 617–624.

14. *Ferraiolo D.F., Kuhn D.R.* Role-based access controls // 15th National Computer Security Conference, Oct. 13–16, 1992. – Baltimore, 1992. – P. 554–563.

15. Interrupt.memfault: website. – URL: https://interrupt.memfault.com/blog/secure-firmware-updates-with-code-signing (accessed: 10.03.2023).

Аникин Андрей Дмитриевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные сети. E-mail: anikin.2020@stud.nstu.ru

Бирюков Кирилл Андреевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные сети. E-mail: k.biryukov.2020@stud.nstu.ru

Архипова Анастасия Борисовна, доцент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – математическое моделирование в информационной безопасности. E-mail: arhipova@corp.nstu.ru

DOI: 10.17212/2782-2230-2023-1-26-35

Analysis of security protocols based on the licensed content distribution system*

A.D. Anikin[1], K.A. Biryukov[2], A.B. Arkhipova[3]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: anikin.2020@stud.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: k.biryukov.2020@stud.nstu.ru*
[3] *Novosibirsk State Technical University, Karl Marx Prospekt, 20, Novosibirsk, 630073, Russian Federation, Associate Professor of the Department of Information Security. E-mail: arhipova@corp.nstu.ru*

In recent years, the number of cyberattacks has increased significantly. Most enterprises need reliable protection of the intracorporate networks. Intrusion prevention systems allow timely and automatic response to threats of various kinds that cannot be identified by firewalls, anti-viruses and other security systems. Many companies are represented on the market, providing their signatures to implement intrusion prevention systems developed by manufacturers of network equipment or personal security. There is a need to preserve the confidentiality of these rules with the implementation of the possibility of application on devices commercial users. That's why systems for the distribution of licensed content to consumer devices are being developed. However, it is necessary to ensure a high level of security of such systems, to avoid leaks of classified data provided by third-party vendors.

Keywords: Intrusion Detection System, Intrusion Prevention System, EDM, security, encryption, system, rules, threats, confidential, encryption key, authentication, access control, signatures

REFERENCES

1. Chaudhuri A. *For the public sector, cyber resilience has never been more important*. World Economic Forum, 2022, 18 July. 13 p.

2. Abdelkarim A.A., Nasereddin H.H.O. Intrusion prevention system. *International Journal of Academic Research*, 2011, vol. 3, no. 1, pp. 432–433.

3. *Positive Technologies*. Website. (In Russian). Available at: https://www.ptsecurity.com/ru-ru/services/ (accessed 10.03.2023).

4. *Kaspersky*. Website. (In Russian). Available at: https://www.kaspersky.ru/safestream2 (accessed 10.03.2023).

5. *Suricata*. Website. Available at: https://suricata.readthedocs.io/en/latest/what-is-suricata.html (accessed 10.03.2023).

* *Received 16 February 2023.*

6. *Eltex Distribution Manager (EDM)*. User manual. Version 1.1.

7. Alenezi M.N., Alabdulrazzaq H.K., Mohammad N.Q. Symmetric encryption algorithms: review and evaluation study. *International Journal of Communication Networks and Information Security*, 2020, vol. 12, no. 2, p. 256–272.

8. Kampourakis V., Kambourakis G., Chatzoglou E., Zaroliagis C. Revisiting man-in-the-middle attacks against HTTPS. *Network Security*, 2022, vol. 2022, no. 3. DOI: 10.12968/S1353-4858(22)70028-1.

9. Shcheglov K.E. Obzor algoritmov dekompilyatsii [Overview of decompilation algorithms]. *Issledovano v Rossii = Investigated in Russia*, 2001, art. 116, pp. 1143–1158.

10. Avetisyan K.R., Aidru A.V. Primenenie printsipov dinamicheskogo polimorfizma pri kompilyatsii prilozheniya s tsel'yu povysheniya ego kriptostoikosti [Application of the principles of dynamic polymorphism at compilation of the appendix on purpose increase of its cryptofirmness]. *Vestnik Moskovskogo universiteta MVD Rossii = Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 2016, no. 2, pp. 213–215.

11. Khanna T. *Rule-based pre-processing of idioms and non-compositional constructions to simplify them and improve black-box machine translation*. Thesis. International Institute of Information Technology. Hyderabad, 2021. 62 p.

12. Avdoshin S.M., Savelieva A.A. Kriptoanaliz: sovremennoe sostoyanie i perspektivy razvitiya [Cryptanalysis: current state and future trends]. *Informatsionnye tekhnologii = Information Technologies*, 2007, no. S3, pp. 1–32.

13. Patila P., Narayankarb P., Narayan D.G., Meena S.M. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, 2016, vol. 78, pp. 617–624.

14. Ferraiolo D.F., Kuhn D.R. Role-based access controls. *15th National Computer Security Conference*, Baltimore, Oct. 13–16, 1992, pp. 554–563.

15. *Interrupt.memfault.* Website. Available at: https://interrupt.memfault.com/blog/secure-firmware-updates-with-code-signing (accessed 10.03.2023).

Для цитирования:

Аникин А.Д., Бирюков К.А., Архипова А.Б. Анализ протоколов безопасности на базе системы распространения лицензируемого контента // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 26–35. – DOI: 10.17212/2782-2230-2023-1-26-35.

For citation:

Anikin A.D., Biryukov K.A., Arkhipova A.B. Analiz protokolov bezopasnosti na baze sistemy rasprostraneniya litsenziruemogo kontenta [Analysis of security protocols based on the licensed content distribution system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 1 (108), pp. 26–35. DOI: 10.17212/2782-2230-2023-1-26-35.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 1 (108). – 36–52

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 004.58 DOI: 10.17212/2782-2230-2023-1-36-52

ВОПРОСЫ ЛИЧНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЭКОНОМИКИ, УПРАВЛЕНИЯ И ОБЩЕСТВЕННЫХ КОММУНИКАЦИЙ*

М.Е. БОЧАРНИКОВА[1], Т.М. ПЕСТУНОВА[2], В.В. СЕЛИФАНОВ[3]

[1] *630090, РФ, Новосибирская область, г. Новосибирск, ул. Пирогова, 2, Новосибирский государственный университет, ассистент кафедры компьютерных систем. E-mail: m.bocharnikova@g.nsu.ru*
[2] *630090, РФ, Новосибирская область, г. Новосибирск, ул. Пирогова, 2, Новосибирский государственный университет, кандидат технических наук, доцент кафедры компьютерных систем. E-mail: t.pestunova@g.nsu.ru*
[3] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru*

В статье дается анализ основных аспектов личной информационной безопасности, знание которых важно для человека в условиях высоких темпов цифровизации социальной и экономической сферы. Они направлены на формирование персонального информационного цифрового пространства и управление им в условиях изменяющихся технологий и правового поля в соответствии с частными и деловыми интересами личности. Первой задачей при этом является осознание человеком своих интересов и потребностей в использовании цифровой среды, а также оценка значимости вопросов безопасности своих персональных данных. Далее обращается внимание на выработку навыков анализа и оценки интернет-ресурсов в контексте достоверности и целей распространения информации, освоение доступных в рамках действующего законодательства методов и средств управления своими персональными данными. Рассмотрены примеры ряда других актуальных задач, существующие возможности практического получения знаний и формирования навыков безопасной работы в цифровой среде для различных категорий пользователей на современном уровне развития информационных технологий, а также обозначены те аспекты, которые пока остаются за рамками методов и технологий, массово используемых для повышения уровня цифровой грамотности населения.

Ключевые слова: информационная безопасность, защита информации, цифровая грамотность, персональные данные, цифровая экономика

* Статья получена 16 февраля 2023 г.

ВВЕДЕНИЕ

Цифровизация экономической и социальной сферы вовлекает в орбиту информационных технологий огромное число пользователей, поскольку одним из краеугольных принципов цифровой экономики является персонализация товаров и услуг. Современный человек всё бóльшую часть жизненных потребностей удовлетворяет посредством цифрового потребления с применением электронной информации и цифровых сервисов для достижения личных целей, решения образовательных или производственных задач. В этих условиях растут риски информационной безопасности (далее – ИБ), вызванные ошибками, легкомыслием, небрежностью и недостаточной цифровой грамотностью людей при работе с многочисленными электронными сервисами, а также действиями злоумышленников, направленными против них, ради получения выгоды. Реализация этих рисков может приводить и уже приводит к ощутимому ущербу как для конкретных людей, так и для организаций, где они работают. Угрозы в информационной сфере, с одной стороны, могут иметь нарушения значимых для деятельности человека качеств информации (конфиденциальность, целостность, доступность и др.), а с другой – навязывать человеку некую информацию с целью формирования такой модели его поведения, при которой он будет совершать действия в интересах третьих лиц, даже не понимая этого. В результате осознания этих рисков в последние годы многократно возросло внимание к проблеме персональной (личной) ИБ как со стороны государства, так и со стороны отдельных отраслей. Так, в число основных направлений в Доктрине информационной безопасности входит «обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности» [1]. Одной из задач национальной программы развития цифровой экономики России является повышение цифровой грамотности населения, что включает и вопросы цифровой безопасности. В статье дается анализ основных аспектов персональной ИБ, изучение которых важно для различных категорий пользователей для снижения негативных последствий от реализации информационных рисков в условиях

1. ЦЕЛИ И ЗАДАЧИ ЛИЧНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Реализация принципа персонализации приводит к накоплению и обработке в глобальной цифровой среде огромных объемов разнообразных данных, которые либо являются *персональными данными* (далее – ПД), либо могут ими стать спустя какое-то время, часто их называют «социальные данные».

На правовом уровне регулирование этих процессов осуществляется посредством законодательства о ПД, целью которого является «обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну» [2]. Достижение целей закона обеспечивается, с одной стороны, предъявлением к организациям-операторам требований о целенаправленности и законности обработки ПД, их актуальности и безызбыточности по отношению к заявленным целям, обеспечению их безопасности. В любом случае необходимо получение согласия субъекта на обработку его ПД (за исключением ряда случаев, прямо указанных в законе). А с другой стороны, субъект ПД имеет право получать от оператора сведения об обработке своих ПД (в том числе о содержании ПД, целях и способах обработки, мерах безопасности), требовать обеспечения актуальности обрабатываемых данных и по желанию отзывать данное ранее согласие на обработку ПД.

Цифровизация бизнес-процессов и концентрация ПД в электронной среде таит немало «подводных камней», которые могут привести к нарушению интересов и прав субъекта ПД, обостряя противоречия между ним и операторами, собирающими и обрабатывающими ПД. Эти противоречия – следствие того, что оператор для повышения эффективности бизнес-процессов стремится расширить состав используемых ПД сверх того, что нужно для целей, установленных в согласии на обработку. Таким образом, цели обработки ПД для субъекта и оператора перестают совпадать.

Данные о личности в цифровой среде, которые могут обрабатываться оператором, можно разделить на три основные группы. Первая группа – первичные данные – это те данные, которые человек предоставляет оператору и на обработку которых он дает согласие. Вторая группа – назовем их дополнительными данными – это данные, которые оператор накапливает в процессе использования человеком соответствующих электронных сервисов (сведения о платежных транзакциях, телефонных звонках, приобретении товаров и услуг и т. п.). Обработка данных, типовых для конкретного электронного бизнеса, также может быть учтена в согласии, однако по мере цифровизации их содержание может существенно расшириться, а цель использования может оказаться совсем не той, которая заявлена при получении согласия. Третья группа – данные о человеке, которые оператор может получить из общедоступных источников (например, из соцсетей, личных страниц на интернет-ресурсах и т. д.) – социальные данные. Даже если эти данные используются для законных целей и получены легитимным путем, то достоверность и актуальность их отнюдь не гарантированы, а следовательно, не гарантирована и корректность решений, принятых на их основе. Важно заметить, что в действующей редакции закона о персональных данных имеются положения,

помогающие человеку регулировать распространение своих персональных данных, размещенных по его желанию на общедоступных ресурсах. Определена особая категория – «персональные данные, разрешенные субъектом персональных данных для распространения» [2], на обработку которых каждый заинтересованный в этом оператор должен получить отдельное согласие субъекта ПД, однако далеко не все люди знают об этих возможностях и о том, как их реализовать. Одной из наиболее критичных для субъекта ПД является ситуация, когда для сбора и обработки указанных данных используются формальные алгоритмы (в том числе интернет-роботы, нейросети и другие средства искусственного интеллекта), и исключительно на основе результатов такого анализа в отношении человека принимаются решения, имеющие юридические, финансовые и другие последствия для него. При этом подобные решения могут быть исполнены автоматически в информационной системе (без участия сотрудника оператора). Человек же узнает об этом только постфактум, когда, например, обнаружит блокирование своего банковского счета или невозможность выезда за границу из-за долга своего тезки-однофамильца, получит отказ в трудоустройстве от работодателя или в получении кредита в банке из-за фейковой информации в соцсетях. Поток такого рода примеров нарастает очень быстрыми темпами. Законодательство и практика его применения явно не успевает за развитием цифровых технологий. В погоне за цифровизацией новых сфер государство и бизнес не спешат исправлять даже регулярно появляющиеся и признанные проблемы. Проблема «тезок-однофамильцев» – один из ярких примеров, решить который можно было бы установлением адекватных требований к минимально необходимой информации для идентификации человека как в государственных, так и в иных информационных системах, а до этого времени – как минимум упрощением процедур «восстановления правды» и отменой автоматических действий, которые могут нанести существенный ущерб человеку. Проблема соотнесения личности человека с его цифровым образом, на основании которого в отношении него принимаются те или иные решения, становится серьезной проблемой обеспечения защиты прав субъекта ПД в цифровой реальности.

Актуальный подход в защите данных о личности в цифровой среде основан на тезисе о том, что данные в цифровой среде принадлежат тому, о ком эти данные. Он изложен в Общем регламенте защиты данных (General Data Protection Rools, GDPR), развивающем положения Конвенции СЕ № 108 о защите данных с учетом процессов цифровизации. Но и в условиях действующей правовой базы в сфере ПД многое (хотя, безусловно, далеко не всё!) зависит от степени понимания человеком значимости этой проблемы, его желания и ответственного отношения к управлению своими ПД и связанной с ними информацией в цифровой среде. Знание правовых основ защиты ПД,

понимание рисков организации бизнес-процессов в цифровой среде, умение работать с соблюдением основных правил ИБ при применении электронных сервисов могут существенно снизить вероятность попадания в ситуации, чреватые ущербом от использования цифровых технологий.

Исходя из сказанного, в условиях цифровой трансформации экономической и социально-культурной сферы можно сформулировать *цель личной ИБ – формирование на основе частных и деловых интересов персонального информационного цифрового пространства и управление им в условиях изменяющихся информационных технологий и правового поля.*

Отправной точкой для достижения поставленной цели является *задача осознания человеком своих интересов и потребностей в использовании цифровой среды, а также необходимых аспектов безопасности своих ПД* как основы при принятии решений об их предоставлении и распространении в цифровом пространстве. Для этого необходимо научиться соотносить цель, объем, условия и способы обработки ПД операторами с собственными потребностями и интересами использования цифровых сервисов (профессиональными, образовательными и др.). Формирование персонального информационного цифрового пространства основано, с одной стороны, на желании человека решать свои задачи и осуществлять коммуникации с использованием новых информационных технологий, с другой – на умении поиска сервисов, обеспечивающих реализацию тех или иных его потребностей, а в-третьих – на понимании рисков ПД, обусловленных выбранным набором ресурсов и сервисов. В частности, особо внимательно надо относиться к применению широко рекламируемых ныне сервисов, требующих предоставления биометрических данных. Информационные сервисы, используемые для решения задач, связанных с частной жизнью (управление финансами, покупка товаров, госуслуги, образование, билеты, новостной интернет-серфинг, соцсети и другие сервисы для общения и развлечения), развиваются очень быстро, высокими темпами растет и количество их пользователей. Заметим, что пандемия COVID-19 стала мощным «ускорителем» этих процессов. Но в условиях, когда далеко не все разработчики придерживаются практик безопасного программирования, это приводит к росту уязвимого ПО и связанных с ними кибератак. А массовый переход сотрудников на дистанционную работу существенно повышает и риски корпоративным информационным ресурсам из-за того, что пользователи не всегда следуют требованиям корпоративных политик безопасности, работая за пределами офиса. Эффективный поиск, выбор и безопасное использование информационных сервисов в профессиональной деятельности и для обеспечения своих частных интересов – один из важнейших навыков для современного человека.

Вторая ключевая задача при формировании личного информационного пространства – научиться анализировать и оценивать интернет-ресурсы в контексте достоверности и целей распространения информации. События последнего года наглядно продемонстрировали всем людям, насколько жесткой может быть «фейковая война» и каковы ее возможности по навязыванию обществу представлений о происходящих событиях на основе псевдофактов. Но опасность попасть на уловки мошенников высока и в обычной жизни, что требует не только знаний, но ряда важных умений и навыков, касающихся выявления фишинговых и других небезопасных сайтов, противодействовия агрессивной таргетированной рекламе, оценки источников и достоверности представленной информации.

Третья важная задача состоит в освоении доступных в рамках действующего законодательства методов и средств управления своими персональными данными. Закон о ПД в целом предоставляет человеку немалые возможности в этом направлении, однако большинство пользователей слабо знакомы с ними и в еще меньшей степени готовы ими пользоваться. Например, нередко складывается ситуация, когда операторы включают в согласие об обработке ПД большое количество необязательных данных (например, в своих маркетинговых целях), а человек не решается их вычеркнуть из своего согласия или хотя бы поинтересоваться у оператора, зачем именно эти данные нужны, ограничиваясь последующим высказыванием недовольства в частных разговорах с коллегами и друзьями. Пользователи далеко не всегда обращают внимание на мелкий шрифт в электронных формах с текстом о согласии на получение рекламной информации и услужливо проставленной «галочкой», которую можно просто убрать, чтобы избежать ненужных писем, звонков и SMS. Еще реже пользуются правом отказа от обработки ПД после того, как их предоставили. Имеющийся личный опыт показывает, что решение многих вопросов не требует больших усилий, но человеку важно знать свои права и порядок их реализации, а также существующие уже сейчас способы и инструменты управления ПД, в том числе возможность ограничить распространение и использование своих данных. Эта задача согласуется с задачей проекта «Информационная безопасность» в национальной программе «Цифровая экономика РФ» [3] – обеспечить «контроль обработки и доступа к персональным, большим пользовательским данным, в том числе в социальных сетях и прочих средствах социальной коммуникации, а также возможность отзыва или уменьшения объема ранее данного согласия на обработку персональных данных».

Четверная входящая в сферу личной ИБ задача – освоение практических навыков безопасной работы при использовании цифровых технологий. Удобство и безопасность часто находятся на разных чашах весов при выборе и ис-

пользовании информационных технологий. Пользователи далеко не всегда в достаточно полной мере знают о существующих информационных рисках, а между тем социальная инженерия вкупе с вредоносным программным обеспечением стабильно занимает лидирующие позиции в статистике атак на информационные системы. Вопросы ИБ не всегда изучаются в качестве отдельных дисциплин в вузах, а часто входят обзорно в другие курсы (например, в информатику), где их можно осветить лишь обзорно [4], что недостаточно для формирования умений и навыков по безопасной работе в цифровой среде. С точки зрения актуальных угроз и способов обеспечения личной ИБ следует обратить внимание на обучение по следующим аспектам. *Аутентификационная информация* является одним из основных объектов атак, поэтому пользователи при использовании любых информационных технологий должны уметь обеспечить надежность и защищенность своей аутентификации (создание сложных паролей, конфиденциальность при хранении и передаче по сети, своевременная замена, конфиденциальность ключевой и парольной информации при использовании съемных электронных носителей – смарт-карт, токенов и др.). *Социальная инженерия* (фишинг: почтовый, телефонный, SMS, интернет) является доминирующим видом атак на пользователей, поэтому умение оперативно определить эту угрозу и правильно отреагировать («не клюнуть на удочку») – насущная потребность для всех пользователей и при работе в корпоративных информационных системах, и при использовании информационных технологий в личных целях. *Вредоносное программное обеспечение* – еще одна давняя, но не теряющая с годами своей актуальности угроза, уметь противодействовать которой должен каждый пользователь. Установка антивируса является началом этой работы, но далее важно не забывать о его правильной настройке, обновлении баз и других деталях (например, о том, что файл, открытый на «недопроверенной» антивирусом «флэшке», вполне может стать источником заражения компьютера), уметь обращать внимание и правильно реагировать на признаки возможных заражений. Следующий обширный блок – *правила безопасной работы с интернет-ресурсами*. Пользователь должен различать безопасное и небезопасное соединение, понимать риски «бездумного» перехода по ссылкам, проявлять осторожность при скачивании информации с интернет-ресурсов, контролировать следующее: безопасность при работе с сайтами, содержащими регистрационные сервисы, особенности угроз и обеспечения безопасности при работе с электронной почтой и в соцсетях, правила безопасности при совершении электронных финансовых операций, риски использования облачных сервисов. Работая на персональном компьютере, надо уметь настраивать основные функции безопасности браузеров, понимать уязвимости полезных на первый взгляд функций (например, автозаполнение полей и сохранение паролей),

настраивать параметры встроенных инструментов безопасности в соответствии со своими потребностями, а также обеспечить безопасность домашнего подключения к сети.

Поскольку одними из самых распространенных устройств доступа в интернет являются смартфоны и другие мобильные устройства, то *безопасность при работе с ними* – еще одна важная тема в личной информационной безопасности. Она имеет много общего с рассмотренной выше проблематикой интернет-безопасности, но есть немало специфических угроз и уязвимостей, характерных именно для мобильных устройств. В частности, в случае утраты устройства уметь избежать ущерба из-за случайного разглашения персональных данных или не допустить такой утечки при желании избавиться от надоевшего устройства (продать, подарить, выбросить), понимать риски неконтролируемого использования видеокамер, диктофонов, геолокации и других встроенных сервисов.

С развитием юридически значимого электронного документооборота и отказом от электронных оригиналов документов во многих сферах деятельности особое значение для пользователей приобретают *навыки обеспечения безопасности при применении электронной подписи*. Они должны иметь представление о принципах функционирования таких технологий и их уязвимостях, знать установленные законодательством виды электронных подписей и понимать, с какими из них они реально работают, знать соответствующие правила безопасности, а также условия признания подписанных электронных документов равнозначными документами на бумажном носителе с собственноручной подписью.

В целях *управления своими персональными данными* пользователю необходимо знать правовые аспекты этой сферы и электронные сервисы взаимодействия с операторами и уполномоченным органом по защите прав субъектов персональных данных, возможности ознакомления со своими ПД и контроля законности их обработки, особенности заполнения и отзыва согласия на обработку ПД (в том числе согласие на обработку ПД, разрешенных для распространения) и т. п.

«Нестареющими» важными темами являются обеспечение *доступности и целостности информации, методы ее резервирования и восстановления.*

С учетом высоких темпов изменчивости цифровой среды проблематика личной информационной безопасности не стоит на месте и постоянно расширяется, охватывая вопросы безопасности, присущие качественно новым информационным технологиям, которые уже стали достаточно массовыми или станут таковыми в ближайшей перспективе. К подобным технологическим новациям можно отнести интернет вещей, умный дом, блокчейн, многочисленные цифровые сервисы на основе искусственного интеллекта, беспилот-

ные аппараты, устройства-роботы и многое другое. Так, в частности, *в последние годы новые актуальные проблемы ИБ обусловлены быстрым развитием интернета вещей,* или, как принято называть, устройств IoT [7–12]. Компании внедряют их для автоматизации сбора информации и управления различными сферами своей деятельности. Может использоваться совокупность устройств, которые объединены концепцией сети передачи данных. Часто объединение происходит с использованием Bluetooth, wi-fi и других беспроводных технологий. Причем это могут быть как бытовые устройства (лампочки, выключатели, кофе-машины, кулеры, печки и т. д.), так и персональные компьютеры, телефоны, которые находятся в критически уязвимом состоянии, если у них общая система с бытовыми IoT-устройствами. И, как правило, такого рода устройства очень уязвимы. Более того, встречаются такие уязвимости, которые могли быть устранены на персональном компьютере с десяток лет назад. В отсутствие должного контроля над IoT-системами компании не могут гарантировать сохранность ПДн. И в частной жизни всё чаще люди используют IoT для широкого спектра целей – от организации «умного дома» до мониторинга своих физиологических параметров. Для бытовых приборов унифицированных требований ИБ практически не существует, и в целом регулирование вопросов безопасности IoT находится на начальном этапе. Хотя была разработана и утверждена концепция построения и развития узкополосных беспроводных сетей связи интернета вещей [9], где прописаны некоторые стандарты создания и управления устройствами IoT, в том числе рекомендации по ИБ, а создатели устройств предлагают собственные концепции их безопасности (не всегда открытые для изучения), этого безусловно недостаточно. В отсутствие действенной системы регулирования интернета вещей повышение осведомленности пользователей IoT об информационных рисках, связанных с этими устройствам, имеет особое значение. И, размышляя о приобретении (например, об «умной кровати»), человек должен думать не только о том, сколько многообещающих для улучшения сна сервисов описано в рекламе, но и об уровне риска для своего здоровья, если в функционирование соответствующего ПО (в клиентском приложении на смартфоне пользователя или в непонятно где размещенной серверной части) вмешается вредоносная программа или злоумышленник. А надевая на руки «умные часы», не следует забывать и возможных последствиях их уязвимостей – ведь, например, получив данные колебаний акселерометра, особенно в сочетании с графиками гироскопа, можно считать специфический поведенческий профиль пользователя, вплоть до расшифровки пин-кода банковской карты по характерным колебаниям руки [11, 12].

Превентивное ознакомление с уязвимостями новых технологий позволит людям более грамотно подходить к их применению, учитывая требования безопасности уже на этапе их освоения.

2. ПРАКТИЧЕСКИЕ АСПЕКТЫ ПОЛУЧЕНИЯ ЗНАНИЙ И ФОРМИРОВАНИЯ НАВЫКОВ ПО ОБЕСПЕЧЕНИЮ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Приобретение знаний и умений обеспечения личной ИБ может осуществляться разными способами. В целом, активное развитие электронных услуг на фоне часто появляющейся в СМИ информации об утечках персональных данных и последствиях инцидентов информационной безопасности, происходящих в том числе из-за неграмотности и беспечности пользователей, способствует осознанию гражданами важности данной проблемы и повышению их интереса к освоению навыков личной ИБ. Так, многие пользователи знакомятся с базовыми правилами обеспечения интернет-безопасности при регистрации в сервисах интернет-банкинга, при использовании электронных государственных услуг – в основном это касается безопасности аутентификационной информации.

Представители органов власти, государственных организаций и предприятий оборонного комплекса обязаны проходить повышение квалификации по ИБ в соответствии с требованиями законодательства. Круг изучаемых вопросов в первую очередь охватывает правила безопасной работы в информационных системах организации, в том числе в государственных информационных системах, на объектах критической информационной инфраструктуры и в информационных системах персональных данных (с акцентом на обязанности обучаемых сотрудников). Полученные при этом знания во многом универсальны и безусловно способствуют формированию необходимых навыков безопасной работы пользователя с информационными технологиями и за пределами корпоративной информационной среды.

В последние годы стало уделяться значительное внимание вопросам информационной безопасности и защиты персональных данных детей. Эта тематика включается в программы среднего образования, а первые знания школьники могут получить уже в начальных классах [13, 14].

В системе высшего и среднего профессионального образования обучающимся даются представления об используемых в профессиональной сфере информационных системах и технологиях. В стандартах большинства направлений высшего образования предусмотрены компетенции, направленные на формирование способности применять их с учетом требований информаци-

онной безопасности. Однако, как показывает опыт, вопросы личной информационной безопасности в силу ограниченности учебного времени в вузах изучаются, как правило, фрагментарно: обучающих обычно знакомят с отдельными аспектами ИТ-безопасности, но вопросы, относящиеся, например, к обеспечению прав субъектов ПД, практически не затрагиваются.

Как и во многих областях знаний, эффективным способом освоения рассматриваемой проблематики являются семинары и деловые игры с применением активных форм обучения на основе сценариев, адаптированных к интересам аудитории. Для этой цели полезно использовать предварительное анкетирование слушателей, сформулировав задачи ИБ в контексте ситуаций, типичных или достаточно реальных для собравшейся аудитории. Анкеты могут заполняться анонимно, в электронной или письменной форме. Анкетирование позволяет выявить наиболее востребованные аспекты и пробелы в знаниях, что дает возможность настройки обсуждения на аудиторию. Коллективное обсуждение проблемных ситуаций, отраженных в анкетах, активизирует аудиторию и позволяет выйти на реальные примеры, с которыми сталкивались пользователи, что способствует усвоению способов безопасного поведения и предотвращения небезопасных действий в будущем. Заметим, что на некоторые вопросы анкеты может не быть однозначно правильных ответов (например, есть разные относительно безопасные способы создания и хранения паролей), пользователям надо понимать достоинства и риски, связанные с каждым из них.

Интерес обучающихся к обсуждаемой тематике можно поддерживать за счет использования инфографики, анимированных электронных ресурсов, где разбираются типичные ситуации в занимательной форме. Примером могут служить материалы, размещенные на ресурсах по безопасности пользователей в сети интернет [17] и цифровой грамотности [18]. Нередко публикуются образовательные анкеты-тесты, в которых в изображенной и (или) словесно описанной ситуации требуется выбрать правильный с точки зрения безопасности вариант действий, при этом после совершения выбора открываются необходимые комментарии, поясняющие правильный выбор. Не подвергая сомнению полезность и востребованность таких ресурсов, следует отметить, что, просматривая анимации и комиксы, человек часто не ассоциирует свои ИТ-потребности с ситуациями вокруг виртуальных персонажей, поэтому задача заключается в использовании их таким образом, чтобы развлекательная форма представления материалов не затмевала реальных проблем слушателей, и они могли бы представленную тематику сопоставить с собственным опытом применения цифровых технологий. Созданный общедоступный электронный сервис по освоению цифровой грамотности позволяет осуществить самооценку ключевых компетенций цифровой экономики [18], в числе кото-

рых есть и компетенции по информационной безопасности. Однако следует заметить, что в тестах по информационной безопасности на этом ресурсе всё же немало вопросов, которые ориентированы в большей степени на специалистов, а не на пользователей даже при выборе самой самого простого уровня.

Перспективной образовательной технологией в рассматриваемой области является проведение с использованием электронных игровых обучающих платформ квестов, викторин, конкурсов, сценарии которых основаны на реальных ситуациях и требуют от пользователей активного применения своих знаний для достижения целей игры, которая может проводиться в командном или личном формате. Подобные форматы были созданы и сейчас активно развиваются в первую очередь для подготовки специалистов по информационной безопасности. В последние годы на общероссийском и региональном уровнях проводится немало соревнований по ИБ для школьников и студентов, требующих решения практико-ориентированных задач в офлайн- и онлайн-форматах, способствующих пониманию особенностей реализации информационных угроз и выработке навыков их предотвращения [5, 6, 15, 16]. Имеющийся опыт показывает, что при правильном подборе сценариев подобные платформы и форматы мероприятий могут быть интересны и эффективны при повышении осведомленности пользователей в сфере информационной безопасности, обучении их способам противодействия информационным угрозам с применением доступных методов и средств [6].

ЗАКЛЮЧЕНИЕ

В целом, как можно увидеть даже из краткого обзора, в настоящее время пользователям информационных технологий доступно немало возможностей формирования навыков безопасной работы в цифровой среде. Однако этого недостаточно для обеспечения личной информационной безопасности, поскольку основополагающая проблема – формирование персонального цифрового пространства, отвечающего частным и деловым информационным потребностям человека в цифровом мире – требует для своего решения углубленного внимания к вопросам анализа качества информационных ресурсов, сопоставления удобств цифровых сервисов с возможными рисками их использования. Эти аспекты, за редким исключением, пока остаются за рамками методов и технологий, массово используемых для повышения уровня цифровой грамотности населения.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646 // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074.

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных» // Собрание законодательства Российской Федерации. – 2006. – № 31, ч. 1–2. – Ст. 3448.

3. Паспорт национальной программы «Цифровая экономика Российской Федерации»: утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24 декабря 2018 г. № 16.

4. *Тушко Т.А. Пестунова Т.М.* Информатика: учебное пособие. – Красноярск: СФУ, 2017. – 204 с.

5. CTF News: web-сайт. – URL: https://ctfnews.ru/ (дата обращения: 10.03.2023).

6. Концепция CTF-квеста по информационной безопасности для студентов непрофильных специальностей / К.В. Курносов, А.И. Пестунов, Т.М. Пестунова, Я.В. Юракова // Труды Межвузовской научно-практической конференции «Актуальные проблемы обеспечения информационной безопасности». – Самара, 2017. – С. 119–123.

7. Горе от ума: Уязвимости IoT-устройств. – URL: https://vc.ru/tech/150042-gore-ot-uma-uyazvimosti-iot-ustroystv (дата обращения: 10.03.2023).

8. Информационная безопасность в IoT. – URL: https://habr.com/ru/post/700800/ (дата обращения: 10.03.2023).

9. Приказ Минцифры России от 29.03.2019 № 113 «Об утверждении Концепции построения и развития узкополосных беспроводных сетей связи “Интернета вещей” на территории РФ».

10. *Верещагина Е.А., Карпецкий И.О., Ярмонов А.С.* Проблемы безопасности Интернета вещей: учебное пособие. – М.: Мир науки, 2021. – URL: https://izd-mn.com/PDF/20MNNPU21.pdf (дата обращения: 10.03.2023).

11. *Лачынова М.Е.* Аналитическое исследование угроз и уязвимостей умных часов // Социотехнические и гуманитарные аспекты информационной безопасности: материалы III Всероссийской научно-практической конференции. – Пятигорск, 2022. – С. 129–140.

12. Безопасны ли умные часы? // Kaspersky: web-сайт. – URL: https://www.kaspersky.ru/resource-center/threats/smartwatch-security-risks (дата обращения: 10.03.2023).

13. Примерная образовательная программа учебного курса «Информационная безопасность» для образовательных организаций, реализующих про-

граммы начального общего образования (одобрена решение ФУМО от 26 октября 2020 г.). – URL: https://fgosreestr.ru/uploads/files/0f72931702387091b607da108ba104d9.pdf (дата обращения: 10.03.2023).

14. Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учетом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности. – URL: https://единыйурок.рф/images/doc/metod/cyber.pdf (Дата обращения: 10.03.2023).

15. На базе СибГУТИ прошла интеллектуально-патриотическая игра «Киберзарница – 2019». – URL: https://sibsutis.ru/news/2901354/ (дата обращения: 10.03.2023).

16. Школьники региона приняли участие в Кубке Новосибирской области по кибербезопасности // Министерство цифрового развития и связи Новосибирской области. – 2022. – 19 апреля. – URL: https://digit.nso.ru/news/1971 (дата обращения: 10.03.2023).

17. Безопасность пользователей в сети интернет: интернет-портал Национального центра по компьютерным инцидентам. – URL: https://safe-surf.ru/ (дата обращения: 10.03.2023).

18. Готов к цифре. Проект о безопасном и эффективном использовании цифровых технологий для людей с разными уровнями цифровых компетенций. – URL: https://готовкцифре.рф (дата обращения: 10.03.2023).

Бочарникова Андрей Дмитриевич, ассистент кафедры компьютерных систем Новосибирского государственного университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: m.bocharnikova@g.nsu.ru

Пестунова Тамара Михайловна, доцент кафедры компьютерных систем Новосибирского государственного университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: t.pestunova@g.nsu.ru

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: sfo1@mail.ru

DOI: 10.17212/2782-2230-2023-1-36-52

Personal information security issues in the context of digital transformation of the economy, management and public communications*

M.E. Bocharnikova[1], T.M. Pestunova[2], V.V. Selifanov[3]

[1] *630090, Russian Federation, Novosibirsk, Pirogov Street 2, Novosibirsk State University, assistant of the Department of Computer Systems. E-mail: m.bocharnikova@g.nsu.ru*
[2] *630090, Russian Federation, Pirogov Street 2, Novosibirsk State University, Candidate. in Technical Sciences, associate professor of Computer Systems Department. E-mail: tmrp54@yandex.ru*
[3] *630087, Russian Federation, Novosibirsk, 20 Karl Marx Prospekt, Novosibirsk State Technical University, senior lecturer of the Department of Information Security. E-mail: sfo1@mail.ru*

The article analyzes the main aspects of personal information security, the knowledge of which is important for a person in conditions of high rates of digitalization of social and economic spheres. They are aimed at the formation of a personal information digital space and its management in the conditions of changing technologies and the legal field in accordance with the private and business interests of the individual. The first task in this case is to make a person aware of their interests and needs in the use of the digital environment, to assess the significance of the issues of the security of their personal data. Further, attention is drawn to the development of skills for analyzing and evaluating Internet resources in the context of the reliability and purposes of information dissemination, the development of methods and means of managing your personal data available within the framework of current legislation. Examples of a number of other relevant tasks, existing opportunities for practical acquisition of knowledge and formation of skills for safe work in a digital environment for various categories of users at the current level of information technology development are considered, and those aspects that remain outside the scope of methods and technologies that are massively used to increase the level of digital literacy of the population are also identified.

Keywords: Information security, information protection, digital literacy, personal data, digital economy, IoT devices, personal information security

REFERENCES

1. Information Security Doctrine of the Russian Federation. Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the legislation of the Russian Federation, 2016, no. 50, art. 7074. (In Russian).

2. Federal Law of the Russian Federation of July 27, 2006 No. 152 "On Personal Data". Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the legislation of the Russian Federation, 2006, no. 31, art. 3448. (In Russian).

* *Received 16 February 2023,*

3. Passport of the national program "Digital Economy of the Russian Federation" (approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects on December 24, 2018 No. 16). (In Russian).

4. Tushko T.A. Pestunova T.M. Informatika [Computer Science]. Krasnoyarsk, Siberian Federal University Publ., 2017. 204 p.

5. CTF News: website. (In Russian). Available at: https://ctfnews.ru/ (accessed 10.03.2023).

6. Kurnosov K.V., Pestunov A.I., Pestunova T.M., Yurakova Yu.V. [Concept of CTF-quest on information security for students of non-core specialties]. Trudy Mezhvuzovskoi nauchno-prakticheskoi konferentsii «Aktual'nye problemy obespecheniya informatsionnoi bezopasnosti» [Proceedings of the Interuniversity Scientific and Practical Conference "Actual Problems of Ensuring Information Security"]. Samara, 2017, pp. 119–123. (In Russian).

7. Woe from Wit: Vulnerabilities of IoT devices. (In Russian). Available at: https://vc.ru/tech/150042-gore-ot-uma-uyazvimosti-iot-ustroystv (accessed 10.03.2023).

8. Information security in the IoT. (In Russian). Available at: https://habr.com/ru/post/700800/ (accessed 10.03.2023).

9. Order of the Ministry of Communications of Russia from 29.03.2019 No. 113 "On approval of the Concept of building and development of narrowband wireless communication networks “Internet of Things” on the territory of the Russian Federation". (In Russian).

10. Vereshchagina E.A., Karpetskii I.O., Yarmonov A.S. Problemy bezopasnosti Interneta veshchei [Internet of Things security issues]. Moscow, Mir nauki Publ., 2021. Available at: https://izd-mn.com/PDF/20MNNPU21.pdf (accessed 10.03.2023).

11. Lachynova M.E. [Analytical study of threats and vulnerabilities of smart watches]. Sotsiotekhnicheskie i gumanitarnye aspekty informatsionnoi bezopasnosti [Sociotechnical and Humanitarian Aspects of Information Security]. Materials of the III All-Russian Scientific and Practical Conference. Pyatigorsk, 2022, pp. 129–140. (In Russian).

12. Are smart watches safe? Kaspersky: website. (In Russian). Available at: https://www.kaspersky.ru/resource-center/threats/smartwatch-security-risks (accessed 10.03.2023).

13. Model educational program of the course "Information security" for educational organizations implementing programs of primary general education (approved by the decision of the federal educational and methodological association for general education on October 26, 2020). (In Russian). Available at: https://fgosreestr.ru/uploads/files/0f72931702387091b607da108ba104d9.pdf. (accessed 10.03.2023).

14. Methodological recommendations on the basics of information security for students of general educational organizations, taking into account information, consumer, technical and communicative aspects of information. (In Russian). Available at: https://единыйурок.рф/images/doc/metod/cyber.pdf (accessed 10.03.2023).

15. SibGUTI hosted an intellectual and patriotic game "Cyberzarnitsa – 2019". (In Russian). Available at: https://sibsutis.ru/news/2901354/ (accessed 10.03.2023).

16. Students of the region took part in the Cup of the Novosibirsk region on cybersecurity. Ministry of Digital Development and Communications of the Novosibirsk Region, 2022, 19 April. (In Russian). Available at: https://digit.nso.ru/news/1971 (accessed 10.03.2023).

17. Security of users on the Internet. National Computer Incident Center Internet Portal. (In Russian). Available at: https://safe-surf.ru/ (accessed 10.03.2023).

18. Ready for digital. A project about the safe and effective use of digital technology for people with different levels of digital competence. (In Russian). Available at: https://готовкцифре.рф (accessed 13.01.2023).

Для цитирования:

Бочарникова М.Е., Пестунова Т.М., Селифанов В.В. Вопросы личной информационной безопасности в условиях цифровой трансформации экономики, управления и общественных коммуникаций // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 36–52. – DOI: 10.17212/2782-2230-2023-1-36-52.

For citation:

Bocharnikova M.E., Pestunova T.M., Selifanov V.V. Voprosy lichnoi informatsionnoi bezopasnosti v usloviyakh tsifrovoi transformatsii ekonomiki, upravleniya i obshchestvennykh kommunikatsii [Personal information security issues in the context of digital transformation of the economy, management and public communications]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 1 (108), pp. 36–52. DOI: 10.17212/2782-2230-2023-1-36-52.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 1 (108). – 53–68

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 621.382.232 DOI: 10.17212/2782-2230-2023-1-53-68

МОДАЛЬНЫЙ СИНТЕЗ РЕГУЛЯТОРОВ ПОЛИНОМИАЛЬНЫМ МЕТОДОМ ДЛЯ СИСТЕМ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ С ИЗБЫТОЧНОЙ РАЗМЕРНОСТЬЮ ВЕКТОРА УПРАВЛЕНИЯ*

А.А. ВОЕВОДА[1], В.И. ШИПАГИН[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет. E-mail: ucit@ucit.ru*
[2] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет. E-mail: shipagin@mail.ru*

При применении полиномиальных методов синтеза многоканальных регуляторов возникает необходимость полиномиального матричного исчисления. Однако при использовании этого метода в основном рассматриваются объекты с числом выходных каналов, равным числу входных каналов. Это необходимо для удобства решения системы линейных алгебраических уравнений при матричном полиномиальном вычислении. Достаточно большое количество реальных технических систем имеет неравное количество входных и выходных каналов. Вопрос синтеза регуляторов полиномиальным методом для многоканальных объектов с неравным числом входных и выходных каналов проработан недостаточно глубоко. Одним из частных случаев таких систем можно считать системы с избыточной размерностью вектора управления. В рамках настоящей работы приводятся примеры таких систем и цели их использования. Приведен иллюстративный пример линейной модели неустойчивого объекта с тремя каналами по входному воздействию и двумя выходными каналами. Необходимо добиться определенных показателей качества выходной векторной величины, при этом управление будет осуществляться в обратной связи системы и суммироваться с входным воздействием. Простота рассматриваемой системы связана с удобством демонстрации на этом примере модального метода синтеза, использующего полиномиальное матричное разложение передаточных функций объекта и регулятора для такого класса объектов. В соответствии с рекомендациями, представленными в алгоритме синтеза регуляторов объектов с неквадратной матричной передаточной функции, решения задачи синтеза регулятора систем с избыточной размерностью вектора управления имеют передаточную функцию объекта управления в виде правого полиномиального матричного разложения, а сам регулятор – в виде левого.

* Статья получена 3 февраля 2023 г.

Ключевые слова: модальные методы синтеза, многоканальный объект, синтез многоканальных регуляторов, полиномиальный матричный метод, избыточная размерность вектора управления, объект с неквадратной матричной передаточной функцией, полиномиальное разложение

ВВЕДЕНИЕ

Реальные технические системы изобилуют примерами систем автоматического управления (САУ) с многоканальными объектами управления, модель которых может быть описана неквадратной матричной передаточной функцией (МПФ), то есть таких систем, у объекта управления которых количества входных (вектор управления) и выходных каналов не равны друг другу. Одним из частных случаев таких систем можно считать системы, содержащие объекты с размером вектора управления, превышающим размер вектора управляемых величин объекта. Автор [1, 2] предлагает называть такие системы с избыточной размерностью вектора управления (ИРВУ). Некоторые публикации, посвященные системам этого класса, рассматривают САУ с привязкой к их целевому назначению – системы с дуальным управлением [3], отказоустойчивые системы [4]. Некоторые авторы рассматривают такие САУ в разрезе принципов функционирования САУ – самонастраивающиеся и адаптивные системы [5, 6], системы с переменной структурой [6, 7].

Автор [1, 2] выделяет достаточно большое число возможных целей использования управления с ИРВУ. Перечислим некоторые из них.

1. Расширение функциональных возможностей управляемых объектов и изменение фундаментальных свойств, характеризующих объект, прежде всего управляемости и достижимости. Изменение нулей системы [9].

2. Придание САУ адаптационных свойств. Повышение надежности системы при нерегламентированных воздействиях внешней среды или выходе из строя некоторых элементов системы [10].

3. Уменьшение влияния нежелательных свойств объекта управления на качество процесса управления. Например, в работе [11] уменьшали люфт механической передачи двухдвигательного привода звеньев манипуляторов.

4. Обеспечение желаемого характера протекания процесса в САУ. Например, этот способ был реализован для объектов управления с переменной структурой в работах [7, 12].

Однако синтез регуляторов для данного класса систем затруднен в связи с тем, что большинство классических методов синтеза хорошо разработано именно для объектов с равным количеством входов и выходов. Распространены различные способы расчета регуляторов для объектов с избыточной размерностью вектора выхода, основанные на преобразовании матричной ПФ

к квадратному виду. К ним относится добавление виртуального выхода, дублирующего один из входов [13], или исключение одного из входов с фиксацией его на определенном значении [14]. Данные способы приводят непременно к уменьшению гибкости работы регулятора. Добавление дополнительных датчиков, уравнивающих количество входов и выходов, непременно ведет к удорожанию изделия [15]. Значительное число публикаций, посвященных объектам с ИРВУ, показывает, что рассмотрение данного класса объектов актуально и заслуживает отдельного внимания.

В настоящей работе рассмотрен подход, использующий модальный синтез с применением полиномиального разложения МПФ объекта и регулятора, приведенный автором [16]. На примере объекта с ИРВУ продемонстрирована работа данного алгоритма, и по ходу примера даны рекомендации, необходимые для его уточнения.

1. ПРИМЕР СИНТЕЗА МОДАЛЬНЫХ РЕГУЛЯТОРОВ ДЛЯ ЛИНЕЙНЫХ ОБЪЕКТОВ С ИЗБЫТОЧНОЙ РАЗМЕРНОСТЬЮ ВЕКТОРА УПРАВЛЕНИЯ

Выбор объекта связан с его простотой для демонстрации применения алгоритма, указанного в работе [16]. В процессе рассмотрения примера предлагаются корректировки и уточнения алгоритма.

1.1. ПОСТАНОВКА ЗАДАЧИ

Для примера работы алгоритма полиномиального синтеза регулятора рассмотрим линейную модель неустойчивого объекта с тремя входными $u(s)=\begin{pmatrix}u_1(s) & u_2(s) & u_3(s)\end{pmatrix}^T$ и двумя выходными воздействиями $y(s)=\begin{pmatrix}y_1(s) & y_2(s)\end{pmatrix}^T$, описанную в [17]. Описание объекта можно представить также в матричном виде:

$$\begin{pmatrix}y_1(s)\\ y_2(s)\end{pmatrix}=\begin{pmatrix}\frac{1}{s+1} & 0 & \frac{s-1}{(s+1)(s+2)}\\ \frac{-1}{s-1} & \frac{1}{s+2} & \frac{1}{s+2}\end{pmatrix}\begin{pmatrix}u_1\\ u_2\\ u_3\end{pmatrix}. \qquad (1)$$

Согласно теоремам Р. Калмана о полной наблюдаемости и управляемости, объект наблюдаем и управляем. Это позволяет строить систему автоматического регулирования для данного объекта. При применении модаль-

ного метода, базирующегося на полиномиальном матричном разложении системы для объектов с МПФ квадратного вида, авторы [18, 19] использовали правое разложение МПФ объекта и левое разложение для регулятора. Однако автором [16] показано, что для объектов с МПФ неквадратного вида выбор вида разложения влияет на сложность характеристической матрицы замкнутой системы (ХМЗС). В частности, для системы с количеством входных каналов, превышающим количество выходных каналов, предлагается использовать левое полиномиальное разложение ПФ объекта и правое полиномиальное разложение ПФ регулятора.

В соответствии с рекомендациями [16] и для простоты дальнейшего вычисления ХМЗС при использовании левого полиномиального разложения МПФ объекта обычно используется правое полиномиальное разложение МПФ регулятора: $u(s) = X_r(s)Y_r^{-1}(s)e(s)$, где $u(s) = \begin{pmatrix} u_1(s) & u_2(s) & u_3(s) \end{pmatrix}^T$ – вектор управляющих сигналов на выходе из регулятора и на входе в объект, $X_r(s) \in \mathbb{R}[s]^{3\times 2}$ – «числитель» ПФ регулятора, $Y_r(s) \in \mathbb{R}[s]^{2\times 3}$ – «знаменатель» ПФ регулятора (при этом $\det(Y_r(s)) \neq 0$), $e(s) = \begin{pmatrix} e_1(s) & e_2(s) \end{pmatrix}^T$ – вектор ошибки регулирования между заданием $v(s) = \begin{pmatrix} v_1(s) & v_2(s) \end{pmatrix}^T$ и выходом системы $y(s) = \begin{pmatrix} y_1(s) & y_2(s) \end{pmatrix}^T$. Вектор ошибки регулирования можно выразить следующим выражением: $e(s) = v(s) - y(s)$. Число входных каналов объекта управления обозначим через $p = 3$, число выходных каналов – через $m = 2$. Структурная схема системы может быть представлена в следующем виде (рис. 1).

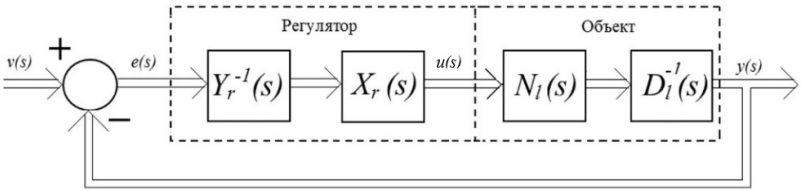


Рис. 1. Структурная схема системы «регулятор – объект»

Fig. 1. Block diagram of the "Controller – Object" system

Так как МПФ представлена в формуле (1), алгоритм синтеза регулятора для объектов, описываемых неквадратной МПФ [16], начнем со второго шага[1].

[1] Первый шаг алгоритма, представленного в [16], предполагает получение МПФ объекта.

Выбор размерности матриц «числителя» и «знаменателя» МПФ объекта и регулятора связан, с одной стороны, с числом входных и выходных каналов объекта управления и регулятора и, с другой стороны, с необходимостью получения обратной матрицы для матриц «числителя» МПФ объекта и регулятора (то есть в этом случае необходимо рассматривать в качестве «числителя» только матрицу квадратного вида).

Шаг 2. По матричной ПФ (1) необходимо найти левое (правое) взаимно простое и строчно (столбцово) приведенное[2] полиномиальное матричное описание (ПМО) объекта. Для нахождения взаимно простого строчно приведенного левого полиномиального разложения матричную ПФ объекта выразим в виде произведения двух полиномиальных матриц: $W_{obj}(s) = D_l^{-1}(s)N_l(s)$, где «числитель» ПФ объекта $N_l(s) \in \mathbb{R}[s]^{2\times 3}$, а «знаменатель» ПФ объекта $D_l(s) \in \mathbb{R}[s]^{2\times 2}$ ($\mathbb{R}[s]$ – множество полиномов)

$$N_l(s) = \begin{pmatrix} -2s-4 & 0 & -2s+2 \\ s+2 & -s+1 & -s+1 \end{pmatrix}, \quad D_l(s) = \begin{pmatrix} -2s^2-6s-4 & 0 \\ 0 & -s^2-s+2 \end{pmatrix}. \quad (2)$$

Взаимная простота полиномиальных матриц «числителя» и «знаменателя» ПФ объекта необходима для внутренней устойчивости всей системы (так как не происходит сокращения множителей, корни[3] которых расположены в правой (замкнутой) полуплоскости). Это является одним из условий существования решения при синтезе регуляторов, в том числе модальным методом, использующим полиномиальное матричное разложение [18, 21].

Шаг 3. По левому ПМО объекта (2) найдем правое взаимно простое и столбцово приведенное ПМО объекта[4]:

$$N_r(s) = \begin{pmatrix} 0 & 0 & s-1 \\ 0 & -1 & 0 \end{pmatrix}, \quad D_r(s) = \begin{pmatrix} -2s+2 & 0 & s^2-1 \\ -4s-8 & -s-2 & s^2+3s+2 \\ 2s+4 & 0 & 0 \end{pmatrix}. \quad (3)$$

---

[2] Столбцово (строчно) приведенная (column (row) reduced) [20, с. 527] полиномиальная матрица – это такая матрица, у которой числовая матрица, составленная из коэффициентов при старших степенях по столбцам (строкам), имеет полный ранг.

[3] Под корнями здесь понимаются корни уравнений, полученные приравниванием данных множителей к нулю.

[4] Алгоритм нахождения правого (левого) взаимно простого матричного полиномиального разложения приведен в работе [16].

Шаг 4. Так как в заданной модели объекта (1) число входных каналов больше числа управляемых выходов $m > p$, то переходим к алгоритму работы [16].

Шаг 4.1. Строчные степени матрицы $D_l(s)$: $\nu_1 = \nu_2 = 2$; столбцовые степени матрицы $D_r(s)$: $\mu_1 = \mu_2 = 1$, $\mu_3 = 2$. Строчный индекс $\nu = \max(\nu_1, \nu_2) = 2$; столбцовый индекс $\mu = \max(\mu_1, \mu_2, \mu_3) = 2$.

Шаг 4.2. Выразим матрицы левого ПМО объекта в виде числовых матриц:

$$N_0 = \begin{pmatrix} -4 & 0 & 2 \\ 2 & 1 & 1 \end{pmatrix}, \quad N_1 = \begin{pmatrix} -2 & 0 & -2 \\ 1 & -1 & -1 \end{pmatrix},$$

$$D_0 = \begin{pmatrix} -4 & 0 \\ 0 & 2 \end{pmatrix}, \quad D_1 = \begin{pmatrix} -6 & 0 \\ 0 & -1 \end{pmatrix}, \quad D_2 = \begin{pmatrix} -2 & 0 \\ 0 & -1 \end{pmatrix},$$

где N_0, $N_1 \in \mathbb{R}^{2\times 3}$; D_0, D_1, $D_2 \in \mathbb{R}^{2\times 2}$ – числовые матрицы параметров полиномов при соответствующих операторах Лапласа *s*.

2.2. СИНТЕЗ РЕГУЛЯТОРА

В этом разделе определим вид и параметры регулятора, выраженные через правое полиномиальное матричное разложение МПФ. Для этого составим систему дифференциальных уравнений в матричном виде с использованием матрицы Сильвестра [16]. Определим линейно зависимые столбцы матрицы Сильвестра, которые впоследствии будут формировать свободные параметры матрицы параметров регулятора. Выбор свободных параметров регулятора влияет на возможность получения дополнительных свойств САУ, таких, например, как астатизм выходных параметров системы.

Шаг 4.3. На этом шаге необходимо найти столбцовые степени регулятора. В алгоритме, представленном в [16], они обозначены через m_i, где $i = \overline{1, p}$ – номер столбца регулятора. Данная переменная уже задействована для обозначения числа входных воздействий на объект управления. Для исключения дальнейшей путаницы предлагается обозначить столбцовые степени регулятора через z_i.

В данном примере предлагается выбрать регулятор полного порядка, поэтому столбцовые степени регулятора выбраны по формуле $z_i = \mu - 1$, где $i = \overline{1, p}$. Таким образом $z = z_0 = z_1 = \mu - 1 = 1$. Числовые матрицы, полученные

из правого полиномиально-матричного разложения ПФ регулятора, принимают следующий вид:

$$X_k = \left\{ x_{ij}^k \right\}, \;\; Y_k = \left\{ y_{ij}^k \right\},$$

где x_{ij}^k, y_{ij}^k, – параметры регулятора, i – номер строки элемента, j – номер столбца элемента, k – порядок оператора.

Кроме этого, в отличие от алгоритма, приведенного в [16], на данном шаге необходимо также определить матрицу параметров регулятора $\tilde{R} \in \mathbb{R}^{(p+m)(n+1)}$, $\tilde{R} = \left(Y_n^T, X_n^T, Y_{n-1}^T, X_{n-1}^T, ..., Y_0^T, X_0^T \right)^T$, так как она необходима для дальнейшей работы алгоритма. Для данного примера $\tilde{R} \in \mathbb{R}^{10\times 2}$, $\tilde{R} = \left(Y_1^T, \, X_1^T, \, Y_0^T, \, X_0^T \right)^T$.

Шаг 4.4. Определим степень и структуру характеристической полиномиальной матрицы системы $C(s) = \sum_{i=0}^{f} C_i s^i$, где $C_i \in \mathbb{R}^{p\times p}$ – числовая матрица[5] коэффициентов при соответствующих параметрах s, $f \triangleq \max(f_i)$, $f_i = z_i + \nu_i$, $i = \overline{1, p}$. Таким образом, получаем $f = 3$. Обычно при синтезе регуляторов модальным методом, использующим полиномиальное матричное разложение, выбирается диагональный вид желаемой ХМЗС [18, 20]. В связи с этим выберем желаемую ХМЗС вида $C(s) = \begin{pmatrix} (s+1)^3 & 0 \\ 0 & (s+1)^3 \end{pmatrix}$, $C_3 = C_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $C_1 = C_2 = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$. Числовая матрица желаемых коэффициентов ХМЗС: $\aleph = \begin{pmatrix} C_3^T & C_2^T & C_1^T & C_0^T \end{pmatrix}^T$.

Шаг 4.6. Сформируем матрицу Сильвестра[6] $\Im \in \mathbb{R}^{p(\nu+1+n)(p+m)(n+1)}$ и получим $\Im \in \mathbb{R}^{8\times 10}$, $rank(\Im) = 8$. При этом в ней нулевых срок нет.

---

[5] Определение размеров характеристической полиномиальной матрицы в алгоритме синтеза регуляторов для неквадратных объектов [16] не приведено.

[6] В работе [16] используется формула определения размеров матрицы Сильвестра, по-видимому, с небольшой опечаткой (в настоящей работе устранено).

$$\Im = \begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -6 & 0 & -2 & 0 & -2 & -2 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & -1 & -1 & 0 & -1 & 0 & 0 & 0 \\ -4 & 0 & -4 & 0 & 2 & -6 & 0 & -2 & 0 & -2 \\ 0 & 2 & 2 & 1 & 1 & 0 & -1 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & -4 & 0 & -4 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 1 \end{pmatrix}.$$

В данной матрице выберем два линейно зависимых столбца, при удалении которых ранг матрицы не изменится. В данном случае это седьмой и восьмой столбцы. Так как ранг матрицы $\Im$ неполный, то переходим к шагу 4.9.

Шаг 4.9. В соответствии с рекомендациями, приведенными в [16], необходимо выбрать базисный минор матрицы Сильвестра $\Im$, не включающий в себя седьмой и восьмой столбцы $\Im_1 \in \mathbb{R}^{8\times 8}$ (выбор столбцов, не включенных в минор, влияет на выбор свободных параметров регулятора и сделан согласно рекомендациям [16] для обеспечения астатизма одной из выходных величин). Соответствующим образом необходимо поступить с матрицей параметров регулятора $\Re$. Сформируем матрицу $\Re_1 \in \mathbb{R}[s]^{8\times 2}$, не включающую в себя седьмую и восьмую строки, соответствующие параметрам регулятора y_{21}^0, y_{22}^0 (для обеспечения астатизма по выходу системы) и x_{11}^0, x_{12}^0 (как остальные линейно зависимые строки):

$$\Re_1 = \begin{pmatrix} y_{11}^1 & y_{21}^1 & x_{11}^1 & x_{21}^1 & x_{31}^1 & y_{11}^0 & x_{21}^0 & x_{31}^0 \\ y_{12}^1 & y_{22}^1 & x_{12}^1 & x_{22}^1 & x_{32}^1 & y_{12}^0 & x_{22}^0 & x_{32}^0 \end{pmatrix}^T.$$

Составим матрицу, не входящую в базисный минор $\overline{\Im} \in \mathbb{R}^{8\times 2}$, и соответствующую матрицу свободных параметров $\overline{\Re} \in \mathbb{R}^{2\times 2}$. Для простоты демонстрации в данном примере матрицу свободных параметров $\overline{\Re} = \{0\}$ возьмем нулевой. Так как в базисный минор $\Im_1$ вошли все строки из $\Im$, переходим к шагу 4.11.

Шаг 4.11. Необходимо решить систему линейных уравнений $\Re_1 = \Im_1^{-1}(\aleph - \overline{\Im}\overline{\Re})$. Так как матрица свободных параметров $\overline{\Re}$ нулевая, система линейных уравнений приобретает вид $\Re_1 = \Im_1^{-1}\aleph$. Матрица параметров регулятора приобретает вид

$$\Re_1 = \begin{pmatrix} -0.5 & 0 & 0 & -1/6 & 1/6 & -1/6 & -1/6 & 1/6 \\ 0 & -1 & 8/3 & 2 & -4/3 & -4/3 & 11/3 & -8/3 \end{pmatrix}^T.$$

Шаг 4.12. В результате расчетов получены полиномиальные матрицы регулятора:

$$X_r(s) = \begin{pmatrix} 0 & 16s \\ -s-1 & 12s+22 \\ s+1 & -8s-16 \end{pmatrix},\ Y_r(s) = \begin{pmatrix} -3s-1 & -8 \\ 0 & -6s \end{pmatrix}.$$

Вычислим ХМЗС для проверки корректности вычислений: $D_l(s)Y_r(s) + N_l(s)X_r(s) = \begin{pmatrix} (s+1)^3 & 0 \\ 0 & (s+1)^3 \end{pmatrix}$. Полученная ХМЗС полностью совпадает с желаемой $C(s)$. Отсюда можно сделать вывод о том, что расчеты проведены корректно.

МПФ регулятора выглядит следующим образом:

$$X_r(s)Y_r^{-1}(s) = \begin{pmatrix} 0 & -8/3 \\ \dfrac{s+1}{3s+1} & -\dfrac{18s^2+43s+15}{9s^2+3s} \\ -\dfrac{s+1}{3s+1} & \dfrac{12s^2+32s+12}{9s^2+3s} \end{pmatrix}. \qquad (4)$$

Смоделируем систему, представленную объектом управления (1) и регулятором (4). В качестве задания на вход системы подадим единичное ступенчатое воздействие по обоим каналам $\nu_1(t) = \nu_2(t) = 1(t)$. Графики переходных процессов системы продемонстрированы на рис. 2.

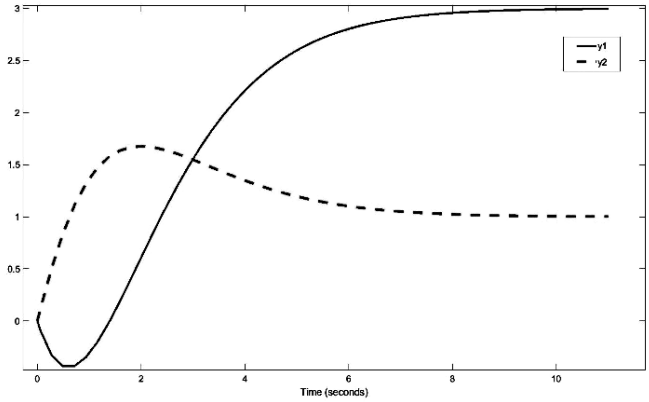


Рис. 2. Графики переходных процессов для системы с регулятором первого порядка

Fig. 2. Transient graphs for a system with a first-order controller

Как видно из представленных графиков переходных процессов по второму выходному каналу y_2 значения выхода системы содержат статическую ошибку. По каналу y_1 удалось добиться астатического выхода благодаря приравниванию свободных параметров регулятора y_{21}^0, y_{22}^0 нулю на шаге 4.9. По первому каналу имеется существенная статическая ошибка. Для улучшения характеристик переходных процессов системы необходимо повысить порядок регулятора. То есть необходимо провести заново процедуру, описанную в данном разделе, с той лишь разницей, что теперь столбцовые степени регулятора будут равны $z = z_0 = z_1 = 2$. Для краткости изложения данную процедуру заново приводить не будем. Приведем только результаты работы данного алгоритма. ПФ регулятора будет выглядеть следующим образом:

$$X_r(s)Y_r^{-1}(s) = \begin{pmatrix} \dfrac{4}{s^3+7s^2+8s} & -\dfrac{5s+9}{s^3+7s^2+8s} \\ \dfrac{0.3s^2-4s-8}{s^3+7s^2+8s} & -\dfrac{10s^2+36s+31}{s^3+7s^2+8s} \\ -\dfrac{0.7s^3+4s^2+3s-1}{s^3+7s^2+8s} & -\dfrac{3s^3+13s^2+24s+15}{s^3+7s^2+8s} \end{pmatrix}. \qquad (5)$$

Представим на рис. 3 переходные процессы системы в случае использования объекта управления (1) и регулятора (5).

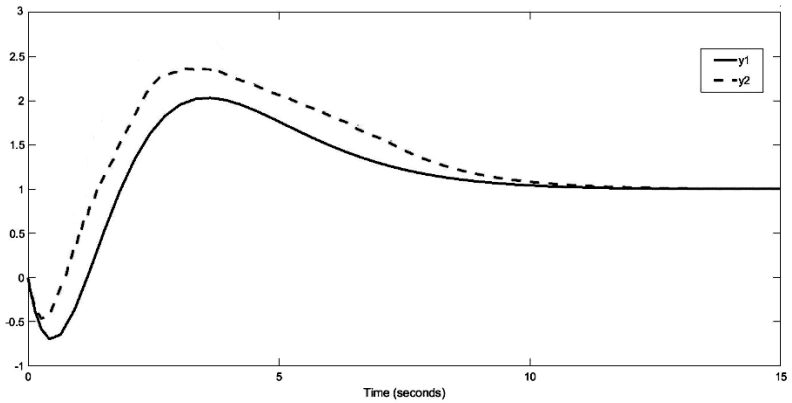


Рис. 3. Графики переходных процессов для системы с регулятором второго порядка

Fig. 3. Transient graphs for a system with a second-order controller

Как видно из рис. 3, оба выхода системы астатичны. Этого удалось добиться благодаря повышению порядка регулятора, что, в свою очередь, увеличило число свободных параметров в нем. По обоим каналам присутствует перерегулирование, и в начале переходного процесса также существует отрицательное колебание выходных параметров системы. Это может быть связано с присутствием в ПФ замкнутой системы положительных нулей.

ЗАКЛЮЧЕНИЕ

Настоящая работа посвящена САУ с избыточной размерностью вектора управления. Продемонстрирован пример синтеза регулятора для многоканального объекта с избыточной размерностью вектора управления с помощью модального метода, использующего полиномиальное матричное разложение матричной передаточной функции объекта и регулятора. В соответствии с рекомендациями [16] для данного типа систем выбрано использование правого взаимно-простого разложения МПФ объекта и левого взаимно-простого разложения МПФ регулятора. По ходу разбора примера в алгоритм внесены некоторые корректировки. Показано, что повышение порядка регулятора позволяет получить большее число его свободных параметров (т. е. таких пара-

метров, которые можно выбирать в соответствии с требованиями к переходным процессам системы). Это, в свою очередь, позволило на демонстрируемом примере добиться астатизма по обоим выходным каналам системы.

На основании вышесказанного можем сделать вывод о возможности применения модального метода синтеза, использующего полиномиальное матричное разложение МПФ объекта и регулятора, для систем с избыточной размерностью вектора управления по сравнению размерностью вектора управляющих воздействий. При повышении порядка полиномиально матричного описания МПФ регулятора появляются свободные параметры, способные придать дополнительные свойства синтезируемой системе автоматического управления.

СПИСОК ЛИТЕРАТУРЫ

1. *Малышенко А.М.* Системы автоматического управления с избыточной размерностью вектора управления. – Томск: Изд-во Том. политехн. ун-та, 2005. – 302 с.

2. *Малышенко А.М.* Системы автоматического управления с избыточной размерностью вектора управления: определение и цели использования // Научный вестник НГТУ. – 2014. – № 4 (57). – С. 31–40.

3. *Фельдбаум А.А.* Теория дуального управления // Автоматика и телемеханика. – 1960. – № 9, 11; 1961. – № 1, 2.

4. *Гришин Ю.П., Казаринов Ю.М.* Динамические системы, устойчивые к отказам. – М.: Радио и связь, 1985. – 176 с.

5. *Антонов В.Н., Терехов В.А., Тюкин И.Ю.* Адаптивное управление в технических системах. – СПб.: Изд-во С.-Петерб. ун-та, 2001. – 244 с.

6. *Буков В.Н.* Адаптивные прогнозирующие системы управления полетом. – М.: Наука, 1987. – 232 с.

7. *Емельянов С.В.* Системы автоматического управления с переменной структурой. – М.: Наука, 1967. – 336 с.

8. Теория систем с переменной структурой / под ред. С.В. Емельянова. – М.: Наука, 1970. – 592 с.

9. *Смагина Е.М.* Определение, вычисление и применение нулей многомерной системы: дис. … д-ра техн. наук: 05.13.15. – Томск, 1994. – 404 с.

10. *Ястребенецкий М.А., Иванова Г.М.* Надежность автоматизированных систем управления технологическими процессами. – М.: Энергоатомиздат, 1989. – 254 с.

11. *Петров Б.А.* Манипуляторы. – Л.: Машиностроение, 1984. – 238 с.

12. *Уткин В.И.* Системы с переменной структурой: состояние, проблемы, перспективы // Автоматика и телемеханика. – 1983. – № 9. – С. 5–25.

13. *Froisy J.* Model predictive control: Past, present and future // ISA Transactions. – 1994. – Vol. 33. – P. 235–243.

14. *Sarimveis H., Genceli H., Nikolaou* M. Design of robust nonsquare constrained model-predictive control // AIChE Journal. – 1996. – Vol. 42 (9). – P. 2582–2593.

15. Design of resilient processing plants – VII. Design of energy management system for unstable reactors – new insights / M. Morari,W. Grimm, M. Oglesby, I. Prosser // Chemical Engineering Science. – 1985. – Vol. 40. – P. 187–198.

16. *Филюшов В.Ю.* Полиномиальный метод синтеза регуляторов для многоканальных объектов с неквадратной матричной передаточной функцией: дис. … канд. техн. наук. – СПб., 2022. – 177 с.

17. *Смагина Е.М.* Нули линейных многмерных систем. Определения, классификация, применение // Автоматика и телемеханика. – 1985. – № 12. – С. 5–33.

18. *Chen C.T.* Linear system theory and design. – 2-nd ed. – New York: Oxford University Press, 1999. – 334 p.

19. *Вороной В.В.* Полиномиальный метод расчета многоканальных регуляторов пониженного порядка: дис. … канд. техн. наук: 05.13.01: защищена 22.10.2013. – Новосибирск, 2013. – 173 с.

20. *Шрейнер Р.Т.*, *Востриков А.С., Сарапулов Ф.Н.* Системы подчиненного регулирования электроприводов. Ч. 1: учебное пособие. – Екатеринбург: Изд-во УГТУ-УПИ, 1997. – 279 с.

21. *Antsaklis P.J., Michel A.N.* Linear systems. – Switzerland: Birkhauser, 1997. – 669 p.

Воевода Александр Александрович, доктор технических наук, профессор кафедры автоматики Новосибирского государственного технического университета. Основное направление научных исследований – управление многоканальными объектами. E-mail: ucit@ucit.ru

Шипагин Виктор Игоревич, аспирант направления подготовки «Управление в технических системах» Новосибирского государственного технического университета. Основное направление научных исследований – нейросетевой синтез подсистем управления техническими системами. E-mail: shipagin@mail.ru

DOI: 10.17212/2782-2230-2023-1-53-68

Modal synthesis of controllers by a polynomial method for automatic control systems with excessive dimension of the control vector*

A.A. Voevoda[1], V.I. Shipagin[2]

[1] *630073, Russian Federation, Novosibirsk, Karl Marx Prospekt, 20, NSTU. E-mail: ucit@ucit.ru*
[2] *630073, Russian Federation, Novosibirsk, Karl Marx Prospekt, 20, NSTU. E-mail: shipagin@mail.ru*

When using polynomial methods of synthesis of multichannel regulators, there is a need for polynomial matrix calculus. However, when using this method, objects with the number of output channels equal to the number of input channels are mainly considered. This is necessary for the convenience of solving a system of linear algebraic equations in matrix polynomial computation. At the same time, a fairly large number of real technical systems have an unequal number of input and output channels. At the same time, the issue of the synthesis of generators by the polynomial method for multichannel objects with an unequal number of input and output impacts has not been worked out sufficiently deeply. One of the special cases of such systems can be considered systems with excessive dimension of the control vector. Within the framework of this work, examples of such systems and the purposes of their use are given.
An illustrative example of a linear model of an unstable object with three channels for input action and two channels for output action is given. It is necessary to achieve certain quality indicators of the output vector quantity, while the control is carried out in the feedback of the system and is summed up with the input effect. The simplicity of the system under consideration is connected with the convenience of demonstrating on this example a modal synthesis method using a polynomial matrix decomposition of the transfer functions of an object and a controller for such a class of objects. In accordance with the recommendations presented in the algorithm for synthesizing regulators for objects with a non-square matrix transfer function, to solve the problem of synthesizing a regulator for systems with an excessive dimension of the control vector, the transfer function of the control object is represented as a right polynomial matrix decomposition, and the regulator is represented as a left one. During the demonstration of the example of the algorithm, some clarifications and edits are proposed in it.

Keywords: modal synthesis methods, multichannel object, synthesis of multichannel regulators, polynomial matrix method, excess dimension of the control vector, non-square object, polynomial decomposition

REFERENCES

1. Malyshenko A.M. *Sistemy avtomaticheskogo upravleniya s izbytochnoi razmernost'yu vektora upravleniya* [Automatic control systems with excessive di-

* *Received 03 February 2023.*

mension of the control vector]. Tomsk, Tomsk Polytechnic University Publ., 2005. 302 p.

2. Malyshenko A.M. Sistemy avtomaticheskogo upravleniya s izbytochnoi razmernost'yu vektora upravleniya: opredelenie i tseli ispol'zovaniya [Automatic control system with redundant dimensions of vector control: definition and application]. *Nauchnyi vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta = Science bulletin of the Novosibirsk state technical university*, 2014, no. 4 (57), pp. 31–40.

3. Feldbaum A.A. Teoriya dual'nogo upravleniya [Theory of dual control]. *Avtomatika i telemekhanika = Automation and Remote Control*, 1960, no. 9, 11, 1961, no. 1, 2. (In Russian).

4. Grishin Yu.P., Kazarinov Yu.M. *Dinamicheskie sistemy, ustoichivye k otkazam* [Dynamic systems resistant to failures]. Moscow, Radio i svyaz' Publ., 1985. 176 p.

5. Antonov V.N., Terekhov V.A., Tyukin I.Yu. *Adaptivnoe upravlenie v tekhnicheskikh sistemakh* [Adaptive control in technical systems]. St. Petersburg, St. Petersburg University Publ., 2001. 244 p.

6. Bukov V.N. *Adaptivnye prognoziruyushchie sistemy upravleniya poletom* [Adaptive predictive flight control systems]. Moscow, Nauka Publ., 1987. 232 p.

7. Emel'yanov S.V. *Sistemy avtomaticheskogo upravleniya s peremennoi strukturoi* [Automatic control systems with variable structure]. Moscow, Nauka Publ., 1967. 336 p.

8. Emel'yanov S.V., ed. *Teoriya sistem s peremennoi strukturoi* [Theory of Systems with Variable Structure]. Moscow, Nauka Publ., 1970. 592 p.

9. Smagina E.M. *Opredelenie, vychislenie i primenenie nulei mnogomernoi sistemy*. Diss. dokt. tekhn. nauk [Definition, calculation and application of zeros of a multi-dimensional system. Dr. eng. sci. diss.]. Tomsk, 1994. 404 p.

10. Yastrebenetskii M.A., Ivanova G.M. *Nadezhnost' avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami* [Reliability of automated control systems for technological processes]. Moscow, Energoatomizdat Publ., 1989. 254 p.

11. Petrov B.A. *Manipulyatory* [Manipulators]. Leningrad, Mashinostroenie Publ., 1984. 238 p.

12. Utkin V.I. Sistemy s peremennoi strukturoi: sostoyanie, problemy, perspektivy [Systems with variable structure: state, problems, prospects]. *Avtomatika i telemekhanika = Automation and Remote Control*, 1983, no. 9, pp. 5–25. (In Russian).

13. Froisy J. Model predictive control: Past, present and future. *ISA Transactions*, 1994, vol. 33, pp. 235–243.

14. Sarimveis H., Genceli H., Nikolaou M. Design of robust nonsquare constrained model-predictive control. *AIChE Journal*, 1996, vol. 42 (9), pp. 2582–2593.

15. Morari M., Grimm W., Oglesby M., Prosser I. Design of resilient processing plants – VII. Design of energy management system for unstable reactors – new insights. *Chemical Engineering Science*, 1985, vol. 40, pp. 187–198.

16. Filyushov V.Yu. *Polinomial'nyi metod sinteza regulyatorov dlya mnogokanal'nykh ob"ektov s nekvadratnoi matrichnoi peredatochnoi funktsiei*. Diss. kand. tekhn. nauk [Polynomial method of synthesis of controllers for multichannel objects with non-square matrix transfer function. PhD eng. sci. diss.]. St. Petersburg, 2022. 177 p.

17. Smagina E.M. Nuli lineinykh mnogmernykh sistem. Opredeleniya, klassifikatsiya, primenenie [Zeros of linear multidimensional systems. Definitions, classification, application]. *Avtomatika i telemekhanika = Automation and Remote Control*, 1985, no. 12, pp. 5–33. (In Russian).

18. Chen C.T. *Linear system theory and design*. 2nd ed. New York, Oxford University Press, 1999. 334 p.

19. Voronoi V.V. *Polinomial'nyi metod rascheta mnogokanal'nykh regulyatorov ponizhennogo poryadka*. Diss. kand. tekhn. nauk [Design of multi-channel reduced degree controllers. PhD eng. sci. diss.]. Novosibirsk, 2013. 173 p.

20. Shreiner R.T., Vostrikov A.S., Sarapulov F.N. *Sistemy podchinennogo regulirovaniya elektroprivodov*. Ch. 1 [Subordinate control systems. Pt. 1]. Ekaterinburg, UGTU-UPI Publ., 1997. 279 p.

21. Antsaklis P.J., Michel A.N. *Linear systems*. Switzerland, Birkhauser, 1997. 669 p.

Для цитирования:

Воевода А.А., Шипагин В.И. Модальный синтез регуляторов полиномиальным методом для систем автоматического управления с избыточной размерностью вектора управления // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 53–68. – DOI: 10.17212/2782-2230-2023-1-53-68.

For citation:

Voevoda A.A., Shipagin V.I. Modal'nyi sintez regulyatorov polinomial'nym metodom dlya sistem avtomaticheskogo upravleniya s izbytochnoi razmernost'yu vektora upravleniya [Modal synthesis of controllers by a polynomial method for automatic control systems with excessive dimension of the control vector]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 1 (108), pp. 53–68. DOI: 10.17212/2782-2230-2023-1-53-68.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 1 (108). – 69–82

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 004.056 DOI: 10.17212/2782-2230-2023-1-69-82

ВОПРОСЫ ОЦЕНКИ ДОВЕРИЯ К СИСТЕМЕ УПРАВЛЕНИЯ РИСКАМИ*

В.В. СЕЛИФАНОВ[1], В.В. АНИКЕЕВА[2], И.А. ОГНЕВ[3]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, ассистент кафедры защиты информации. E-mail: veronika.korotkova.95@mail.ru*
[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, ассистент кафедры защиты информации. E-mail: i.ognev.2016@corp.nstu.ru*

Настоящая статья посвящена вопросам оценки доверия к системе управления рисками. Термин «доверие» в отношении информационных систем практически не применяется в настоящее время. Предложена процедура оценки доверия к системе управления рисками, состоящая из четырех этапов: 1) соответствие требованиям законодательства РФ; 2) соответствие национальным стандартам; 3) оценка оптимальности существующий системы управления рисками; 4) переоценка рисков. Приведено описание существующих методов оценки доверия к системе управления рисками. Сделан вывод о том, что сегодня нет существующих требований к системе оценки рисков даже в отдельных сегментах. В работе предлагается использовать предварительно согласованную заинтересованными сторонами выборку критериев для оценки рисков из системы стандартов, описывающих процесс определения рисков с точки зрения системной инженерии. Рассмотрены критерии и показатели, используемые в стандартах, определяющих системный анализ. За основу оценки рисков принята вероятностная оценка ряда показателей: риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации. Для расчета этих показателей рисков исследуемые сущности рассматриваются в виде моделируемой системы сложной структуры. Приведена математическая модель оценки рисков в соответствии с положениями стандартов по системной инженерии.

Ключевые слова: архитектура системы, риск, оценка рисков, защита информации, пользователь, системная инженерия, информационная безопасность, государственная информационная система

* Статья получена 17 февраля 2023 г.

ВВЕДЕНИЕ

Одной из основных особенностей функционирования информационных систем в настоящее время является обязательное взаимодействие между собой. Важным вопросом при этом является оценка доверия между ними.

С учетом последних изменений требований к функционированию и развитию систем данный вопрос необходимо рассматривать прежде всего сквозь призму нормативно-правового регулирования.

Термином «доверие» обозначаются меры, принятые для должной реализации потенциальных возможностей безопасности и состоящие из сформированного свидетельства и независимой оценки пригодности этих возможностей [1]. В настоящее время данный термин в законодательных, нормативных правовых актах Российской Федерации практически не используется применительно к информационным системам и предоставляемым сервисам. Начальным этапом оценки уровня доверия к субъекту информационного обмена в недоверенной среде является оценка доверия к системе оценки и управления рисками.

Оценку доверия к системе управления рисками можно разбить на следующие этапы:

1) соответствие требованиям законодательства РФ при оценке недопустимых рисков [2–5];

2) соответствие национальным стандартам [6–31];

3) оценка оптимальности существующей системы управления рисками;

4) проведение переоценки рисков.

1. ОПИСАНИЕ СУЩЕСТВУЮЩИХ ПОДХОДОВ

Первичный процесс оценки рисков осуществляется в соответствии законодательством в зависимости от типа объекта: государственные информационные системы – приказ ФСТЭК России № 17 [2]; информационные системы персональных данных – постановление Правительства РФ № 1119 [4]; автоматизированные системы управления производственными и технологическими процессами – приказ ФСТЭК России № 31 [3]; значимые объекты критической информационной инфраструктуры – постановление Правительства РФ № 127 [5].

В указанных нормативных правовых актах присутствуют критерии определения рисков, а также некоторые процедуры их переоценки. Проведение переоценки рисков в соответствии с данными нормативными правовыми актами проводится крайне редко.

Определены следующие критерии проведения переоценки рисков для каждого типа объекта:

– для значимых объектов критической информационной инфраструктуры переоценка рисков (категории значимости) осуществляется не реже чем один раз в 5 лет, а также в случае изменения показателей критериев значимости объектов критической информационной инфраструктуры или их значений. Также результаты определения рисков (категорирования) в обязательном порядке согласуются с ФСТЭК России;

– для государственных информационных систем пересмотр класса защищенности осуществляется при изменении масштаба информационной системы или значимости обрабатываемой в ней информации;

– для информационных систем персональных данных контроль за выполнением требований [4] проводится не реже одного раза в 3 года;

– для автоматизированной системы управления производственными и технологическими процессами переоценка рисков (класса защищенности) проводится только в случае модернизации системы, в результате которой меняется уровень значимости (критичности) информации, обрабатываемой в автоматизированной системе управления или ее сегменте.

Стоит отметить две достаточно большие проблемы: во-первых, нормативно существует требование только к определению неприемлемых рисков [2–5], остальные вынесены за черту, и, во-вторых, отсутствие четких требований по управлению рисками. Они заданы только требованием по переоценке условий и максимальным промежутком времени, по истечении которого в любом случае необходимо повторно их оценить.

Таким образом, владелец системы должен сам создать систему управления рисками при отсутствии нормативных требований.

Результат ошибки здесь может стоить дорого и привести к неактуальности рисков и нанесению ущерба организации. Отсутствие цикличности рассмотрения актуальности конкретных рисков может привести к пересмотрению модели нарушителя, к неактуальности модели угроз, а также самой системы безопасности организации.

Таким образом, можно сделать вывод о том, что сейчас не существует системы требований к оценке рисков даже в отдельных сегментах, таких как значимые объекты критической информационной инфраструктуры Российской Федерации, государственные и муниципальные информационные системы. То есть при установлении взаимодействия между двумя системами у нас не существует системы и критериев оценки, исходя из которых можно будет определять базовый элемент доверия – доверие к тому, как определены риски. Причем отдельным вопросом будет стоять не только вопрос определения неприемлемых рисков, но и вопрос определения допустимых рисков.

Единственным универсальным инструментом в руках работников подразделений информационной безопасности остается ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [6], который определяет процесс управления рисками ИБ, состоящий из следующих этапов:

- установление контекста: определение области оценки рисков ИБ, установление внешних и внутренних факторов;
- оценка риска: определение ценности информационных активов, выявление потенциальных угроз и уязвимостей, определение существующих мер и средств контроля и управления и их воздействие на идентифицированные риски, определение возможных последствий и назначение приоритетов установленным рискам, а также их ранжирование по критериям оценки риска, зафиксированным при установлении контекста;
- обработка риска: определение мер и средств контроля и управления для снижения, сохранения, предотвращения или переноса рисков;
- принятие риска: документированное решение о принятии рисков с установленной за это ответственностью;
- коммуникация риска: обмен информацией о риске или ее совместное использование;
- мониторинг и переоценки риска: проведение непрерывного мониторинга происходящих изменений и регулярный пересмотр рисков ИБ, а также способов их обработки на предмет актуальности и адекватности потенциально изменившейся ситуации.

Использование данного документа носит рекомендательный характер.

Стоит отметить: в последнее время была принята система стандартов [7–31], описывающая процесс определения рисков с точки зрения системной инженерии.

В рамках развития государственной системы защиты информации на основе ГОСТ Р 57193–2016 «Системная и программная инженерия. Процессы жизненного цикла систем» [7] в 2021 году разработаны 23 национальных стандарта (ГОСТ Р 59329, ГОСТ Р 59357 [8–31]), описывающих оценку рисков в рамках процессов в жизненном цикле системы, объединенных в 4 группы процессов:

– процессы соглашения (приобретение и поставка продукции и услуг для системы);

– процессы организационного обеспечения проекта (управление моделью жизненного цикла, инфраструктурой, портфелем проекта, человеческими ресурсами, качеством, знаниями о системе);

– процессы технического управления (планирование, оценка и контроль проекта; управление решениями, рисками, конфигурацией, информацией; измерения; гарантии качества);

– технические процессы (анализ бизнеса или назначения; определение потребностей и требований заинтересованной стороны; определение системных требований; определение архитектуры проекта; системный анализ реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, сопровождения, изъятия и списания системы).

Допускается использование стадий жизненного цикла системы различным образом, чтобы удовлетворить стратегиям разнообразного бизнеса и снизить риски. Использование стадий одновременно и в различных последовательностях может привести к формам жизненного цикла с отчетливо различными характеристиками.

Основные усилия системной инженерии для обеспечения защиты информации сосредоточены:

– на определении выходных результатов и действий, предназначенных для достижения целей процесса и защиты активов, информация о которых необходима для достижения этих целей;

– выявлении потенциальных угроз и определении возможных сценариев возникновения и развития угроз для активов, подлежащих защите, выходных результатов и выполняемых действий процесса;

– определении и прогнозировании рисков, подлежащих системному анализу;

– проведении системного анализа для обоснования мер, направленных на противодействие угрозам и достижение целей процесса.

Система стандартов опирается на математические модели, отличающиеся от подходов, изложенных в ГОСТ Р 27005–2010.

С точки зрения оценки доверия к системе управления рисками, а именно корректного определения рисков в каждом процессе, необходимо рассмотреть критерии и показатели, используемые в стандартах, определяющих системный анализ.

За основу принята вероятностная оценка следующих показателей [8–31]:

– оценка риска нарушения надежности реализации процесса без учета требований по защите информации;

– оценка риска нарушения требований по защите информации в процессе;

– оценка интегрального риска нарушения реализации процесса с учетом требований по защите информации.

Для расчета этих показателей рисков исследуемые сущности рассматривают в виде моделируемой системы сложной структуры.

Моделируемая система сложной структуры представляется как совокупность взаимодействующих элементов, каждый из которых необходимо рассматривать как «черный ящик», функционирующий в условиях неопределенности.

При анализе «черного ящика» для вероятностного прогнозирования рисков осуществляют формальное определение пространства элементарных состояний. Это пространство элементарных состояний формируют в результате статистического анализа произошедших событий с их привязкой к временной оси. Предполагается повторяемость событий. Чтобы провести системный анализ для ответа на условный вопрос «Что будет, если...», при формировании сценариев возможных нарушений статистика реальных событий по желанию исследователя процессов может быть дополнена гипотетичными событиями, характеризующими ожидаемые и(или) прогнозируемые условия функционирования системы. Применительно к анализируемому сценарию осуществляют расчет вероятности пребывания элементов моделируемой системы в определенном элементарном состоянии в течение задаваемого периода прогноза. Для негативных последствий при оценке рисков этой расчетной вероятности сопоставляют возможный ущерб.

Для математической формализации используют следующие основные положения:

– к началу периода прогноза предполагается, что целостность моделируемой системы обеспечена, включая изначальное выполнение требований по защите информации в системе (в качестве моделируемой системы простой или сложной структуры могут быть рассмотрены выходные результаты с задействованными активами и действия процесса, к которым предъявлены определенные требования, включая требования по защите информации);

– в условиях неопределенностей возникновение и разрастание различных угроз описывается в терминах случайных событий;

– для различных вариантов развития угроз средства, технологии и меры противодействия угрозам с формальной точки зрения представляют собой совокупность мер и(или) защитных преград, предназначенных для воспрепятствования реализации угроз.

Обоснованное использование выбранных мер и защитных преград является предупреждающими контрмерами, нацеленными на обеспечение реализации рассматриваемого процесса.

В общем случае для системы, представленной в виде «черного ящика», применительно к выполняемым действиям, выходным результатам рассматриваемого процесса и защищаемым активам формально определяют следующие исходные данные:

– частота возникновения источников угроз в системе с точки зрения нарушения надежности реализации процесса;

– среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности системы (выполняемых действий процесса, выходных результатов и(или) защищаемых активов) с точки зрения нарушения надежности реализации процесса;

– среднее время между окончанием предыдущей и началом очередной диагностики целостности системы;

– среднее время системной диагностики целостности системы;

– среднее время восстановления нарушенной целостности;

– задаваемая длительность периода прогноза.

Оценки осуществляют с использованием вероятностных показателей нахождения элементов моделируемой системы в определенном элементарном состоянии. Прогнозирование интегрального риска предлагается оценивать в сопоставлении с возможным ущербом по формуле

$$R_{\text{инт}}(T_{\text{зд}}) = 1 - [1 - R_{\text{нд}}(T_{\text{зд}})] \cdot [1 - R_{\text{нр}}(T_{\text{зд}})], \quad (1)$$

где $R_{\text{нд}}(T_{\text{зд}})$ – риск нарушения надежности реализации процесса без учета требований по защите информации; $R_{\text{нр}}(T_{\text{зд}})$ – риск нарушения требований по защите информации в процессе; $R_{\text{инт}}(T_{\text{зд}})$ – интегральный риск нарушения реализации процесса с учетом требований по защите информации.

Сами значения рисков $R_{\text{нд}}(T_{\text{зд}})$ и $R_{\text{нр}}(T_{\text{зд}})$ предлагается рассчитывать с использованием метода, подробно изложенного в [8–31].

В зависимости от процесса в системе стандартов приведены критерии оценки, позволяющие оценить полученные прогнозные данные.

Стоит отметить, что данные стандарты предназначены для прогнозирования рисков и прежде всего могут использоваться для построения цифровых двойников взаимодействующих систем.

В настоящей работе предлагается использовать их положения для взаимной предварительной оценки рисков в системах как перед установлением взаимодействия, так и в его процессе.

Принимая за основу показатели, приведенные для каждого из процессов, их конечную выборку следует согласовать с соответствующими подразделениями, ответственными за информационную безопасность.

Процессы управления рисками должны быть построены исходя из положений ГОСТ 27005–2010 и оцениваться также по указанным в нем требованиям.

ЗАКЛЮЧЕНИЕ

В настоящее время нормативно не определены методы и критерии оценки систем управления рисками взаимодействующих систем. В работе предлагается использовать предварительно согласованную заинтересованными сторонами выборку критериев для оценки рисков из системы стандартов [8–31], а также оценивать систему управления рисками, исходя из положений стандарта ГОСТ Р 27005–2010, что позволит создать универсальную систему, основанную не на «личном мировоззрении» отдельных работников, а на универсальной системе стандартов, исключающей субъективное мнение.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК ТО 19791–2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. – М.: Стандартинформ, 2010. – 127 с.

2. Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3. Приказ ФСТЭК России от 14.03.2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

4. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации. – 2012. – № 45, ч. 4. – Ст. 6257.

5. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателе критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // Собрание законодательства Российской Федерации. – 2018. – № 8, ч. 4. – Ст. 1204.

6. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 52 с.

7. ГОСТ Р 57193–2016. Системная и программная инженерия. Процессы жизненного цикла систем. – М.: Стандартинформ, 2016. – 99 с.

8. ГОСТ Р 59329–2021. Системная инженерия. Защита информации в процессах приобретения и поставки продукции и услуг для системы. – М.: Стандартинформ, 2021. – 27 с.

9. ГОСТ Р 59330–2021. Системная инженерия. Защита информации в процессе управления моделью жизненного цикла системы. – М.: Стандартинформ, 2021. – 29 с.

10. ГОСТ Р 59331–2021. Системная инженерия. Защита информации в процессе управления инфраструктурой системы. – М.: Стандартинформ, 2021. – 45 с.

11. ГОСТ Р 59332–2021. Системная инженерия. Защита информации в процессе управления портфелем проектов. – М.: Стандартинформ, 2021. – 33 с.

12. ГОСТ Р 59333–2021. Системная инженерия. Защита информации в процессе управления человеческими ресурсами системы. – М.: Стандартинформ, 2021. – 41 с.

13. ГОСТ Р 59334–2021. Системная инженерия. Защита информации в процессе управления качеством системы. – М.: Стандартинформ, 2021. – 31 с.

14. ГОСТ Р 59335–2021. Системная инженерия. Защита информации в процессе управления знаниями о системе. – М.: Стандартинформ, 2021. – 29 с.

15. ГОСТ Р 59336–2021. Системная инженерия. Защита информации в процессе планирования проекта. – М.: Стандартинформ, 2021. – 29 с.

16. ГОСТ Р 59337–2021. Системная инженерия. Защита информации в процессе оценки и контроля проекта. – М.: Стандартинформ, 2021. – 33 с.

17. ГОСТ Р 59338–2021. Системная инженерия. Защита информации в процессе управления решениями. – М.: Стандартинформ, 2021. – 46 с.

18. ГОСТ Р 59339–2021. Системная инженерия. Защита информации в процессе управления рисками для системы. – М.: Стандартинформ, 2021. – 47 с.

19. ГОСТ Р 59340–2021. Системная инженерия. Защита информации в процессе управления конфигурацией системы. – М.: Стандартинформ, 2021. – 29 с.

20. ГОСТ Р 59342–2021. Системная инженерия. Защита информации в процессе измерений системы. – М.: Стандартинформ, 2021. – 31 с.

21. ГОСТ Р 59344–2021. Системная инженерия. Защита информации в процессе анализа бизнеса или назначения системы. – М.: Стандартинформ, 2021. – 31 с.

22. ГОСТ Р 59345–2021. Системная инженерия. Защита информации в процессе определения потребностей и требований заинтересованной стороны для системы. – М.: Стандартинформ, 2021. – 27 с.

23. ГОСТ Р 59347–2021. Системная инженерия. Защита информации в процессе определения архитектуры системы. – М.: Стандартинформ, 2021.

24. ГОСТ Р 59348–2021. Системная инженерия. Защита информации в процессе определения проекта. – М.: Стандартинформ, 2021. – 41 с.

25. ГОСТ Р 59350–2021. Системная инженерия. Защита информации в процессе реализации системы. – М.: Стандартинформ, 2021. – 28 с.

26. ГОСТ Р 59351–2021. Системная инженерия. Защита информации в процессе комплексирования системы. – М.: Стандартинформ, 2021. – 29 с.

27. ГОСТ Р 59353–2021. Системная инженерия. Защита информации в процессе передачи системы. – М.: Стандартинформ, 2021. – 45 с.

28. ГОСТ Р 59354–2021. Системная инженерия. Защита информации в процессе аттестации системы. – М.: Стандартинформ, 2021. – 33 с.

29. ГОСТ Р 59355–2021. Системная инженерия. Защита информации в процессе функционирования системы. – М.: Стандартинформ, 2021. – 29 с.

30. ГОСТ Р 59356–2021. Системная инженерия. Защита информации в процессе сопровождения системы. – М.: Стандартинформ, 2021. – 27 с.

31. ГОСТ Р 59357–2021. Системная инженерия. Защита информации в процессе изъятия и списания системы – М.: Стандартинформ, 2021. – 46 с.

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: sfo1@mail.ru

Аникеева Вероника Валерьевна, ассистент кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: veronika.korotkova.95@mail.ru

Огнев Игорь Александрович, ассистент кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: i.ognev.2016@corp.nstu.ru

DOI: 10.17212/2782-2230-2023-1-69-82

Issues of assessing the credibility of the risk management system*

V.V. Selifanov[1], V.V. Anikeeva[2], I.A. Ognev[3]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Senior Lecturer, Department of Information Security. E-mail: sfo1@mail.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, assistant of Data Protection Department. E-mail: veronika.korotkova.95@mail.ru*
[3] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Assistant of Data Protection Department. E-mail: i.ognev.2016@corp.nstu.ru*

This article is devoted to the assessment of confidence in the risk management system. The term trust in relation to information systems is practically not used nowadays. The author proposes a procedure for assessing confidence in the risk management system, which consists of four stages: compliance with the requirements of Russian legislation and national standards, assessing the optimality of the existing risk management system and reassessing risks. A description of existing methods for assessing confidence in risk management systems has been given. It is concluded that at present there are no existing requirements to the system of risk assessment even in some segments. The paper proposes to use a pre-agreed by stakeholders' selection of criteria for assessing risks from a system of standards that describe the process of risk assessment in terms of systems engineering. The criteria and indicators used in the standards that define systems analysis are considered. Probabilistic assessment of a few indicators is taken as the basis of risk assessment: risk of violation of reliability of process implementation without regard to information protection requirements; risk of violation of information protection requirements in the process; integral risk of violation of process implementation with regard to information protection requirements. To calculate these risk indicators the investigated entities are examined in the form of a modeled system of a complex structure. A mathematical model for assessing risks in accordance with the provisions of systems engineering standards is presented.

Keywords: system architecture, risk, risk assessment, information protection, user, system engineering, information security, government information system

REFERENCES

1. State Standard R ISO/MEK TO 19791–2008. Information technology. Methods and means of ensuring safety. Safety assessment of automated systems. Moscow, Standartinform Publ., 2010. 127 p. (In Russian).

2. Order of the FSTEC of Russia dated 11.02.2013 N 17 "On approval of requirements for the protection of information not constituting a state secret contained in state information systems". (In Russian).

* *Received 17 February 2023.*

3. Order of the FSTEC of Russia dated March 14, 2014 No. 31 "On approval of the requirements for ensuring the protection of information in automated control systems for production and technological processes at critically important facilities, potentially hazardous facilities, as well as facilities that pose an increased danger to life and human health and for the environment". (In Russian).

4. Decree of the Government of the Russian Federation dated November 1, 2012 No. 1119 "On approval of requirements for the protection of personal data during their processing in personal data information systems". S Sobranie zakonodatel'stva Ros-siiskoi Federatsii = Collection of the legislation of the Russian Federation, 2012, no. 45, pt. 4, art. 6257. (In Russian).

5. Decree of the Government of the Russian Federation of 08.02.2018 No. 127 "On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values". Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the legislation of the Russian Federation, 2018, no. 8, pt. 4, art. 1204. (In Russian).

6. State Standard R ISO/MEK 27005–2010. Information technology. Methods and means of ensuring safety. Information security risk management. Moscow, Standartinform Publ., 2011. 52 p. (In Russian).

7. State Standard R ISO/MEK 27005–2010. System and software engineering. Systems Life Cycle Processes. Moscow, Standartinform Publ., 2016. 99 p. (In Russian).

8. State Standard R 59329–2021. System engineering. Protection of information in the processes of acquisition and supply of products and services for the system. Moscow, Standartinform Publ., 2021. 27 p. (In Russian).

9. State Standard R 59330–2021. System engineering. Protection of information in the process of managing the system life cycle model. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

10. State Standard R 59331–2021. System engineering. Information protection in the process of system infrastructure management. Moscow, Standartinform Publ., 2021. 45 p. (In Russian).

11. State Standard R 59332–2021. System engineering. Protection of information in the process of managing a portfolio of projects. Moscow, Standartinform Publ., 2021. 33 p. (In Russian).

12. State Standard R 59333–2021. System engineering. Protection of information in the process of managing human resources of the system. Moscow, Standartinform Publ., 2021. 41 p. (In Russian).

13. State Standard R 59334–2021. System engineering. Protection of information in the process of system quality management. Moscow, Standartinform Publ., 2021. 31 p. (In Russian).

14. State Standard R 59335–2021. System engineering. Protection of information in the process of knowledge management about the system. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

15. State Standard R 59336–2021. System engineering. Protection of information in the process of project planning. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

16. State Standard R 59337–2021. System engineering. Protection of information in the process of evaluation and control of the project. Moscow, Standartinform Publ., 2021. 33 p. (In Russian).

17. State Standard R 59338–2021. System engineering. Protection of information in the process of decision management. Moscow, Standartinform Publ., 2021. 46 p. (In Russian).

18. State Standard R 59339–2021. System engineering. Protection of information in the process of risk management for the system. Moscow, Standartinform Publ., 2021. 47 p. (In Russian).

19. State Standard R 59340–2021. System engineering. Protection of information in the process of system configuration management. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

20. State Standard R 59342–2021. System engineering. Protection of information in the process of measuring the system. Moscow, Standartinform Publ., 2021. 31 p. (In Russian).

21. State Standard R 59344–2021. System engineering. Protecting information during business analysis or system assignment. Moscow, Standartinform Publ., 2021. 31 p. (In Russian).

22. State Standard R 59345–2021. System engineering. Protection of information in the process of determining the needs and requirements of the interested party for the system. Moscow, Standartinform Publ., 2021. 27 p. (In Russian).

23. State Standard R 59347–2021. System engineering. Protection of information in system architecture definition process. Moscow, Standartinform Publ., 2021. (In Russian).

24. State Standard R 59348–2021. System engineering. Protection of information in the process of defining a project. Moscow, Standartinform Publ., 2021. 41 p. (In Russian).

25. State Standard R 59350–2021. System engineering. Protection of information in the process of system implementation. Moscow, Standartinform Publ., 2021. 28 p. (In Russian).

26. State Standard R 59351–2021. System engineering. Protection of information in the process of complexing the system. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

27. State Standard R 59353–2021. System engineering. Protection of information during the transfer of the system. Moscow, Standartinform Publ., 2021. 27 p. (In Russian).

28. State Standard R 59354–2021. System engineering. Protection of information in the process of system certification. Moscow, Standartinform Publ., 2021. 33 p. (In Russian).

29. State Standard R 59355–2021. System engineering. Protection of information in the process of system operation. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

30. State Standard R 59356–2021. System engineering. Protection of information in the process of system maintenance. Moscow, Standartinform Publ., 2021. 27 p. (In Russian).

31. State Standard R 59357–2021. System engineering. Protection of information in the process of withdrawal and decommissioning of the system. Moscow, Standartinform Publ., 2021. 46 p. (In Russian).

Для цитирования:

Селифанов В.В., Аникеева В.В., Огнев И.А. Вопросы оценки доверия к системе управления рисками // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 69–82. – DOI: 10.17212/2782-2230-2023-1-69-82.

For citation:

Selifanov V.V., Anikeeva V.V., Ognev I.A. Voprosy otsenki doveriya k sisteme upravleniya riskami [Issues of assessing the credibility of the risk management system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 1 (108), pp. 69–82. DOI: 10.17212/2782-2230-2023-1-69-82.

ПРАВИЛА ДЛЯ АВТОРОВ

УСЛОВИЯ ПРИЕМА СТАТЕЙ

Перед отправкой рукописи в редакцию авторам необходимо проверить свою статью с помощью системы «Антиплагиат». Принятый редакционной коллегией уровень оригинальности статей должен составлять не менее 85 %.

Все статьи и сопровождающие их материалы в журнал подаются через сайт журнала в электронном виде после регистрации всех авторов статьи. Регистрация обязывает каждого автора иметь международный идентификационный номер ORCID. Иные варианты подачи материалов не рассматриваются.

Автор (один из соавторов) в своем личном кабинете выбирает в меню пункт «Подать статью» и вводит все необходимые данные. Своих соавторов при этом он выбирает из списка зарегистрированных пользователей.

Рукопись статьи готовится в соответствии с правилами оформления в редакторе MS Word и прикрепляется в формате *.doc, *.docx.

Сканированные лицензионный договор с подписями авторов и экспертное заключение (цветной режим сканирования, разрешение не менее 600 dpi) необходимо также разместить на сайте журнала в разделе «Подать статью» в формате *.pdf, *.jpg, *.jpeg.

По окончании всех работ обязательно нажать кнопку «Отправить в редакцию».

В редакцию журнала предоставляются следующие материалы.

1. **Статья**, подготовленная в соответствии с правилами оформления, – печатная версия, 2 экземпляра, подписанных авторами.

2. **Контактная информация** (телефоны рабочий и сотовый, адреса электронной почты, место работы, адрес места работы, должность, ученая степень, ученое звание автора) – печатная версия, 2 экземпляра.

3. **Описание статьи для базы данных «Российский индекс научного цитирования (РИНЦ)»**, подготовленное в соответствии с правилами оформления, – печатная версия, один экземпляр.

4. **Лицензионный договор**, заполненный и подписанный.

5. **Электронная версия статьи, контактной информации, описания статьи для базы данных РИНЦ, сканированный лицензионный договор и экспертное заключение о возможности опубликования (в отдельных файлах на адрес редакции)**.

6. **Экспертное заключение о возможности опубликования**.

Редакцией рассматриваются только те материалы авторов, которые полностью соответствуют вышеобозначенным требованиям. Неполный пакет материалов редакцией не рассматривается.

Подготовленные материалы направляются на почтовый адрес редакции: 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет (НГТУ), корп. 7, ком. 606, в редакцию журнала «Безопасность цифровых технологий».

Все рукописи рецензируются, по результатам рецензирования редколлегия принимает решение о целесообразности опубликования материалов.

ВНИМАНИЕ!

Авторы несут ответственность за оформление, содержание и сам факт публикации статьи. Редакция журнала не несет ответственности за возможный ущерб, вызванный публикацией статьи. При наличии существенных недостатков в оформлении и содержании статьи редакция принимает решение об отклонении статьи без приведения полного перечня ошибок автора.

Ранее опубликованные материалы, а также материалы, представленные для публикации в других журналах, к рассмотрению не принимаются.

ПРАВИЛА ОФОРМЛЕНИЯ

При подготовке документов для отправки в редакцию журнала авторам рекомендуется внимательно прочитать правила и посмотреть примеры оформления статей и всех необходимых сопутствующих документов. Редакция рассматривает статьи, подготовленные как на русском, так и на английском языке. Для опубликования статьи на английском языке необходимо дополнительно предоставить ее русскоязычный вариант, оформленный по правилам журнала (кроме зарубежных авторов).

Чтобы статья была направлена на рецензирование, необходимо подготовить следующее:

1) **статью** в соответствии с правилами оформления;

2) **контактную информацию** в одном файле предоставить по каждому автору: ФИО полностью, ученая степень, ученое звание автора, должность, место работы, адрес места работы, телефон рабочий и мобильный, адрес электронной почты;

3) **описание статьи для базы данных «Российский индекс научного цитирования (РИНЦ)»**;

4) **лицензионный договор** заполнить, бланк лицензионного договора должен быть подписан только авторами (он доступен авторам также в личном кабинете). Если авторов несколько, то необходимо добавить поля на всех авторов и подписать каждому из них;

5) **экспертное заключение** о возможности опубликования, принятое в вашей организации;

6) согласие на публикацию, обработку и распространение персональных данных авторов статей;

7) авторы, не являющиеся сотрудниками НГТУ, предоставляют **сопроводительное письмо** на имя проректора по научной работе НГТУ (ссылка на страницу сайта НГТУ). Письмо нужно подготовить на бланке организации с подписью и печатью руководителя.

ОСНОВНЫЕ РАЗДЕЛЫ ЖУРНАЛА

1.2. Компьютерные науки и информатика.
2.2. Электроника, фотоника, приборостроение и связь.
2.3. Информационные технологии и телекоммуникации.

RULES FOR AUTHORS

CONDITIONS FOR ACCEPTANCE OF ARTICLES

Before sending the manuscript to the editorial office, authors must check their article using the Antiplagiarism system. The level of originality of articles adopted by the Editorial Board should be at least 85 %.

All articles and their accompanying materials are submitted to the magazine through the magazine's website in electronic form after registration of all the authors of the article. Registration obliges each author to have an international ORCID. No other material supply options are considered.

The author (one of the co-authors) in his personal account selects the item "Submit article" in the menu and enters all the necessary data. At the same time, he selects his co-authors from the list of registered users.

The manuscript of the article is prepared in accordance with the design rules in the MS Word editor and attached in the format * .doc, * .docx.

Scanned license agreement with signatures of authors and expert opinion (color mode scanning, resolution not less than 600 dpi) can also be attached on the website of the magazine in the section "Submit article" in the format * .pdf, * .jpg, * .jpeg.

At the end of all works, be sure to click the "Send to Design" button.

The following materials are provided to the journal editor:

1. **The article**, prepared in accordance with the rules of design, is a private version, 2 copies signed by the authors.

2. **Contact information** (working and cellular phones, e-mail addresses, place of work, address of the place of work, position, scientific degree, academic title of the author) – printed version, 2 copies.

3. **The description of the article** for the database "**Russian Scientific Citation Index (RSCI)**", prepared in accordance with the rules of form-making, is a printed version, one copy.

4. **License agreement** completed and signed.

5. **Electronic version of the article**, contact information, description of the article for the RSCI database, scanned license agreement and expert opinion on the possibility of publication (in separate files to the editorial address).

6. **Expert opinion** on the possibility of publication.

The editors consider only those materials of the authors that fully meet the above requirements. Incomplete package of materials is not considered by the revision.

The prepared materials are sent to the postal address of the editorial office: 630073, Novosibirsk, Karl Marx Prospekt, 20, Novosibirsk State Technical Univer-

sity (NSTU), building 7, office 606, to the editors of the journal "Digital Technology Security".

All manuscripts were reviewed, and according to the results of the review, the editorial board decided on the appropriateness of publishing the materials.

ATTENTION!

The authors are responsible for the design, content and the fact of publication of the article. The editorial board of the journal is not responsible for possible damage caused by the publication of the article. If there are significant shortcomings in the design and content of the article, the editorial board decides to reject the article without giving a full list of the author's mistakes.

Previously published materials, as well as materials submitted for publication in other journals, are not accepted for consideration.

FORMATTING RULES

When preparing documents for submission to the journal editor, authors are advised to carefully read the rules and see examples of the design of articles and all necessary related documents. The Drafting Committee considered articles prepared in both Russian and English. To publish the article in English, it is necessary to additionally provide its Russian-language version, drawn up according to the rules of the magazine (except for foreign authors).

For the article to be aimed at peer review, you need to prepare the following:

1) **the article** in accordance with the rules of design (volume from 7 to 30 pages);

2) **provide contact information** in one file for each author: full name, degree, academic title of the author, position, place of work, address of the place of work, telephone number of the worker and mobile, e-mail address;

3) **description of the article** for the database "Russian Scientific Citation Index (RSCI)";

4) fill out the **license agreement**, the form of the license agreement must be signed only by the authors (it is also available to the authors in the personal office), if there are several authors, then it is necessary to add fields on all authors and sign each of them;

5) **expert opinion** on the possibility of publication, adopted in your organization;

6) consent to the publication, processing and dissemination of the personal data of the authors of the articles;

7) authors who are not employees of the NSTU provide a **companion letter** addressed to the vice-rector for scientific work of the NSTU (link to the page of the

NSTU website). The letter should be prepared on the form of the organization with the signature and seal of the manager.

JOURNAL SECTION

1.2. Computer science and computer science.
2.2. Electronics, photonics, instrumentation and communications.
2.3. Information technologies and telecommunications.