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

№ 2 (109) **2023**

СОДЕРЖАНИЕ

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

Митрохин В.Е., Наумов А.С. Дистанционный мониторинг состояния заземляющего устройства 9

Шипагин В.И., Филюшов В.Ю. Модальный синтез системы управления полиномиальным методом для перевернутого маятника с двумя степенями свободы..... 21

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

Иванов А.В., Никрошкин И.В., Огнев И.А., Киселев М.А. Применение средств экспертизы Blue Team в процессе мониторинга информационных систем на примере платформы TI (Threat Intelligence) 34

Селифанов В.В., Звягинцева П.А., Плахотникова Е.А. Экспертиза модели угроз безопасности информации для информационных систем..... 52

Циберман Н.Ю., Белов В.М. Использование методологии IDEF0 в разработке системы мониторинга 71

Правила для авторов 82

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

Лицензия № ИД 04303 от 20.03.01. Подписано в печать 22.06.2023. Выход в свет 28.06.2023
Формат 60×84/16. Бумага офсетная. Тираж 300 экз. Уч.-изд. л. 5,11
Печ. л. 5,5. Изд. № 131. Заказ № 178. 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

№ 2 (109) **2023**

CONTENTS

ELECTRONICS, PHOTONICS, INSTRUMENTATION AND THE CONNECTION

Mitrokhin V.E., Naumov A.S. Remote monitoring of the condition of the grounding device 9

Shipagin V.I., Filiushov V.Yu. Modal design of a polynomial control system for the inverted pendulum with two degrees of freedom 21

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Ivanov A.V., Nikroshkin I.V., Ognev I.A., Kiselev M.A. Application of the Blue Team expertise tools in the process of monitoring information systems on the example of the TI platform (Threat Intelligence) 34

Selifanov V.V., Zvyagintseva P.A., Plahotnikova E.A. Examination of the information security threats model for information systems..... 52

Tsiberman N.Y., Belov V.M. Using the IDEF0 methodology in monitoring system development 71

Rules for authors 82

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

License № ID 04303 from 20.03.01. Signed in print June 22, 2023
Date of publication June 28, 2023. Format 60 × 84 1/16
Offset Paper. Circulation is 300 copies. Educational-ed. liter. 5,11. printed pages 5,5
Publishing number 131. Order number 178

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

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 2 (109). – 9–20

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

УДК 621.316.993 DOI: 10.17212/2782-2230-2023-2-9-20

ДИСТАНЦИОННЫЙ МОНИТОРИНГ СОСТОЯНИЯ ЗАЗЕМЛЯЮЩЕГО УСТРОЙСТВА*

В.Е. МИТРОХИН[1], А.С. НАУМОВ[2]

[1] *644046, РФ, г. Омск, пр. Маркса, 35, Омский государственный университет путей сообщения, профессор кафедры телекоммуникационных, радиотехнических систем и сетей. E-mail: mitrokhin@list.ru*
[2] *644046, РФ, г. Омск, пр. Маркса, 35, Омский государственный университет путей сообщения, аспирант кафедры телекоммуникационных, радиотехнических систем и сетей. E-mail: sommerboy@rambler.ru*

В связи с бурным развитием технологий, наращиванием объемов обмена данными и повышением требований к информационной безопасности возникает необходимость уделить особое внимание к причинам возможной потери данных. Одной из наиболее распространенных причин является качество электроснабжения телекоммуникационных сетей. Так как на кристаллах микросхем многократно увеличилась плотность элементов, напряжение пробоя этих элементов значительно уменьшилось. Следовательно, при небольшом перенапряжении или электромагнитном воздействии электронные компоненты могут выйти из строя либо могут возникнуть ошибки при передаче информации и даже может произойти уничтожение данных в запоминающих устройствах. На качество электроснабжения значительное влияние оказывает состояние заземляющего устройства, основным параметром которого является сопротивление протеканию электрического тока. Для своевременного выявления нарушения работы заземляющего устройства необходимо обеспечить дистанционный мониторинг его состояния. В статье представлены основные положения метода дистанционного мониторинга состояния заземляющего устройства.

Ключевые слова: заземляющее устройство, дистанционный контроль, сопротивление заземления, методы измерения, телекоммуникационная сеть, заземляющая система, электромагнитная совместимость, измерение сопротивления, непрерывный контроль, передача данных

* Статья получена 15 мая 2023 г.

ВВЕДЕНИЕ

В современном мире надежный обмен информацией посредством телекоммуникационных систем является одним из ключевых факторов обеспечения жизнедеятельности общества. Потеря данных или сбой информационного обмена даже на незначительный промежуток времени на объектах критической инфраструктуры может привести к серьезным последствиям. Оснащение систем телекоммуникации инновационными электронными компонентами повышает скорость и объем передачи данных, но в то же время делает их более чувствительными и уязвимыми к внешним воздействиям [1–5].

Современные технологии позволили значительно повысить плотность элементов на поверхности электронных компонентов, что привело к значительному снижению их напряжения питания, а дальнейшее усовершенствование электронных компонентов потребует еще большего снижения напряжение питания.

Такие электронные компоненты становятся крайне чувствительны даже к незначительным перепадам напряжения и внешним электромагнитным помехам.

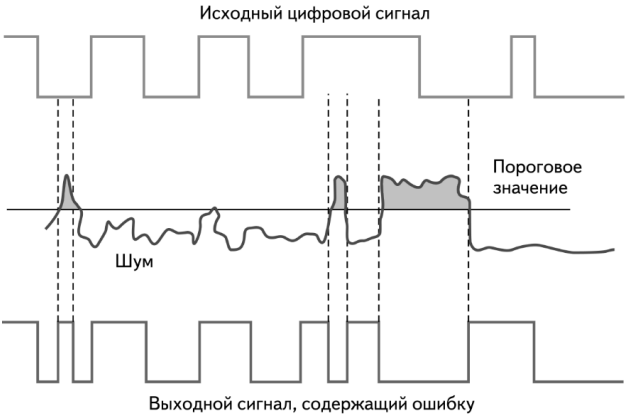

Рис. 1. График искажения данных

Fig. 1. Graph of the data distortion

Кроме того, перенапряжения способны привести к снижению срока службы электронных компонентов и даже к выходу их из строя [6].

По статистическим данным [7] Ассоциации защиты информации Российской Федерации, основной причиной потерь данных и отказа оборудования центра обработки данных компании «РТК-ЦОД» является сбой электроснабжения.

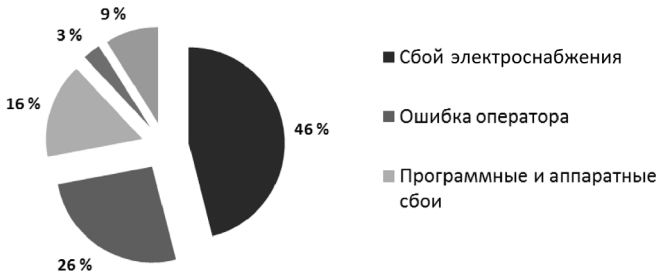

Рис. 2. Статистика отказов оборудования

Fig. 2. Equipment failure statistics

Значительное влияние на качество электроснабжения оказывает состояние заземляющего устройства опор воздушных линий, металлических корпусов оборудования подстанций и оборудования телекоммуникационных систем [8].

Надежное заземляющее устройство кроме защиты от перенапряжений способно снизить влияние индуктивных и кондуктивных помех на телекоммуникационное оборудование [9].

1. КОНТРОЛЬ СОСТОЯНИЯ ЗАЗЕМЛЯЮЩЕГО УСТРОЙСТВА

Для заземляющего устройства важнейшим параметром является величина сопротивления протеканию электрического тока. В общем случае сопротивление заземления объектов телекоммуникационных систем не должно превышать 4 Ом.

Под воздействием окружающей среды неизбежно возникает коррозия элементов заземляющего устройства, что приводит к нарушению электрического контакта и, как следствие, увеличению сопротивления протеканию электрического тока.

Для контроля состояния заземляющего устройства осуществляются периодические замеры сопротивления заземления. В общем случае контроль сопротивления заземления на объектах телекоммуникационных систем осуществляется два раза в год. А это значит, что если в промежуточный период произойдет значительное изменение сопротивления заземления под воздействием коррозии или непредвиденным механическим воздействием, то телекоммуникационное оборудование останется без защиты от перенапряжений и внешних электромагнитных помех. Кроме того, периодическое осуществление замеров сопротивления заземления требует значительных финансовых и трудовых затрат, а если подконтрольных объектов много, то затраты увеличиваются многократно [10].

2. НЕПРЕРЫВНЫЙ МОНИТОРИНГ СОСТОЯНИЯ ЗАЗЕМЛЯЮЩЕГО УСТРОЙСТВА

С целью исключения потери данных и выхода из строя оборудования телекоммуникационных систем под воздействием перенапряжений и внешних электромагнитных помех, а также снижения затрат на периодические замеры сопротивления заземления необходимо оснастить заземляющее устройство системой непрерывного дистанционного мониторинга состояния заземляющего устройства [11].

В настоящее время таких систем не существует. Используемые приборы являются переносными и либо не имеют возможности передачи данных, либо являются мультифункциональными, и их стоимость и излишний функционал не подходят для использования в качестве стационарно устанавливаемой системы. Существующие технологии основаны на сборке схемы измерения сопротивления заземления непосредственно в месте расположения контура заземления и записи показаний прибора измеренного сопротивления заземления. В разрабатываем методе это не требуется, что сокращает технико-экономические затраты и время измерения, а также повышает достоверность результатов за счет исключения человеческого фактора.

Наиболее подходящим методом измерения сопротивления заземления для использования в системе непрерывного дистанционного мониторинга является безэлектродный метод [12], основанный на взаимодействии излучающего трансформатора и трансформатора тока через контур заземляющего устройства.

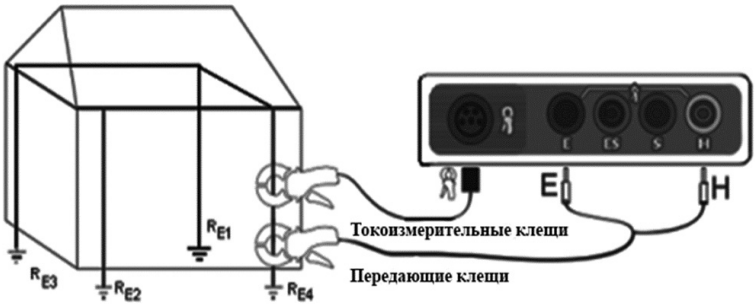

Рис. 3. Безэлектродный метод измерения сопротивления заземляющего устройства

Fig. 3. Electrodeless method for measuring the resistance of a grounding device

Такой метод измерения сопротивления заземления исключает необходимость установки дополнительных электродов, что повышает надежность, и лишает необходимости в доработке установленного заземляющего устройства

3. ПЕРЕДАЧА ДАННЫХ О СОСТОЯНИИ ЗАЗЕМЛЯЮЩЕГО УСТРОЙСТВА

При установке устройства мониторинга состояния заземляющего устройства на одиночный объект, где постоянно находится обслуживающий персонал, данные можно получать непосредственно с устройства [13, 14].

Рис. 4. Схема считывания информации о состоянии заземляющего устройства

Fig. 4. Scheme for reading information about the condition of the grounding device

Для получения истории изменения состояния заземляющего устройства данные считываются из ПЗУ через USB-интерфейс.

При отсутствии обслуживающего персонала на объекте необходимо использовать средства дистанционной передачи данных. Для одиночного объекта можно использовать радиоканал.

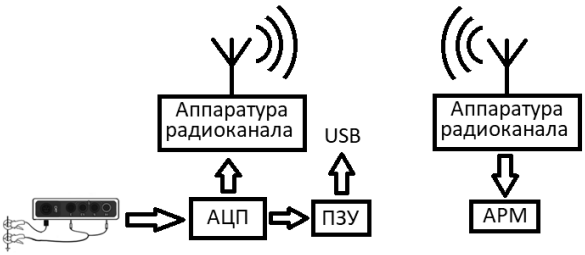

Рис. 5. Схема передачи данных посредством радиоканала

Fig. 5. Scheme of data transmission via radio channel

При наличии значительного количества объектов контроля такой способ передачи данных может быть неудобен и экономически невыгоден. Поэтому данные, полученные безэлектродным методом о состоянии заземляющего устройства с нескольких объектов контроля по волоконно-оптическим линиям связи, отправляются на сервер, где обрабатываются и сохраняются [15].

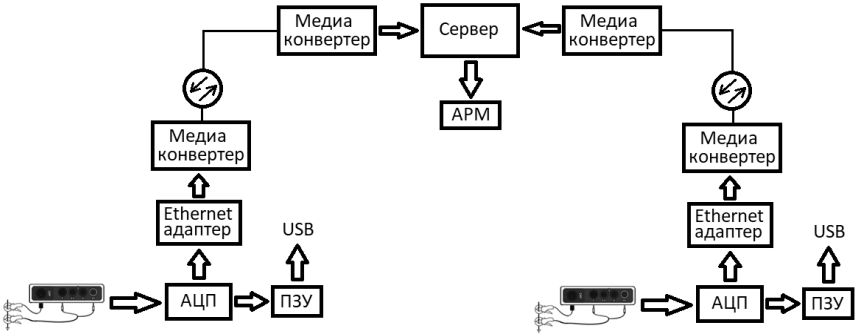

Рис. 6. Схема передачи данных посредством ВОЛС

Fig. 6. Scheme of data transmission via FOCL

В любой момент времени обслуживающий персонал с любого компьютера, подключенного к сети с сервером, может получить доступ к данным о состоянии заземляющего устройства в реальном времени и историю изменения сопротивления заземления.

По полученной информации обслуживающий персонал может принять решение о внеплановых работах по техобслуживанию или ремонту заземляющего устройства, исключив при этом возникновение сбоев в работе телекоммуникационной системы или потерю данных.

4. ПРИНЦИП ОБРАБОТКИ ДАННЫХ ОТ ДАТЧИКОВ СИСТЕМЫ НЕПРЕРЫВНОГО ДИСТАНЦИОННОГО МОНИТОРИНГА СОСТОЯНИЯ ЗАЗЕМЛЯЮЩЕГО УСТРОЙСТВА

Работа системы непрерывного дистанционного мониторинга состояния заземляющего устройства основана на сборе аналоговой информации от трех датчиков:

– датчика контроля напряжения излучающего трансформатора;
– датчика контроля измерительного тока;
– датчика контроля токов утечки.

В связи с тем, что в контролируемом заземляющем устройстве протекают как измерительный ток, так и токи утечек, для обеспечения электромагнитной совместимости и исключения взаимного влияния сигналов после датчиков устанавливаются узкополосные фильтры.

После фильтров аналоговая информация поступает на 10-битные аналого-цифровые преобразователи (АЦП) микроконтроллера. Микроконтроллер опрашивает АЦП несколько тысяч раз в секунду, что позволяет организовать дополнительный цифровой фильтр, после которого полученные данные обрабатываются микропрограммой расчета сопротивления заземляющего устройства и с интервалом в одну секунду передаются для дальнейшей обработки.

Данные о величине сопротивления заземляющего устройства и тока утечек, имеющие размер 32 бита, а также данные о дате и времени проведения измерения размером 32 бита записываются во внешнее запоминающее устройство. С учетом интервала передачи данных в одну секунду за один год непрерывного использования объем полученных данных составит 360 мегабайт, что для современных Flash-накопителей является приемлемым.

Данные, передаваемые во Flash-накопитель, передаются и на Ethernet-адаптер, где совместно с адресной информацией будут иметь объем в 64 байта. Следовательно, для обеспечения стабильной передачи данных в реальном времени необходима пропускная способность в 64 байта в секунду, что обеспечивается во всех современных цифровых линиях связи.

ЗАКЛЮЧЕНИЕ

Система непрерывного дистанционного мониторинга состояния заземляющего устройства позволит своевременно выявлять и устранять нарушения в работе заземляющего устройства, что обеспечит надежную работу телекоммуникационных систем и передачу данных, снизит затраты на ремонт дорогостоящего оборудования.

СПИСОК ЛИТЕРАТУРЫ

1. *Митрохин В.Е., Шаламов С.С.* Регистрация импульсного сигнала на базе микроконтроллерной системы // Концепции фундаментальных и прикладных научных исследований: сборник статей Международной научно-практической конференции. – Омск, 2016. – Ч. 2. – С. 62–70.

2. *Митрохин В.Е., Демиденко Д.В.* Регистрация импульсных процессов в системах телекоммуникаций и радиосвязи // Радиотехника, электроника и

связь: сборник докладов V Международной научно-технической конференции. – Омск, 2019. – С. 277–282.

3. Методика определения воздействия электромагнитного импульса на эксплуатационные характеристики электронных систем и систем связи вооружения и военной техники / Ю.Ю. Ушнурцева, В.Е. Митрохин, А.А. Сидоренко, Д.А. Писарев // Материалы VII Межвузовской научно-практической конференции «Совершенствование системы эксплуатации ВВСТ. Основные направления развития системы ремонта в ВС РФ». – Омск, 2019. – Ч. 1. – С. 211–217.

4. Цифровой имитатор сигналов GPS C/A / В.Е. Митрохин, А.В. Ряполов, Н.В. Фамбулов, Д.А. Гредяев // Техника радиосвязи. – 2021. – Вып. 1 (48). – С. 64–78. – DOI: 10.33286/2075-8693-2021-48-64-78.

5. *Митрохин В.Е., Бондаренко К.А., Ряполов А.В.* Оценка проникновения электромагнитных полей различной поляризации в экранирующую оболочку с отверстием // Доклады ТУСУР. – 2017. – № 2. – С. 125–129.

6. *Гуревич В.И.* Проблема электромагнитных воздействий на микропроцессорные устройства релейной защиты. Ч. 1 // Компоненты и технологии. – 2010. – № 2. – С. 80–84.

7. Облачный провайдинг 2014–2018: экономика, стратегии, бизнес-модели / iKS-Consulting. – URL: http://www.iksconsulting.ru/reports-91.html (дата обращения: 31.05.2023).

8. *Клименко Т.Б., Зезюля Е.В.* Заземление подвижных комплексов связи // Техника радиосвязи. – 2014. – Вып. 2 (22). – С. 33–38.

9. *Митрохин В.Е., Ряполов А.В.* Защищенность радиоэлектронных систем к дестабилизирующему воздействию электромагнитных полей // Доклады ТУСУР. – 2014. – № 2 (32). – С. 125–129.

10. *Митрохин В.Е., Рингенблюм П.Г.* Математическая модель влияния средств защиты информации на характеристики узла связи телекоммуникационной сети // Вестник СибГУТИ. – 2016. – № 1. – С. 66–73.

11. *Митрохин В.Е., Митрохин М.В.* Дистанционный мониторинг заземлений и устройств защиты // Интерэкспо Гео-Сибирь. – 2013. – Т. 5, № 1. – С. 89–93.

12. *Митрохин В.Е., Наумов А.С.* Анализ существующих методов контроля состояния заземляющего устройства // Сборник трудов III Всероссийской научно-практической конференции «Современные научные исследования: актуальные проблемы и тенденции». «Речной Форум 2022». – Омск, 2022. – Ч. 1. – С. 205–211.

13. *Митрохин В.Е., Легоцкий Е.И.* Методика выбора параметров встраиваемых систем мониторинга грозозащиты объектов телекоммуникаций // Теоретические и практические аспекты развития современной науки: материалы

XVIII Международной научно-практической конференции. – М., 2015. – С. 12–17.

14. *Митрохин В.Е., Легоцкий Е.И.* Потенциал применения микроконтроллеров для целей разработки систем мониторинга электромагнитных помех и защиты информации в оборудовании телекоммуникаций и радиосвязи // Вестник СибГУТИ. – 2016. – № 1. – С. 30–37.

15. *Mitrokhin V.E., Mitrokhin E.V., Mitrokhin M.V.* Visualization of data from the information system for monitoring leakage current from geographically distributed grounding devices of telecommunications equipment and power supply // Infographics and Information Design: Data visualization (Omsk, Russia), Scopus, 17–18 November. – Omsk, 2018.

Митрохин Валерий Евгеньевич, профессор кафедры телекоммуникационных, радиотехнических систем и сетей Омского государственного университета путей сообщения. Область научных интересов – разработка принципов и методов повышения эффективности функционирования телекоммуникационных сетей и устройств при импульсных электромагнитных воздействиях. E-mail: mitrokhin@list.ru

Наумов Александр Сергеевич, аспирант кафедры телекоммуникационных, радиотехнических систем и сетей Омского государственного университета путей сообщения. Основное направление научных исследований – разработка принципов и методов повышения эффективности функционирования телекоммуникационных сетей и устройств при импульсных электромагнитных воздействиях. E-mail: sommerboy@rambler.ru

DOI: 10.17212/2782-2230-2023-2-9-20

Remote monitoring of the condition of the grounding device*

V.E. Mitrokhin[1], A.S. Naumov[2]

[1] *Omsk State University of Communications, 35 Marx Avenue, Omsk, 644046, Russian Federation, Professor of the Department of Telecommunication, Radio Engineering Systems and Networks. E-mail: mitrokhin@list.ru*
[2] *Omsk State University of Communications, 35 Marx Avenue, Omsk, 644046, Russian Federation, postgraduate of the Department of Telecommunication, Radio Engineering Systems and Networks. E-mail: sommerboy@rambler.ru*

In connection with the rapid development of technologies, increasing the volume of data exchange and increasing requirements for information security, there is a need to pay special attention to the causes of possible data loss. One of the most common reasons is the quality of power supply of telecommunications networks. Since the density of elements on the microcircuit crystals has increased many times over, the breakdown voltage of these elements has significantly decreased. Therefore, with a slight overvoltage or electromagnetic influence, electronic components may fail, or errors may occur in the transmission of information, and even data destruction in memory devices may occur. The quality of power supply is significantly affected by the state of the grounding device, the main parameter of which is the resistance to the flow of electric current. In order to timely detect a malfunction of the grounding device, it is necessary to provide remote monitoring of its condition. The article presents the main provisions of the method of remote monitoring of the condition of the grounding device.

Keywords: Grounding device, remote control, grounding resistance, measurement methods, telecommunication network, grounding system, electromagnetic compatibility, resistance measurement, continuous monitoring, data transmission

REFERENCES

1. Mitrokhin V.E., Shalamov S.S. [Registration of a pulse signal based on a microcontroller system]. *Kontseptsii fundamental'nykh i prikladnykh nauchnykh issledovanii* [Proceedings of the International scientific and practical conference "2016 Concepts of fundamental and applied scientific research"]. Omsk, 2016, pt. 2, pp. 62–70. (In Russian).

2. Mitrokhin V.E., Demidenko D.V. [Registration of impulse processes in telecommunication and radio communication systems]. *Radiotekhnika, elektronika i svyaz'* [Materials of the V International scientific and technical conference “Radio engineering, electronics and communications”]. Omsk, 2019, pp. 277–282. (In Russian).

* *Received 15 May 2023.*

3. Ushnurtseva Yu.Yu., Mitrokhin V.E., Sidorenko A.A., Pisarev D.A. [Method for determining the impact of an electromagnetic pulse on the operational characteristics of electronic systems and communication systems of weapons, and military equipment]. *Materialy VII Mezhvuzovskoi nauchno-prakticheskoi konferentsii «Sovershenstvovanie sistemy ekspluatatsii VVST. Osnovnye napravleniya razvitiya sistemy remonta v VS RF»* [Proceedings of the VII Interuniversity scientific and practical conference "Improving the system of operation of military and military equipment. The main directions of development of the repair system in the Armed Forces of the Russian Federation]. Omsk, 2019, pt. 1, pp. 211–217. (In Russian).

4. Mitrokhin V.E.,. Ryapolov A.V, Fambulov N.V., Gredyaev D.A. Tsifrovoi imitator signalov GPS C/A [Digital simulator of GPS C/A signals]. *Tekhnika radiosvyazi = Radio Communication Technology*, 2021, iss. 1 (48), pp. 64–78. DOI: 10.33286/2075-8693-2021-48-64-78.

5. Mitrokhin V.E., Bondarenko K.A., Ryapolov A.V. Otsenka proniknoveniya elektro-magnitnykh polei razlichnoi polyarizatsii v ekraniruyushchuyu obolochku s otverstiem [Survey of the penetration in shielding enclosure with aper- ture of electromagnetic field with different polarizations]. *Doklady TUSUR = Proceedings of TUSUR University*, 2017, no. 2, pp. 125–129.

6. Gurevich V.I. Problema elektromagnitnykh vozdeistvii na mikroprotsessornye ustroistva releinoi zashchity. Ch. 1 [The problem of electromagnetic influences on microprocessor devices of relay protection]. *Komponenty i tekhnologiii = Components and Technologies*, 2010, no. 2, pp. 80–84.

7. iKS-Consulting. *Cloud provider 2014–2018: economics, strategies, business models*. (In Russian). Available at: http://www.iksconsulting.ru/reports-91.html (accessed 31.05.2023).

8. Klimenko T.B., Zezyulya E.V. Zazemlenie podvizhnykh kompleksov svyazi [Grounding of mobile communication systems]. *Tekhnika radiosvyazi = Radio Communication Technology*, 2014, iss. 2 (22), pp. 33–38.

9. Mitrokhin V.E., Ryapolov A.V. Zashchishchennost' radioelektronnykh sistem k desta-biliziruyushchemu vozdeistviyu elektromagnitnykh polei [Security of radio-electronic systems to the destabilizing effect of electromagnetic fields]. *Doklady TUSUR = Proceedings of TUSUR University*, 2014, no. 2 (32), pp. 125–129.

10. Mitrokhin V.E., Ringenblyum P.G. Matematicheskaya model' vliyaniya sredstv zashchity informatsii na kharakteristiki uzla svyazi telekommunikatsionnoi seti [Mathematical model of the effect of information security facilities on telecommunication center characteristics]. *Vestnik SibGUTI = The Herald of the Siberian State University of Telecommunications and Information Science*, 2016, no. 1, pp. 66–73.

11. Mitrokhin V.E., Mitrokhin M.V. Distantsionnyi monitoring zazemlenii i ustroistv zashchity [Remote monitoring of grounding and protection devices]. *Interekspo Geo-Sibir' = Interexpo GEO-Siberia*, 2013, vol. 5, no. 1, pp. 89–93.

12. Mitrokhin V.E., Naumov A.S. [Analysis of existing methods for monitoring the state of the grounding device]. *Sbornik trudov III Vserossiiskoi nauchno-prakticheskoi konferentsii «Sovremennye nauchnye issledovaniya: aktual'nye problemy i tendentsii». "Rechnoi Forum 2022"* [Proceedings of the International Scientific and Practical Conference "River Forum 2022"]. Omsk, 2022, pt. 1, pp. 205–211. (In Russian).

13. Mitrokhin V.E., Legotskii E.I. [Technique for selecting the parameters of embedded monitoring systems for lightning protection of telecommunications facilities]. *Teoreticheskie i prakticheskie aspekty razvitiya sovremennoi nauki* [Theoretical and practical aspects of the development of modern science]. Materials of the XVIII International Scientific and Practical Conference.Moscow, 2015, pp. 12–17. (In Russian).

14. Mitrokhin V.E., Lehocky E.I. Potentsial primeneniya mikrokontrollerov dlya tseley razrabotki sistem monitoringa elektromagnitnykh pomekh i zashchity informatsii v oborudovanii telekommunikatsiy i radiosvyazi [Microcontrollers application potential for the development of electromagnetic interference monitoring systems and information security in telecommunication and radio equipment]. *Vestnik SibGUTI = The Herald of the Siberian State University of Telecommunications and Information Science*, 2016, no. 1, pp. 30–37.

15. Mitrokhin V.E., Mitrokhin E.V., Mitrokhin M.V. Visualization of data from the information system for monitoring leakage current from geographically distributed grounding devices of telecommunications equipment and power supply. *Infographics and Information Design. Data visualization* (Omsk, Russia), Scopus 17–18 November. Omsk, 2018.

Для цитирования:

Митрохин В.Е., Наумов А.С. Дистанционный мониторинг состояния заземляющего устройства // Безопасность цифровых технологий. – 2023. – № 2 (109). – С. 9–20. – DOI: 10.17212/2782-2230-2023-2-9-20.

For citation:

Mitrokhin V.E., Naumov A.S. Distantsionnyi monitoring sostoyaniya zazemlyayushchego ustroistva [Remote monitoring of the condition of the grounding device]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 2 (109), pp. 9–20. DOI: 10.17212/2782-2230-2023-2-9-20.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 2 (109). – 21–33

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

УДК 621.382.232 DOI: 10.17212/2782-2230-2023-2-21-33

МОДАЛЬНЫЙ СИНТЕЗ СИСТЕМЫ УПРАВЛЕНИЯ ПОЛИНОМИАЛЬНЫМ МЕТОДОМ ДЛЯ ПЕРЕВЕРНУТОГО МАЯТНИКА С ДВУМЯ СТЕПЕНЯМИ СВОБОДЫ*

В.И. ШИПАГИН[1], В.Ю. ФИЛЮШОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет. E-mail: shipagin@mail.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет. E-mail: vl.fil91@gmail.com*

Приведен пример расчета системы автоматического управления для многоканальной линеаризованной модели объекта управления – двухстепенной обратный маятник на тележке со способностью к перемещению для мобильной платформы и опорной стойки в двух плоскостях. Такие системы принято называть системами с двумя степенями свободы 2-degree of freedom (2-DOF). Данная модель описывается неквадратной матричной передаточной функцией с числом выходных параметров, большим по сравнению с числом входных параметров. Получено описание линеаризованной модели объекта через пространство состояний и через матричную передаточную функцию. По полученным описаниям видно, что для линеаризованного варианта описания объекта для разных осей координат описания системы симметричны. В связи с этим существует подход к синтезу системы управления по каждой координате мобильной платформы отдельно. Однако при дальнейшем переходе к нелинейному описанию системы симметричность описания будет нарушена и применить полученные регуляторы для нелинейного объекта в некоторых случаях будет проблематично. В настоящей статье продемонстрирована работа алгоритма синтеза системы управления мобильной платформой по стабилизации опорной стойки к вертикальному положению и выводу мобильной платформы в заданное положение по обеим координатам одновременно. Расчет проводился с использованием алгоритма синтеза регулятора модальным методом, использующим полиномиальное матричное разложение матричных передаточных функций объекта и регулятора. Проведенное моделирование работы полученной системы автоматического управления показывает, что регулятор справляется с задачей стабилизации угла опорной стойки в вертикальном положении и вывода мобильной платформы в заданное положение.

* Статья получена 16 мая 2023 г.

Ключевые слова: система автоматического управления, полиномиальное матричное разложение, нейросетевой регулятор, модальный метод синтеза, неквадратный объект, многоканальная система, диофантово уравнение, управление по рассогласованию, перевернутый маятник на тележке

ВВЕДЕНИЕ

Авторы работы [1] предложили линеаризованное описание системы «перевернутый маятник на тележке со способностью к перемещению» для мобильной платформы и опорной стойки в двух плоскостях в виде системы дифференциальных уравнений, которое и будет использовано в настоящей работе. Продемонстрируем процедуру синтеза регулятора для многоканальной линеаризованной системы модальным методом, использующим полиномиальное матричное разложение матричных передаточных функций объекта и регулятора.

1. ОПИСАНИЕ СИСТЕМЫ

Тележка массой *M* находится на всенаправленных колесах и способна перемещаться как в направлении вдоль оси *X,* так и в направлении вдоль оси *Y.* К тележке закреплен перевернутый маятник массой *m.* Данная система способна отследить в каждый момент времени текущий угол отклонения перевернутого маятника от вертикали с проекцией на плоскость ZOY – φ и с проекцией на плоскость ZOX – θ, а также текущие координаты центра мобильной платформы (x, y). Длина перевернутого маятника l. Линеаризованная математическая модель двухстепенного обратного маятника на тележке может быть представлена в виде

$$\begin{cases} (M+m)\ddot{x} + ml\ddot{\theta} = F_x, \quad ml^2\ddot{\theta} + ml\ddot{x} - mgl\theta = 0; \\ (M+m)\ddot{y} + ml\ddot{\varphi} = F_y, \quad ml^2\ddot{\varphi} + ml\ddot{y} - mgl\varphi = 0, \end{cases} \tag{1}$$

где F_x – сила, приложенная к мобильной платформе вдоль оси X; F_y – сила, приложенная к мобильной платформе вдоль оси Y. В качестве параметров модели объекта примем следующие: $m = 1$, $M = 10$, $l = 1$, $g = 10$. Необходимо построить систему автоматического управления, которая выводит центр мобильной платформы в заданные координаты $(\tilde{x}, \tilde{y})$, при этом также необходимо стабилизировать углы опорной стойки $\tilde{\varphi} = 0^0$, $\tilde{\theta} = 0^0$ в вертикальном положении.

Поскольку данный объект является неквадратным (*nonsquare object*), он может быть описан матричной передаточной функцией (МПФ) неквадратного вида.

Подобные объекты рассматривались в работах [2, 3]. Воспользуемся алгоритмом синтеза регуляторов для неквадратных объектов, приведенным в [4].

Шаг 1. Получим матричную передаточную функцию объекта управления. Для этого представим систему (1) в векторно-матричном виде:

$$\begin{pmatrix} M+m & 0 & ml & 0 \\ 0 & M+m & 0 & ml \\ ml & 0 & ml^2 & 0 \\ 0 & ml & 0 & ml^2 \end{pmatrix} \begin{pmatrix} \ddot{x} \\ \ddot{y} \\ \ddot{\theta} \\ \ddot{\varphi} \end{pmatrix} = \begin{pmatrix} F_x \\ F_y \\ mgl\theta \\ mgl\varphi \end{pmatrix}. \qquad (2)$$

Запишем ее относительно ускорений:

$$\begin{pmatrix} \ddot{x} \\ \ddot{y} \\ \ddot{\theta} \\ \ddot{\varphi} \end{pmatrix} = \begin{pmatrix} M^{-1} & 0 & -(Ml)^{-1} & 0 \\ 0 & M^{-1} & 0 & -(Ml)^{-1} \\ -(Ml)^{-1} & 0 & \dfrac{M+m}{Ml^2 m} & 0 \\ 0 & -(Ml)^{-1} & 0 & \dfrac{M+m}{Ml^2 m} \end{pmatrix} \begin{pmatrix} F_x \\ F_y \\ mgl\theta \\ mgl\varphi \end{pmatrix}.$$

Пусть $x_1 = x$, $x_2 = \dot{x}$, $x_3 = y$, $x_4 = \dot{y}$, $x_5 = \theta$, $x_6 = \dot{\theta}$, $x_7 = \phi$, $x_8 = \dot{\varphi}$, $y_1 = x_1$, $y_2 = x_3$, $y_3 = x_5$, $y_4 = x_7$. Матрицы собственных свойств A, управляющих воздействий B и выходных переменных C будут иметь следующий вид:

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dfrac{-mg}{M} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dfrac{-mg}{M} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dfrac{g(M+m)}{Ml} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dfrac{g(M+m)}{Ml} & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ M^{-1} & 0 \\ 0 & 0 \\ 0 & M^{-1} \\ 0 & 0 \\ (Ml)^{-1} & 0 \\ 0 & 0 \\ 0 & (Ml)^{-1} \end{pmatrix},$$

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Как видно из указанных матриц, система имеет два канала управления и четыре выходных канала. С учетом принятых в постановке задачи параметров объекта получим передаточную функцию объекта управления:

$$W_{\text{о}} = C(sI - A)^{-1}B = \frac{1}{10s^2(s^2 - 11)} \begin{pmatrix} s^2 - 11 & 1 \\ 1 & s^2 - 11 \\ -s^2 & 0 \\ 0 & -s^2 \end{pmatrix}. \qquad (3)$$

Согласно теоремам Калмана о полной наблюдаемости и управляемости, объект наблюдаем и управляем. Это позволяет строить систему автоматического регулирования для данного объекта. Особенности управляемых объектов с вектором управляющих воздействий, меньшим по сравнению с вектором выходных каналов, показаны в работе [5].

Шаг 2. Найдем левое полиномиальное взаимно простое разложение МПФ объекта (3):

$$N_l(s) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \; D_l(s) = \begin{pmatrix} 0 & 0 & 0 & 10s^2 - 110 \\ 0 & 0 & 10s^2 - 110 & 0 \\ -11s^2/120 & -s^2/120 & 1 - 11s^2/120 & -s^2/120 \\ s^2 & 11s^2 & s^2 & 11s^2 - 120 \end{pmatrix}.$$

Взаимная простота полиномиальных матриц «числителя» и «знаменателя» МПФ объекта необходима для внутренней устойчивости всей системы (так как не происходит сокращения множителей, корни 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 [4–7].

Шаг 3. Найдем правое взаимно просто полиномиальное разложение объекта[1] и получим столбцовые степени матрицы $D_r(s)$: $\mu_1 = 4$, $\mu_2 = 4$, $\mu = \max(\mu_1, \mu_2) = 4$.

Шаг 4. Далее воспользуемся той частью алгоритма, которая предполагает использование левого полиномиального разложения МПФ объекта и правое полиномиальное разложение МПФ регулятора.

Шаг 4.1. Строчные степени матрицы $D_l(s)$: $\nu_i = 2$, $i = \overline{1,4}$ $\nu = \max(\nu_i) = 2$.

Шаг 4.2. Выразим матрицы левого полиномиального матричного описания объекта в виде числовых матриц:

$$N_0 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad D_0 = \begin{pmatrix} 0 & 0 & 0 & -110 \\ 0 & 0 & -110 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -120 \end{pmatrix}, \quad D_1 = \mathrm{O},$$

$$D_2 = \begin{pmatrix} 0 & 0 & 0 & 10 \\ 0 & 0 & 10 & 0 \\ -11/120 & -1/120 & -11/120 & -1/120 \\ 1 & 11 & 1 & 11 \end{pmatrix},$$

где $\mathrm{O} \in R^{4\times 4}$ – нулевая матрица; N_0, D_0, D_1, D_2 – числовые матрицы параметров полиномов при соответствующих операторах Лапласа s.

2. СИНТЕЗ РЕГУЛЯТОРА

Систему автоматического управления построим по принципу управления по рассогласованию. Регулятор находится в прямой связи с объектом управления. У системы присутствует единичная обратная отрицательная связь. В соответствии с рекомендациями [8] и для простоты дальнейшего вычисления характеристической матрицы замкнутой системы (ХМЗС) при использовании левого полиномиального разложения МПФ объекта обычно используется правое полиномиальное разложение МПФ регулятора: $u(s) = X_r(s)Y_r^{-1}(s)e(s)$,

[1] Из-за большого размера матриц правого взаимно простого полиномиального разложения МПФ объекта и так как они необходимы только для вычисления столбцового индекса, в статье они не приводятся.

где $u(s)=(u_j(s))_{j=\overline{1,2}}$ – вектор управляющих сигналов на выходе из регулятора и на входе в объект; $X_r(s)\in R[s]^{2\times 4}$ – «числитель» МПФ регулятора; $Y_r(s)\in R[s]^{4\times 4}$ – «знаменатель» МПФ регулятора ($R[s]^{p\times m}$ – множество матриц размером $p\times m$, элементами которой являются полиномы от s с вещественными коэффициентами); $e(s)=(e_i(s))^T_{i=\overline{1,4}}$ – вектор рассогласования между заданием $v(s)=(v_i(s))^T_{i=\overline{1,4}}$ и выходом системы $y(s)=(y_i(s))^T_{i=\overline{1,4}}$. Структурная схема системы может быть представлена в виде, показанном на рис. 1.

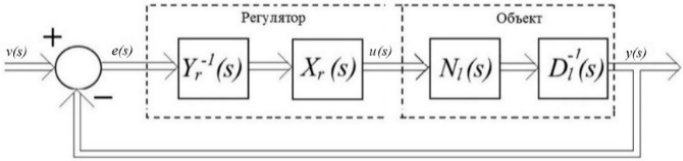

Рис. 1. Структурная схема системы «регулятор – объект»

Fig. 1. Block diagram of the "controller – object" system

Далее 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.

Шаг 4.3. Будем использовать регулятор полного порядка, поэтому столбцовые степени регулятора выбраны по формуле: $z=\mu-1=3$. Числовые матрицы, составленные из коэффициентов полиномов МПФ «числителя» $X_r(s)\in R[s]^{2\times 4}$ и «знаменателя» $Y_r(s)\in R[s]^{4\times 4}$ МПФ:

$$X_k=\left\{x_{ij}^k\right\}_{i=\overline{1,2}\ j=\overline{1,4}},\qquad Y_k=\left\{y_{ij}^k\right\}_{i=\overline{1,4}\ j=\overline{1,4}},$$

где $X_k\in R^{2\times 4}$, $Y_k\in R^{4\times 4}$ – числовые матрицы коэффициентов регулятора; x_{ij}^k, y_{ij}^k – коэффициенты регулятора; i – номер строки элемента; j – номер столбца элемента; $k=1,2,3$ – оператор, указывающий, при каком порядке

оператора полинома числится данный коэффициент. Матрица параметров регулятора примет вид: $Reg = (Y_3\ , X_3\ , Y_2\ , X_2\ , Y_1\ , X_1\ , Y_0\ , X_0\ )^T$.

Шаг 4.4. Определим степень и структуру характеристической полиномиальной матрицы системы $C(s) = \sum_{i=0}^{f} C_i s^i$, где $C_i \in \mathbb{R}^{4\times 4}$ – числовая матрица коэффициентов при соответствующих параметрах s, $f = \nu + z = 5$. Выберем желаемую[2] характеристическую матрицу замкнутой системы: $\overline{C}(s) = diag\left\{(s+1)^5\right\}$. Тогда числовые матрицы коэффициентов при соответствующих параметрах s: $\tilde{C}_0 = \tilde{C}_5 = diag\{1\}$, $\tilde{C}_1 = \tilde{C}_4 = diag\{5\}$, $\tilde{C}_2 = \tilde{C}_3 = diag\{10\}$. Блочная числовая матрица желаемых коэффициентов ХМЗС: $\aleph = \begin{pmatrix}\tilde{C}_5 & \tilde{C}_4 & \dots & \tilde{C}_0\end{pmatrix}^T$.

Шаг 4.6. Сформируем матрицу Сильвестра $\Im \in R^{p(\nu+1+n)\times(p+m)(n+1)}$ и получим $\Im \in \mathbb{R}^{24\times 24}$, $rank(\Im) = 24$. При этом в ней нулевых строк нет. Так как ранг матрицы $\Im$ полный, то переходим к шагу 4.7.

Шаг 4.7. Решим систему уравнений вида: $Reg = \Im^{-1}\aleph$ и получим параметры регулятора $\left\{x_{ij}^k\right\}_{i=\overline{1,2}\ j=\overline{1,4}}^{k=\overline{0,3}}$, $\left\{y_{ij}^k\right\}_{i=\overline{1,4}\ j=\overline{1,4}}^{k=\overline{0,3}}$.

Шаг 4.8. Эти параметры применим для МПФ «числителя» $X_r(s)$ и «знаменателя» $Y_r(s)$ регулятора и получим МПФ регулятора:

$$W_r(s) = X_r(s)Y_r^{-1}(s) =$$

$$= \begin{pmatrix} -\dfrac{11(5s+1)}{12(s+5)} & -\dfrac{5s+1}{12(s+5)} & -\dfrac{2575s+7811}{12(s+5)} & -\dfrac{5s+1}{12(s+5)} \\ -\dfrac{5s+1}{12(s+5)} & -\dfrac{11(5s+1)}{12(s+5)} & -\dfrac{5s+1}{12(s+5)} & -\dfrac{2575s+7811}{12(s+5)} \end{pmatrix}. \quad (4)$$

---

[2] Выбор желаемых полюсов характеристической матрицы замкнутой системы выходит за рамки исследуемых вопросов данной статьи. Выбранные полюса связаны с удобством вычисления полученной СЛАУ.

Характеристическая матрица замкнутой системы $C(s) = D_l(s)Y_r(s) + N_l(s)X_r(s)$ совпадает с желаемой $\tilde{C}(s)$. Значит, расчет проведен корректно.

Смоделируем систему (рис. 1), представленную объектом управления (1) и регулятором (4). В качестве задания на вход системы подадим по перемещению тележки по оси X: $\nu_1(t) = 1(t)$, по перемещению тележки по оси Y: $\nu_2(t) = -1(t)$, стабилизация углов опорной стойки в вертикальном положении $\nu_3(t) = \nu_4(t) = 0$ (рис. 2).

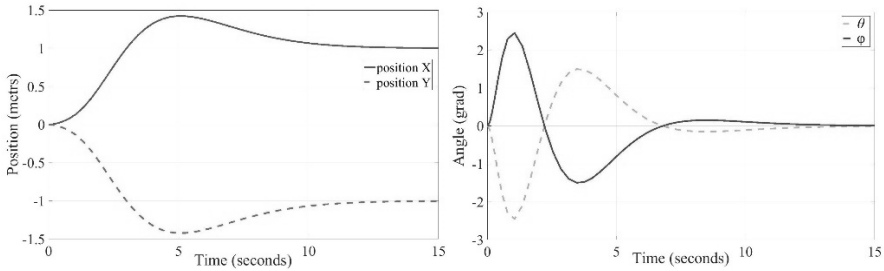

Рис. 2. Графики φ переходных процессов на выходе системы

Fig. 2. Graphs of transients at the output of the system

Как видно из представленных графиков переходных процессов, регулятор справляется с выводом тележки в заданное положение. Переходные процессы длятся около 15 секунд. Система астатична. По всем каналам присутствует перерегулирование, и в начале переходного процесса по углам опорной стойки также существует отрицательное колебание выходных параметров системы.

ЗАКЛЮЧЕНИЕ

Рассмотрен многоканальный линеаризованный объект управления (перевернутый маятник на тележке со способностью к перемещению для мобильной платформы и опорной стойки в двух плоскостях) с размерностью вектора управления, меньшей по сравнению с выходным вектором.

В работе [1] продемонстрирована система автоматического управления с управлением по каждой координате мобильной платформы по отдельности с помощью настроенных четырех ПИД-регуляторов. При этом два из них осуществляли программное управление [9] отклонением опорной стойки,

а остальные контролировали скорость движения платформы и осуществляли управление по отклонению. В работе [10] показан регулятор, синтезированный модальным и линейно-квадратичными методами для данных систем. Однако, так же как и в предыдущем случае, управление по каждой координате мобильной платформы осуществлялось раздельно. При рассмотрении линеаризованной модели объекта управления данное разделение возможно, но при рассмотрении нелинейной модели объекта появляются перекрестные взаимодействия и рассматривать отдельно виды управления не получится.

В настоящей работе продемонстрирована модель объекта управления в пространстве состояний и через МПФ. Синтез многоканального регулятора для всей системы в целом осуществлялся с принципом управления по отклонению. Кроме этого, был получен физически реализуемый многоканальный ПИ-регулятор. Синтез регулятора осуществлялся с помощью модального метода, использующего полиномиальное матричное разложение МПФ объекта и регулятора. Это, в свою очередь, позволило на демонстрируемом примере добиться астатизма по всем выходным каналам системы и меньшей колебательности переходных процессов по сравнению с САУ, предложенной в [1]. В дальнейшем планируется синтез регулятора с использованием нейросетевого аппарата для модели объекта управления, содержащей нелинейности в своей структуре.

СПИСОК ЛИТЕРАТУРЫ

1. Разработка модели и системы управления мобильным роботом для обезвешивания солнечных панелей / А.С. Беляев, А.А. Филипас, А.М. Малышенко, О.В. Суменков // Известия Тульского государственного университета. Технические науки. – 2020. – № 12. – С. 3–12. – EDN WRPEXT.

2. *Воевода А.А., Шипагин В.И.* Синтез нейросетевого регулятора управления нелинейной моделью перевернутого маятника на тележке // Научный вестник Новосибирского государственного технического университета. – 2020. – № 2–3 (79). – С. 25–36. – DOI: 10.17212/1814-1196-2020-2-3-25-36. – EDN MTQRCS.

3. *Воевода А.А., Шипагин В.И.* Синтез нейросетвого регулятора для линеаризованной модели объекта – два перевернутых маятника на тележке // Известия СпбГЭТУ «ЛЭТИ». – 2023. – Т. 16, № 1. – С. 39–52. – DOI: 10.32603/2071-8985-2023-16-1-39-52.

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

5. *Воевода А.А., Шипагин В.И.* Об управляемости и наблюдаемости многоканальных САУ при синтезе модальным методом с использованием полиномиального матричного разложения объекта и регулятора // Безопасность цифровых технологий. – 2022. – № 3 (106). – С. 26–48. – DOI: 10.17212/2782-2230-2022-3-26-48.

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

7. *Antsaklis P.J., Michel A.N.* Linear systems. – New York: McGraw-Hill, 1997. – 670 p.

8. *Бобобеков К.М.* Полиномиальный метод синтеза многоканальных регуляторов с использованием матрицы Сильвестра: дис. … канд. техн. наук: 05.13.01. – СПб., 2019. – 168 с.

9. *Ким Д.П.* Теория автоматического управления. Т. 1. Линейные системы: учебное пособие. – М.: Физматлит, 2003. – 288 с.

10. *Sumenkov O.Y., Belyaev A.S.* Comparison of control methods for inverted 2-degree of freedom pendulum mounted on the cart // IOP Conference Series: Materials Science and Engineering. – 2021. – Vol. 1118. – P. 012017. – DOI: 10.1088/1757-899X/1118/1/012017.

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

Филюшов Владислав Юрьевич, кандидат технических наук, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – управление многоканальными объектами. E-mail: vl.fil91@gmail.com

DOI: 10.17212/2782-2230-2023-2-21-33

Modal design of a polynomial control system for the inverted pendulum with two degrees of freedom*

V.I. Shipagin[1], V.Yu. Filiushov[2]

[1] *630073, Russian Federation, Novosibirsk, 20 Karl Marks Avenue, NSTU. E-mail: shipagin@mail.ru*
[2] *630073, Russian Federation, Novosibirsk, 20 Karl Marks Avenue, NSTU. E-mail: vl.fil91@gmail.com*

An example of calculating an automatic control system for a multi-channel linearized model of a control object is given – a 2-degree of freedom pendulum on a cart with the ability to move, for a mobile board and a support rack, in two planes. This model is described by a non-square matrix transfer function with a large number of output parameters compared to the number of input parameters. A description of a linear model of an object is obtained through the state space and through a matrix transfer function. According to the obtained descriptions, it can be seen that for a linearized version of the description of the object, for different coordinate axes, the description of the system is symmetrical. In this regard, there is an approach to synthesizing the control system for each coordinate of the mobile platform separately. However, with the further transition to a nonlinear description of the system, the symmetry of the description will be violated and it will be problematic to apply the obtained regulators for a nonlinear object in some cases. In this article, the work of the algorithm for the synthesis of the control system of the mobile platform for stabilizing the support rack to a vertical position and bringing the mobile platform to a given position at both coordinates at the same time is illustrated. The calculation was carried out using the algorithm of synthesis of the controller by a modular method using a polynomial matrix decomposition of the matrix transfer functions of the object and the controller. The simulation of the operation of the resulting automatic control system shows that the controller copes with the task of stabilizing the angle of the support post in the vertical position and bringing the mobile platform to the desired position.

Keywords: automatic control system, polynomial matrix decomposition, neural network controller, modal synthesis method, non-square object, multi-channel system, diophantine equation, mismatch control, inverted pendulum on a cart

REFERENCES

1. Belyaev A.S., Filipas A.A., Malyshenko A.M., Sumenkov O.Yu. Razrabotka modeli i sistemy upravleniya mobil'nym robotom dlya obezveshivaniya solnechnykh panelei [Modeling and control system development for mobile robots for solar panels weightlessness imitation]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki = News of the Tula state university. Technical sciences*, 2020, no. 12, pp. 3–12.

* *Received 16 May 2023*

2. Voevoda A.A., Shipagin V.I. Sintez neirosetevogo regulyatora upravleniya nelineinoi model'yu perevernutogo mayatnika na telezhke [Synthesis of a neural network control regulator of a nonlinear model of an inverted pendulum on a cart]. *Nauchnyi vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta = Science bulletin of the Novosibirsk state technical university*, 2020, no. 2–3 (79), pp. 25–36. DOI: 10.17212/1814-1196-2020-2-3-25-36. EDN MTQRCS.

3. Voevoda A.A., Shipagin V.I. Sintez neirosetvogo regulyatora dlya linearizovannoi modeli ob"ekta – dva perevernutykh mayatnika na telezhke [Synthesis of a neural network controller for a linearized model of an object - two inverted pendulums on a cart]. *Izvestiya SpbGETU «LETI» = LETI Transactions on Electrical Engineering & Computer Science*, 2023, vol. 16, no. 1, pp. 39–52. DOI: 10.32603/2071-8985-2023-16-1-39-52.

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

5. Voevoda A.A., Shipagin V.I. Ob upravlyaemosti i nablyudaemosti mnogokanal'nykh SAU pri sinteze modal'nym metodom s ispol'zovaniem polinomial'nogo matrichnogo razlozheniya ob"ekta i regulyatora [On controllability and observability of multichannel automatic control systems in the synthesis by the modal method using the polynomial matrix decomposition of the object and controller]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2022, no. 3 (106), pp. 26–48. DOI: 10.17212/2782-2230-2022-3-26-48.

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

7. Antsaklis P.J., Michel A.N. *Linear systems*. New York, McGraw-Hill, 1997. 670 p.

8. Bobobekov K.M. Polinomial'nyy metod sinteza mnogokanal'nykh regulyatorov s ispol'zova-niem matritsy Sil'vestra. Diss. kand. tekhn. nauk [Polynomial control method for multichannel dynamic system by Silvester matrix. PhD eng. sci. diss.]. St. Petersburg, 2019. 168 p.

9. Kim D.P. *Teoriya avtomaticheskogo upravleniya*. T. 1. *Lineinye sistemy* [The theory of automatic control. Vol. 1. Linear systems]. Moscow, Fizmatlit Publ., 2003. 288 p.

10. Sumenkov O.Y., Belyaev A.S. Comparison of control methods for inverted 2-degree of freedom pendulum mounted on the cart. *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1118, p. 012017. DOI: 10.1088/1757-899X/1118/1/012017.

Для цитирования:

Шипагин В.И., Филюшов В.Ю. Модальный синтез системы управления полиномиальным методом для перевернутого маятника с двумя степенями свободы // Безопасность цифровых технологий. – 2023. – № 2 (109). – С. 21–33. – DOI: 10.17212/2782-2230-2023-2-21-33.

For citation:

Shipagin V.I., Filiushov V.Yu. Modal'nyi sintez sistemy upravleniya polinomial'nym metodom dlya perevernutogo mayatnika s dvumya stepenyami svobody [Modal design of a polynomial control system for the inverted pendulum with two degrees of freedom]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 2 (109), pp. 21–33. DOI: 10.17212/2782-2230-2023-2-21-33.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 2 (109). – 34–51

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 004 DOI: 10.17212/2782-2230-2023-2-34-51

ПРИМЕНЕНИЕ СРЕДСТВ ЭКСПЕРТИЗЫ BLUE TEAM В ПРОЦЕССЕ МОНИТОРИНГА ИНФОРМАЦИОННЫХ СИСТЕМ НА ПРИМЕРЕ ПЛАТФОРМЫ TI (THREAT INTELLIGENCE)*

А.В. ИВАНОВ[1], И.В. НИКРОШКИН[2], И.А. ОГНЕВ[3], М.А. КИСЕЛЕВ[4]

[1] 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент, заведующий кафедрой защиты информации. E-mail: andrej.ivanov@corp.nstu.ru
[2] 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, аспирант кафедры защиты информации. E-mail: I.nikroshkin@corp.nstu.ru
[3] 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, аспирант кафедры защиты информации. E-mail: i.ognev.2016@corp.nstu.ru
[4] 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант инжинирингового центра «Информационная безопасность». E-mail: m.kiselev.2019@stud.nstu.ru

Целью данного научного исследования является анализ возможностей повышения эффективности защиты от киберугроз путем применения экспертных систем Blue Team. В работе осуществлен обзор различных экспертных систем Blue Team, включающий системы расширенного выявления и реагирования (XDR), платформы реагирования на инциденты информационной безопасности (IRP), системы управления, автоматизации и реагирования на инциденты (SOAR), а также системы киберразведки для анализа угроз (TI). Проанализированы процессы Threat Intelligence, включающие в себя сбор, анализ и интерпретацию информации о киберугрозах. Особое внимание уделено платформе киберразведки для анализа угроз – TI MISP, в том числе проанализирована модель данных этой платформы. Приведен пример работы с уязвимостью CVE-2022–26134, демонстрирующий эффективность использования платформы TI MISP для выявления угроз и принятия мер по их предотвращению. В заключении работы были сделаны выводы о преимуществах и недостатках применения платформы киберразведки для анализа угроз. В связи с этим применение экспертных систем Blue Team, включая платформу TI, в процессе мониторинга информационных систем может значительно повысить эффективность выявления компьютерных инцидентов и обеспечить более надежную защиту информационной инфраструктуры.

* Статья получена 10 мая 2023 г.

Ключевые слова: информационная безопасность, кибербезопасность, мониторинг, мониторинг событий безопасности, мониторинг информационных систем, Threat Intelligence, Blue Team, экспертные системы

ВВЕДЕНИЕ

В последнее время популярность центров мониторинга безопасности (SOC) значительно возросла, и они стали активной темой исследований [1–16]. SOC – это централизованное подразделение внутри или вне организации, которое помогает компаниям защищать свою сеть от кибератак, отслеживая инциденты информационной безопасности и реагируя на них. Операции SOC осуществляют киберанаалитики (аналитики), которым поручено обеспечить их бесперебойную работу. Аналитик обязан отслеживать, анализировать киберугрозы и инциденты и сообщать о них.

Минимальная реализация центра обработки событий (SOC) ограничивается автоматизацией сбора, нормализации и корреляции событий информационной безопасности. Однако процессы по выявлению, реагированию и расследованию инцидентов информационной безопасности выполняются вручную специалистами и аналитиками отделов по информационной безопасности. С целью повышения эффективности и оптимизации некоторых аспектов данных процессов используются экспертные системы Blue Team.

1. ЭКСПЕРТНЫЕ СИСТЕМЫ BLUE TEAM

Экспертные системы Blue Team – специализированные системы, которые используются в следующих случаях:

1) для обогащения информации о событиях и инцидентах информационной безопасности (системы Threat Intelligence, SOAR, XDR);

2) автоматизации базовых действий по реагированию на инциденты информационной безопасности (системы IRP);

3) обогащения информацией руководств (плейбуков, от англ. playbook) по реагированию на инциденты информационной безопасности (системы Threat Intelligence).

Экспертные системы Blue Team являются компьютерными системами, которые дополняют знания и решения специалистов по информационной безопасности в различных проблемных ситуациях. Они предназначены для повышения эффективности работы центров мониторинга информационных систем (SOC), которые отвечают за обнаружение, анализ инцидентов информационной безопасности и реагирование на них в ИТ-инфраструктуре организации.

1.1. XDR (Extended Detection and Response)

Концепция XDR (Extended Detection and Response) представляет собой подход к обнаружению и реагированию на киберугрозы, который обеспечивает комплексную защиту от несанкционированного доступа и атак [17–20]. Она предусматривает сбор и корреляцию данных из разных уровней безопасности, таких как конечные точки, приложения, электронная почта, облака и сети, что позволяет получить обширную картину технологической среды организации. Система XDR автоматически обнаруживает, оценивает и устраняет известные угрозы в режиме реального времени, что существенно упрощает и ускоряет работу специалистов и снижает риски сложных атак. Преимущества подхода XDR заключаются в повышении уровня защиты и снижении общих затрат на эффективное обнаружение и реагирование на угрозы безопасности.

1.2. IRP (Incident Response Platform)

IRP (от англ. Incident Response Platform) – платформа реагирования на инциденты, является системой, которая автоматизирует рутинные операции в процессе реагирования на инциденты информационной безопасности [21]. IRP позволяет собирать дополнительную информацию, локализовать и устранять угрозы, восстанавливать атакованные системы, уведомлять соответствующих заинтересованных лиц, а также собирать и структурировать данные об инцидентах кибербезопасности. Это платформа, которая служит для систематизации информации об инцидентах информационной безопасности и автоматизации действий оператора-специалиста ИБ, что существенно ускоряет процесс реагирования на угрозы безопасности.

1.3. SOAR (Security Orchestration, Automation and Response)

SOAR (от англ. Security Orchestration, Automation, and Response) представляет собой программное обеспечение, созданное для управления системами безопасности, включающее их оркестровку и координацию [22–24]. Решения SOAR позволяют собирать и обрабатывать данные о событиях безопасности из различных источников, а также автоматизировать стандартные сценарии реагирования. Объединяя различные решения безопасности в единую систему, решения SOAR позволяют экономить время специалистов по безопасности, которые больше не нуждаются в управлении каждым из них отдельно и могут сосредоточиться на анализе сложных инцидентов.

Хотя решения для управления событиями и информацией безопасности (SIEM, от англ. Security Information and Event Management) похожи на решения SOAR, эти два понятия не являются взаимозаменяемыми. SIEM и SOAR – это разные концепции для управления событиями и информацией безопасности. В отличие от решений SIEM, которые в основном направлены на сбор информации и ручное управление инцидентами, решения SOAR предназначены для автоматизации и организации работы множества различных систем безопасности, особенно на этапе реагирования. Таким образом, решения SOAR дополняют SIEM в качестве источника информации о событиях.

1.4. TI (Threat Intelligence)

Разведывательные данные об угрозах могут быть определены как информация, полученная из фактических данных о существующих или возникающих угрозах или опасностях для активов, которые могут быть использованы для принятия решений о реагировании на эти угрозы или опасности [25–27]. Термин «разведка угроз» имеет различные интерпретации, но в области информационной безопасности он означает специфические знания, которые могут быть использованы для понимания текущих угроз и их влияния на организацию или отрасль. Необходимость такой разведки является результатом зрелости и развития индустрии информационной безопасности.

Данные, полученные в результате анализа угроз, позволяют повысить осведомленность об угрозах и выбрать наиболее подходящие меры защиты, учитывая специфику деятельности организации и ее сектор экономики или отрасли. Также анализ угроз позволяет повысить качество обнаружения и реагирования на угрозы как проактивно, так и реактивно.

2. ПЛАТФОРМА THREAT INTELLIGENCE

Как было сказано ранее, Threat Intelligence – это специфические знания о кибератаках, которые эксперты по кибербезопасности систематизируют и анализируют. Эти знания (информация) могут включать:

– механизмы атаки;
– способы воздействия различных типов атак на бизнес;
– практические рекомендации по защите от атак.

Сегодня распространены многие формы кибератак, включая вредоносные программы, фишинг, атаки типа «человек посередине» и атаки типа «отказ в обслуживании». Различные способы атак на компьютерные системы и сети

постоянно развиваются по мере того, как киберпреступники находят новые уязвимости для использования. Threat Intelligence помогает организациям постоянно получать актуальную информацию о новых угрозах. Процесс Threat Intelligence можно отобразить в форме цикла, который включает в себя 5 ключевых этапов (рис. 1).

Рис. 1. Процессы Threat Intelligence

Fig. 1. Threat Intelligence processes

В процессе планирования определяются цели, требования к информации и устанавливаются приоритеты. На этапе сбора информации осуществляются действия, направленные на достижение поставленных на первом этапе целей. В рамках этого этапа используются как внутренние источники информации, так и данные от провайдеров Threat Intelligence, таких как Group-IB, Palo Alto, ESET, Kaspersky Lab, FireEye и др. На этапе обработки производится интерпретация, трансляция и унификация собранных данных. Завершающим этапом цикла является распространение информации конечным потребителям, которыми могут быть как внутренние, так и внешние подразделения информационной безопасности в филиалах, дочерних и зависимых бизнес-единицах компании. Существует несколько типов анализа угроз, включая высокоуровневую и нетехническую информацию, а также технические детали конкретных атак. Основные виды анализа угроз могут быть разделены на четыре категории.

Стратегический анализ угроз является процессом высокого уровня, направленным на выявление угроз, имеющих значение в контексте организации. При этом используется нетехническая информация, которая может быть представлена совету директоров. Примером такого анализа может служить оценка рисков, связанных с принятием бизнес-решений, которые могут сделать организацию уязвимой для кибератак.

Тактический анализ угроз включает в себя подробное изучение методов реализации угроз и разработку стратегий защиты, включая анализ векторов атак, используемых злоумышленниками, инструментов и систем, используемых для проведения атак, а также типов предприятий или технологий, которые могут быть нацелены на атаку. Это позволяет организации определить вероятность того, что она станет объектом атак, и разработать соответствующие меры по управлению рисками. Эксперты в области кибербезопасности используют тактический анализ для принятия обоснованных решений о мерах безопасности и управлении системами защиты.

Оперативный анализ угроз – это информация, которую ИТ-отдел может использовать для активного управления угрозами и принятия мер по защите от конкретных атак. Это включает информацию о намерениях злоумышленников, а также о времени и способе проведения атак.

Технический анализ угроз включает в себя изучение конкретных доказательств того, что происходит атака или использование индикаторов компрометации (IoC). Для поиска таких индикаторов используются специализированные инструменты анализа угроз, включая искусственный интеллект. Эти индикаторы могут включать содержимое электронной почты из фишинговых компаний, IP-адреса инфраструктуры C&C или артефакты из известных образцов вредоносных программ.

Для автоматизации цикла работы, описанного выше (см. рис. 1), используются специализированные платформы, называемые Threat Intelligence Platform (TIP). На молодом рынке TIP функциональными лидерами являются такие компании, как ThreatConnect, ThreatQuotinet, EclecticIQ и Anomali. Существует также много альтернатив open source, но по функциональным возможностям, регулярности обновления и поддержке сообщества можно выделить только одну достойную альтернативу коммерческим решениям – Malware Information Sharing Platform (MISP).

3. ПРАКТИКА ПРИМЕНЕНИЯ ПЛАТФОРМЫ TI MISP

MISP – это платформа анализа угроз с открытым исходным кодом, которая используется для обмена, хранения и сравнения показателей компрометации целевых атак, а также для анализа угроз. Она ранее была известна как платформа

для обмена информацией о вредоносных программах. С помощью MISP можно собирать, хранить и распространять показатели кибербезопасности и угрозы, связанные с инцидентами в этой сфере, а также обмениваться ими. MISP обеспечивает поддержку обмена информацией и ее потребления сетевыми системами обнаружения вторжений (NIDS), системами обнаружения вторжений на основе журналов (LIDS) и инструментами анализа журналов (SIEMs).

MISP, платформа для обмена информацией об угрозах, обладает возможностью создания и обновления событий, атрибутов и индикаторов через простой и интуитивно понятный пользовательский интерфейс. Кроме того, MISP позволяет экспортировать данные в различные форматы, такие как правила для IDS, OpenIOC, CSV, MISP XML или JSON, а также импортировать данные в различных форматах, включая пакетный импорт и импорт из песочницы, ThreatConnect CSV или самой платформы MISP.

Дополнительно MISP обладает Python-библиотекой с API для извлечения, добавления или обновления параметров событий, обработки образцов вредоносных программ или поиска атрибутов. Платформа поддерживает обмен данными об угрозах в формате STIX (XML и JSON), включая экспорт / импорт в формате STIX 2.0.

Все уведомления и передаваемые материалы защищены встроенным шифрованием или подтверждением при помощи электронной подписи (PGP, S/MIME) в зависимости от настроек пользователя. Кроме того, MISP позволяет интеграцию с системой IRP TheHive, что обеспечивает гибкий механизм реагирования на инциденты.

3.1. Модель данных TI MISP

Модель данных TI MISP состоит из объектов и атрибутов. Объекты представляют собой базовые элементы информации о киберугрозах, такие как уязвимости, инциденты или угрозы. Атрибуты используются для дополнительного описания этих объектов и могут содержать различные типы информации, такие как IP-адреса, домены, хэши файлов, типы файлов и другие характеристики угроз.

Модель данных TI MISP также включает в себя классификации угроз. Классификации помогают организациям категоризировать и организовывать информацию о киберугрозах для более эффективного анализа. TI MISP использует таксономии, галактики и матрицы для категоризации угроз.

Таксономии представляют собой иерархическую структуру категорий, в которых угрозы могут быть классифицированы по типу или сектору деятельности. Галактики представляют собой группы объектов и атрибутов, которые могут быть связаны между собой для образования галактик угроз. Матрицы представляют собой отношения между угрозами и таксономиями для идентификации связей между ними.

Модель данных TI MISP является гибкой и может быть расширена для учета специфических потребностей организаций.

3.2. Преимущества TI MISP

Преимущества TI MISP:

– MISP предоставляет возможность хранения технической информации о вредоносных программах и атаках, а также связывает их атрибуты и данные в структурированном формате;

– платформа делится атрибутами и данными по умолчанию с другими доверенными группами, что позволяет избежать дублирования работ и улучшить обмен информацией между организациями;

– MISP может улучшить обнаружение вредоносных программ и обратную разработку, что делает его ценным инструментом для обмена информацией;

– информация хранится локально, что обеспечивает конфиденциальность запросов;

– гибкий API позволяет интегрировать MISP с собственными решениями;

MISP предоставляет обширный формат для детального описания угроз, используя атрибуты, таксономии и галактики для кластеризации угроз.

3.3. Применение TI MISP

Рассмотрим работу TI MISP с практической точки зрения на примере уязвимости CVE-2022-26134. В результате поиска CVE были получены следующие данные, благодаря которым можно отслеживать и структурировать информацию по вышеуказаному событию (рис. 2).

Рис. 2. Графическое представление TI MISP

Fig. 2. Graphical representation of TI MISP

Также можем видеть, что TI MISP выстраивает связь объектов или атрибутов с контекстом, который дает более детальное описание объектов / атрибутов (рис. 3).

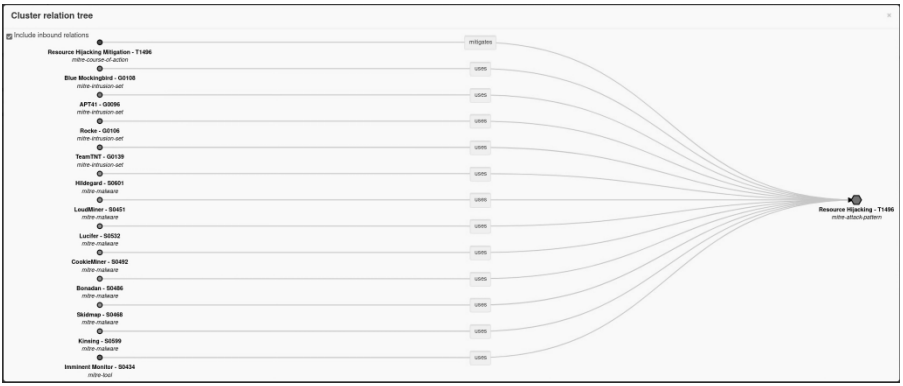

Рис. 3. Представление связи между объектами / атрибутами

Fig. 3. Representation of the relationship between objects / attributes

В данном случае на основе mitre-attack-platform было выстроено дерево отношений для DDOS-атаки с tag T1499, информацию о которой также можно найти в данной системе (рис. 4).

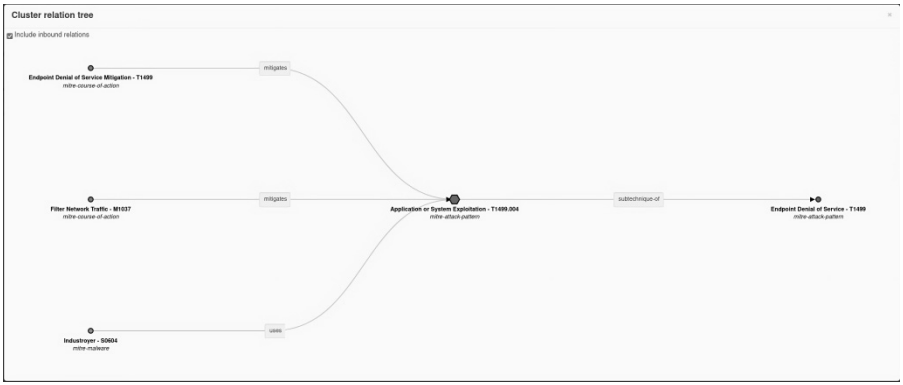

Рис. 4. Дерево отношений для DDOS-атаки

Fig. 4. Relationship tree for DDOS-attack

Также в TI MISP можно просматривать событие, которое уже полностью структурировано, по всем моделям данных (Event ID, Tags, UUID и т. д.) (рис. 5).

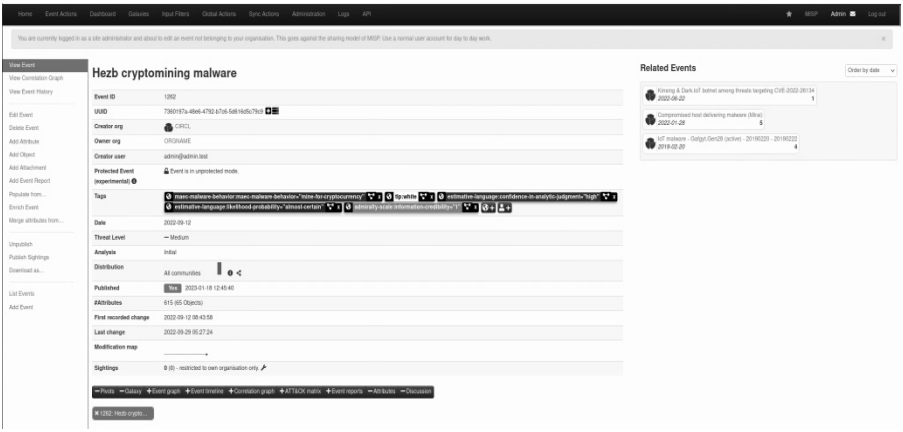

Рис. 5. Просмотр событий

Fig. 5. Viewing events

Стоит отметить, что ручное пользование TI MISP является достаточно трудоемким процессом, так как на поиск необходимой нам информации уходит достаточно много времени и сил, но эта проблема легко решается, так как платформа поддерживает интеграцию с IRP-системой TheHive, с помощью которой можно реализовать гибкий механизм реагирования на инциденты.

В данном случае был произведен анализ одного из атрибутов (hash md5) отобранного события в IRP-системе TheHive и получен отфильтрованный результат с помощью анализатора MISP 2.1. analysis, по которому уже можно ориентироваться при поиске необходимой информации для расследования инцидентов информационной безопасности (рис. 6).

ЗАКЛЮЧЕНИЕ

Применение средств экспертизы Blue Team в процессе мониторинга информационных систем на примере платформы Threat Intelligence (TI) позволяет значительно повысить эффективность защиты от киберугроз. Автоматизированные процессы анализа данных и принятия решений, реализуемые с по-

мощью экспертных систем, значительно ускоряют время реакции на потенциальные угрозы и позволяют снизить количество ложных срабатываний.

Рис. 6. Анализ отобранного атрибута с помощью IRP-системы TheHive

Fig. 6. Analysis of the selected attribute using TheHive IRP system

Ниже приведены достоинства применения Threat Intelligence.

1. Большой объем информации. При использовании Threat Intelligence собирается огромное количество информации об угрозах, которая позволяет обнаруживать новые уязвимости и способы атак.

2. Увеличение точности анализа. Благодаря обширной базе данных и возможности ее систематического обновления Threat Intelligence помогает анализировать угрозы более точно и оперативно.

3. Повышение скорости реакции. При наличии информации о новых угрозах эксперты могут оперативно принимать меры по их устранению, что позволяет минимизировать потенциальный ущерб.

4. Улучшение решений о рисках. Threat Intelligence предоставляет данные для принятия решений о том, какие риски могут возникнуть в будущем и как их можно уменьшить.

Недостатки применения Threat Intelligence.

1. Сложность анализа информации. Обработка большого объема информации, собранной с помощью Threat Intelligence, может быть трудной задачей для многих организаций. Для этого может потребоваться привлечение дополнительных ресурсов и специалистов.

2. Стоимость. Применение методологии Threat Intelligence может потребовать дополнительных затрат на приобретение соответствующего программного обеспечения и оборудования.

3. Возможность ложных срабатываний при использовании автоматизированных платформ TI. Использование Threat Intelligence может привести к ложным срабатываниям, когда экспертная система определяет какую-то действительно несуществующую угрозу.

Рассмотренная в статье модель данных TI MISP предоставляет возможность для сбора, обработки и анализа данных об угрозах, а также позволяет интегрировать данные из различных источников, что повышает качество и полноту информации от угроз информационной безопасности.

Таким образом, применение средств экспертизы Blue Team и модели данных TI MISP является эффективным подходом для повышения уровня защиты информационных систем от киберугроз. Однако необходимо учитывать, что системы защиты должны постоянно совершенствоваться и обновляться, чтобы обеспечить эффективную защиту в быстро меняющейся цифровой обстановке.

СПИСОК ЛИТЕРАТУРЫ

1. Cybersecurity incident response in organizations: an exploratory case study and process model of situation awareness / A. Ahmad, S.B. Maynard, K.C. Desouza, J. Kotsias, M.T. Whitty, R.L. Baskerville // Computers & Security. – 2021. – Vol. 101. – P. 102122.

2. *Cho S.Y., Happa J., Creese S.* Capturing tacit knowledge in security operation centers // IEEE Access. – 2020. – Vol. 8. – P. 42021–42041. – DOI: 10.1109/ACCESS.2020.2976076.

3. *Schlette D., Vielberth M., Pernul G.* CTI-SOC2M2 – The quest for mature, intelligence-driven security operations and incident response capabilities // Computers & Security. – 2021. – Vol. 111. – P. 102482. – DOI: 10.1016/j.cose.2021.102482.

4. Security operations center: a systematic survey and open challenges / M. Vielberth, F. Böhm, I. Fichtinger, G. Pernul // IEEE Access. – 2020. – Vol. 8. – P. 227756–227779. – DOI: 10.1109/ACCESS.2020.3045514.

5. *Chamkar S.A., Maleh Y., Gherabi N.* The human factor capabilities in Security Operation Centre (SOC) // EDPACS: The EDP Audit, Control, and Security Newsletter. – 2022. – Vol. 66 (1). – DOI: 10.1080/07366981.2021.1977026.

6. *Majid M.A., Ariffi K.A.Z.* Success factors for cyber security operation center (SOC) // Establishment International Conference on Informatics, Engineering, Sci-

ence and Technology. INCITEST 2019, Bandung, Indonesia, 2019. – EAI, 2019. – DOI: 10.4108/eai.18-7-2019.2287841.

7. Matched and mismatched SOCs: a qualitative Study on security operations center issues / F.B. Kokulu, T. Bao, A. Doupé, Y. Shoshitaishvili, G.-J. Ahn, Z. Zhao // CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. – ACM, 2019. – P. 1955–1970. – DOI: 10.1145/3319535.3354239.

8. *Smith M.* The SOC is dead, long live the SOC! // ITNOW. – 2020. – Vol. 62, iss. 1. – P. 34–35. – DOI: 10.1093/itnow/bwaa015.

9. A human capital model for mitigating security analyst burnout / S. Sundaramurthy, X. Ou, A.G. Bardas, J. Case, M. Wesch, J. Mchugh, S.R. Rajagopalan // Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), Ottawa, Canada, 22–24 July. – USENIX Association, 2015. – P. 347.

10. *Onwubiko C., Ouazzane K.* SOTER: a playbook for cyber security incident management // IEEE Transaction of Engineering and Management. – 2022. – Vol. 69, N 6. – P. 3771–3791. – DOI: 10.1109/TEM.2020.2979832.

11. *Onwubiko C.* Cyber security operations centre: security monitoring for protecting business and supporting cyber defense strategy // 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). – London, 2015. – DOI: 10.1109/CyberSA.2015.7166125.

12. A tale of three security operation centers / S.C. Sundaramurthy, J. Case, T. Truong, L. Zomlot, M. Hoffmann // SIW '14: Proceedings of the 2014 ACM Workshop on Security Information Workers. – ACM, 2014. – P. 43–50. – DOI: 10.1145/2663887.2663904.

13. *Andrade R.O., Yoo S.G.* Cognitive security: a comprehensive study of cognitive science in cybersecurity // Journal of Information Security and Applications. – 2019. – Vol. 48. – P. 102352.

14. *Ahmed R.K.A.* Overview of security metrics // Software Engineering. – 2016. – Vol. 4, iss. 4. – P. 59–64.

15. *Houngbo P.J., Hounsou J.T.* Measuring information security: understanding and selecting appropriate metrics // International Journal of Computer Science and Security (IJCSS). – 2015. – Vol. 9 (2). – P. 108–120.

16. What is XDR? // Microsoft Security: website. – URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-xdr (accessed: 01.06.2023).

17. What is XDR? // Palo Alto Networks: website. – URL: https://www.paloaltonetworks.com/cyberpedia/what-is-xdr (accessed: 01.06.2023).

18. What Is Extended Detection and Response (XDR)? // Cisco: website. – URL: https://www.cisco.com/c/en/us/products/security/what-is-xdr.html (accessed: 01.06.2023).

19. XDR & XDR Security. – URL: https://www.kaspersky.com/resource-center/definitions/what-is-xdr (accessed: 01.06.2023).

20. Что такое IRP (Incident Response Platform) // Энциклопедия «Касперского»: web-сайт. – URL: https://encyclopedia.kaspersky.ru/glossary/irp/ (дата обращения: 01.06.2023).

21. *Shea Sh.* SOAR (security orchestration, automation and response). – URL: https://www.techtarget.com/searchsecurity/definition/SOAR (accessed: 01.06.2023).

22. What Is SOAR? // Palo Alto Networks: website. – URL: https://www.paloaltonetworks.com/cyberpedia/what-is-soar (accessed: 01.06.2023).

23. SOAR (security orchestration, automation and response) // Энциклопедия «Касперского»: web-сайт. – URL: https://encyclopedia.kaspersky.ru/glossary/security-orchestration-automation-and-response-soar/ (accessed: 01.06.2023).

24. What is Cyber Threat Intelligence? [Beginner's guide] // CrowdStrike: website. – URL: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/ (accessed: 09.04.2023).

25. What is Threat Intelligence? – Definition, Types & Tools // VMware: website. – URL: https://www.vmware.com/topics/glossary/content/threat-intelligence.html (accessed: 01.06.2023).

26. What is Cyber Threat Intelligence? // Cisco: website. – URL: https://www.cisco.com/c/en/us/products/security/what-is-cyber-threat-intelligence.html (accessed: 01.06.2023).

Иванов Андрей Валерьевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, кибербезопасность. E-mail: andrej.ivanov@corp.nstu.ru

Никрошкин Иван Владимирович, аспирант кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – кибербезопасность, мониторинг событий безопасности, экспертные системы. E-mail: I.nikroshkin@corp.nstu.ru

Огнев Игорь Александрович, аспирант кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – кибербезопасность, мониторинг событий информационной безопасности. E-mail: i.ognev.2016@corp.nstu.ru

Киселев Максим Алексеевич, лаборант инжинирингового центра «Информационная безопасность». Основное направление научных исследований – мониторинг событий безопасности, экспертные системы. E-mail: m.kiselev.2019@stud.nstu.ru

DOI: 10.17212/2782-2230-2023-2-34-51

Application of the Blue Team expertise tools in the process of monitoring information systems on the example of the TI platform (Threat Intelligence)*

A.V. Ivanov[1], I.V. Nikroshkin[2], I.A. Ognev[3], M.A. Kiselev[4]

[1] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, PhD in Technology, head of the Information Security Department. E-mail: andrej.ivanov@corp.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, graduate student of Information Security Department. E-mail: I.nikroshkin@corp.nstu.ru*
[3] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, graduate student of Information Security Department. E-mail: i.ognev.2016@corp.nstu.ru*
[4] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant at the engineering center "Information Security". E-mail: m.kiselev.2019@stud.nstu.ru*

The purpose of this scientific study is to analyze the possibilities of increasing the effectiveness of protection against cyber threats through the use of Blue Team expert systems. The paper provides an overview of various Blue Team expert systems, including advanced detection and response (XDR) systems, information security incident response platforms (IRPs), incident management, automation and response (SOAR) systems, as well as cyber intelligence systems for threat analysis (TI). Threat Intelligence processes are analyzed, including the collection, analysis and interpretation of information about cyber threats. Particular attention is paid to the cyber intelligence platform for threat analysis – TI MISP, including the analysis of the data model of this platform. An example of working with the CVE-2022-26134 vulnerability is provided, demonstrating the effectiveness of using the TI MISP platform to identify threats and take measures to prevent them. At the end of the work, conclusions were drawn about the advantages and disadvantages of using a cyber intelligence platform for threat analysis. In this regard, the use of Blue Team expert systems, including the TI platform, in the process of monitoring information systems can significantly increase the efficiency of identifying computer incidents and provide more reliable protection of information infrastructure, despite their shortcomings.

Keywords: information security, cybersecurity, monitoring, monitoring of security events, monitoring of information systems, threat intelligence, Blue Team, expert systems

* *Received 10 May 2023.*

REFERENCES

1. Ahmad A., Maynard S.B., Desouza K.C., Kotsias J., Whitty M.T., Baskerville R.L. Cybersecurity incident response in organizations: an exploratory case study and process model of situation awareness. *Computers & Security*, 2021, vol. 101, p. 102122.

2. Cho S.Y., Happa J., Creese S. Capturing tacit knowledge in security operation centers. *IEEE Access*, 2020, vol. 8, pp. 42021–42041. DOI: 10.1109/ACCESS.2020.2976076.

3. Schlette D., Vielberth M., Pernul G. CTI-SOC2M2 – The quest for mature, intelligence-driven security operations and incident response capabilities. *Computers & Security*, 2021, vol. 111, p. 102482. DOI: 10.1016/j.cose.2021.102482.

4. Vielberth M., Böhm F., Fichtinger I., Pernul G. Security operations center: a systematic survey and open challenges. *IEEE Access*, 2020, vol. 8, pp. 227756–227779. DOI: 10.1109/ACCESS.2020.3045514.

5. Chamkar S.A., Maleh Y., Gherabi N. The human factor capabilities in Security Operation Centre (SOC). *EDPACS: The EDP Audit, Control, and Security Newsletter*, 2022, vol. 66 (1). DOI: 10.1080/07366981.2021.1977026.

6. Majid M.A., Ariffi K.A.Z. Success factors for cyber security operation center (SOC). *Establishment International Conference on Informatics, Engineering, Science and Technology. INCITEST 2019*, Bandung, Indonesia, 2019. EAI, 2019. DOI: 10.4108/eai.18-7-2019.2287841.

7. Kokulu F.B., Bao T., Doupé A., Shoshitaishvili Y., Ahn G.-J., Zhao Z. Matched and mismatched SOCs: a qualitative Study on security operations center issues. *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2019, pp. 1955–1970. DOI: 10.1145/3319535.3354239.

8. Smith M. The SOC is dead, long live the SOC! *ITNOW*, 2020, vol. 62, iss. 1, pp. 34–35. DOI: 10.1093/itnow/bwaa015.

9. Sundaramurthy S., Ou X., Bardas A.G., Case J., Wesch M., Mchugh J., Rajagopalan S.R. A human capital model for mitigating security analyst burnout. *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, Ottawa, Canada, 22–24 July. USENIX Association, 2015, p. 347.

10. Onwubiko C., Ouazzane K. SOTER: a playbook for cyber security incident management. *IEEE Transaction of Engineering and Management*, 2022, vol. 69, no. 6, pp. 3771–3791. DOI: 10.1109/TEM.2020.2979832.

11. Onwubiko C. Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, London, 2015. DOI: 10.1109/CyberSA.2015.7166125.

12. Sundaramurthy S.C., Case J., Truong T., Zomlot L., Hoffmann M. A tale of three security operation centers. *SIW '14: Proceedings of the 2014 ACM Workshop on Security Information Workers*. ACM, 2014, pp. 43–50. DOI: 10.1145/2663887.2663904.

13. Andrade R.O., Yoo S.G. Cognitive security: a comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications*, 2019, vol. 48, p. 102352.

14. Ahmed R.K.A. Overview of security metrics. *Software Engineering*, 2016, vol. 4, iss. 4, pp. 59–64.

15. Houngbo P.J., Hounsou J.T. Measuring information security: understanding and selecting appropriate metrics. *International Journal of Computer Science and Security (IJCSS)*, 2015, vol. 9 (2), pp. 108–120.

16. What is XDR? *Microsoft Security*: website. Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-xdr (accessed 01.06.2023).

17. What is XDR? *Palo Alto Networks*: website. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-xdr (accessed 01.06.2023).

18. What Is Extended Detection and Response (XDR)? *Cisco*: website. Available at: https://www.cisco.com/c/en/us/products/security/what-is-xdr.html (accessed 01.06.2023).

19. *XDR & XDR Security*. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-xdr (accessed 01.06.2023).

20. IRP (Incident Response Platform). *Enciklopedia by Kaspersky*. (In Russian). Available at: https://encyclopedia.kaspersky.ru/glossary/irp/ (accessed 01.06.2023).

21. Shea Sh. *SOAR (security orchestration, automation and response)*. Available at: https://www.techtarget.com/searchsecurity/definition/SOAR (accessed 01.06.2023).

22. What Is SOAR? *Palo Alto Networks*: website. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-soar (accessed 01.06.2023).

23. SOAR (security orchestration, automation and response). *Enciklopedia by Kaspersky*. (In Russian). Available at: https://encyclopedia.kaspersky.ru/glossary/security-orchestration-automation-and-response-soar/ (accessed 01.06.2023).

24. What is Cyber Threat Intelligence? [Beginner's guide]. *CrowdStrike*: website. Available at: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/ (accessed 09.04.2023).

25. What is Threat Intelligence? – Definition, Types & Tools.| *VMware*: website. Available at: https://www.vmware.com/topics/glossary/content/threat-intelligence.html (accessed 01.06.2023).

26. What is Cyber Threat Intelligence? *Cisco*: website. Available at: https://www.cisco.com/c/en/us/products/security/what-is-cyber-threat-intelligence.html (accessed 01.06.2023).

Для цитирования:

Применение средств экспертизы Blue Team в процессе мониторинга информационных систем на примере платформы TI (Threat Intelligence) / А.В. Иванов, И.В. Никрошкин, И.А. Огнев, М.А. Киселев // Безопасность цифровых технологий. – 2023. – № 2 (109). – С. 34–51. – DOI: 10.17212/2782-2230-2023-2-34-51.

For citation:

Ivanov A.V., Nikroshkin I.V., Ognev I.A., Kiselev M.A. Primenenie sredstv ekspertizy Blue Team v protsesse monitoringa informatsionnykh sistem na primere platformy TI (threat intelligence) [Application of the Blue Team expertise tools in the process of monitoring information systems on the example of the TI platform (Threat Intelligence)]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 2 (109), pp. 34–51. DOI: 10.17212/2782-2230-2023-2-34-51.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 2 (109). – 52–70

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 004.056.5 DOI: 10.17212/2782-2230-2023-2-52-70

ЭКСПЕРТИЗА МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ*

В.В. СЕЛИФАНОВ[1], П.А. ЗВЯГИНЦЕВА[2], Е.А. ПЛАХОТНИКОВА[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] *630108, РФ, г. Новосибирск, ул. Плахотного, 10, Сибирский государственный университет геосистем и технологий, старший преподаватель кафедры информационной безопасности. E-mail: polinasgugit@mail.ru*
[3] *630091, РФ, г. Новосибирск, ул. Красный проспект, 41, Управление ФСТЭК России по Сибирскому федеральному округу, специалист-эксперт отдела Управления ФСТЭК России. E-mail: plahotnikova.elena@mail.ru*

Основой работы является разработка автоматизированного программного средства для проведения экспертизы модели угроз безопасности информации, разрабатываемой для различных информационных систем, обрабатывающих данные на соответствие требованиям нормативным правовым актам и нормативно-методической документации, инициированных Постановлением Правительства, ФСБ России и ФСТЭК России.

Ключевые слова: модель угроз, государственная информационная система, экспертиза модели угроз, угрозы, защита информации

ВВЕДЕНИЕ

Для любых информационных систем, так или иначе подлежащих защите, необходимо разрабатывать и актуализировать модель угроз. Для государственных и муниципальных информационных систем, а также значимых объектов критической информационной инфраструктуры это является требованием соответствующих нормативных правовых документов [1–3].

Модель угроз должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов

* Статья получена 20 апреля 2023 г.

реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации [3, 4], и разрабатываться в соответствии с методическими документами ФСТЭК России [5, 6].

В настоящее время обязательным требованием для модели угроз государственных информационных систем является ее согласование с ФСТЭК России и ФСБ России, то есть проведение государственной экспертизы документов [6]. Указанная работа является весьма трудоемкой, при этом сроки проведения ограничены десятью рабочими днями. Всё это требует автоматизации процессов экспертизы. Задачей настоящей работы является разработка программного средства для автоматизации процессов экспертизы моделей угроз.

Разрабатываемое программное средство должно решить данные проблемы и уменьшить временные затраты на проведение экспертизы модели угроз за счет автоматизации процессов. Для достижения заданной цели были поставлены следующие задачи:

– анализ руководящих документов;

– исследование и реализация алгоритма создания модели угроз в государственных информационных системах (далее – ГИС);

– разработка программного средства для автоматизированного создания модели угроз.

Результатом работы является программа, позволяющая составить заключение в условиях ограниченного времени на проведение экспертизы модели угроз. С помощью этого программного средства оператор сможет проверить документ быстрее с минимизацией ошибок, связанных с человеческим фактором. Программа может использоваться работниками ФСТЭК России и ее территориальными органами или другими организациями как при проверке модели угроз, так и при ее разработке.

1. ТРЕБОВАНИЯ К МОДЕЛИ УГРОЗ ДЛЯ ПРОВЕДЕНИЯ ЭКСПЕРТИЗЫ

После изучения руководящих документов был составлен список общих требований для проведения экспертизы модели угроз безопасности информации государственных информационных систем. Для корректного создания модели угроз необходимо выявление актуальных угроз, так как именно они влияют на устанавливаемые средства защиты информации (далее – СЗИ).

Анализ требований к модели угроз [3–8] и опыт подобной работы, накопленный в Управлении ФСТЭК России по Сибирскому федеральному округу, показывает, что для проведения экспертизы достаточным условием будет оценка по следующим основным пунктам:

– оценка правильности определения класса защищенности;

– оценка правильности определения объекта воздействия и технологий, используемых для обработки информации;

– оценка правильности определения возможных негативных последствий от реализации угроз безопасности информации;

– оценка правильности определения выявления источника угроз безопасности информации, описания возможных видов нарушителей, определения категории нарушителя и уровня возможностей;

– оценка правильности определения актуальных способов реализации угроз безопасности информации;

– оценка правильности определения актуальности угроз безопасности информации;

– оценка правильности определения тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации, предлагаемая ФСТЭК России и матрицей MITRE ATT&CK [8, 9].

Актуальной считается угроза, которая может быть реализована в информационной системе и представляет опасность [20, 22–24]. При оценке возможности реализации угрозы должны быть объект воздействия, источник угрозы, способ реализации, возможные негативные последствия. Далее необходимо провести углубленный разбор каждого из пунктов.

Указанная последовательность действий детально описана в Методике определения угроз безопасности информации [6] и хорошо алгоритмизирована.

Программное обеспечение, разработанное для проведения экспертизы модели угроз, включает стандартные пункты методики [6], редактирования которых не требуется. Они необходимы для того, чтобы не рушить общий вид стандартной модели угроз. Также могут служить помощником, если программное обеспечение будет использоваться не с целью проведения экспертизы модели угроз.

В ходе оценки угроз безопасности информации должны быть определены информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям на объекты воздействия.

При анализе 222 угроз, предлагаемых банком данных угроз безопасности информации ФСТЭК России [8, 18], очевидно, что БДУ предлагает нам большое количество объектов воздействия, которые можно объединить по группам. После объединения получим:

– аппаратное обеспечение;

– системное ПО;

– программное обеспечение;
– сетевое ПО;
– прикладное ПО;
– средства виртуализации;
– информационную систему;
– сервер;
– сетевой узел, сетевой трафик;
– микропрограммное и аппаратное обеспечение BIOS / UEFI;
– мобильное устройство;
– облачную систему;
– объекты файловой системы;
– грид-систему;
– технологии Big Data (хранилища больших данных);
– суперкомпьютеры.

Даже после объединения групп в таком виде можно пронаблюдать, что список можно сократить и объединить в большие классы. Но список в том виде, в котором представлен выше, помогает минимизировать ошибки, сокращает время при определении актуальности угроз, которое потратит оператор, выполняя последний пункт программы.

Но выбора одних только объектов воздействия недостаточно, для определения актуальных угроз, при проведении экспертизы, понадобится определить возможные источники угроз, как и говорилось ранее.

2. РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА НА БАЗЕ АЛГОРИТМА ДЛЯ АВТОМАТИЗИРОВАННОГО ПРОВЕДЕНИЯ ЭКСПЕРТИЗЫ МОДЕЛИ УГРОЗ

2.1. Обзор аналогов и актуальность задачи

Программный продукт является уникальной разработкой. Проблема автоматизации при проверке моделей угроз рассматривается уже несколько лет, но на данный момент нет аналогов созданному приложению.

На сайте ФСТЭК России 04.05.2022 г. был добавлен новый раздел угроз [8]. Для формирования угроз с помощью нового раздела предлагается пройти пять этапов. На первом этапе мы попадаем на начальную страницу (рис. 1). На данный момент она не несет никакой информации, так как функционал находится в разработке. Возможно, после завершения модернизации раздела появится новая информация или изменится внешний вид.

Рис. 1. Начальная страница раздела, предназначенного для автоматизации процесса формирования перечня возможных УБИ

Fig. 1. Home page of the section designed to automate the process of generating a list of possible threats

Проанализировав наработки от ФСТЭК, можно выделить как положительные, так и отрицательные моменты. К положительным можно отнести:

– перечень угроз формируется на сайте ФСТЭК, и нет необходимости нагружать компьютер новым приложением;

– присутствует окно «Назад». Так, при совершении ошибки можно вернуться назад и исправить (добавить или убрать компонент). Нет необходимости в перезапуске страницы;

– результат подлежит фильтрации.

К отрицательным можно отнести:

– отсутствует функция копирования информации на этапе формирования перечня угроз;

– не предусматривает добавление новых источников угроз безопасности информации, а также новых сценариев реализации угроз;

– при возвращении к предыдущему этапу информация не сохраняется и требует повторного заполнения;

– при выборе возможностей нарушителя отметки делаются в хаотичном порядке.

Анализ литературы показал отсутствие методик или статей, посвященных разработке программного обеспечения для проведения экспертизы модели угроз безопасности информации в государственных информационных системах.

Отсюда и вытекает вывод об актуальности создания такого программного продукта для ускоренного проведения экспертизы разработанных моделей угроз.

2.2. Реализация программного приложения

Для решения поставленной задачи было разработано программное обеспечение. Приложение разработано для проведения экспертизы модели угроз безопасности информации в информационных системах. Приложение ориентировано на операторов, специалистов по защите информации и т. д. Но и неопытный пользователь справится с построением модели угроз. Именно построением, проведением экспертизы должен заниматься специалист.

По результатам работы с программным обеспечением выдается отчет с базовым заполнением документа, актуальными угрозами и подобранными для них тактиками, и соответствующими им типовыми техниками, предлагаемыми ФСТЭК России и матрицей MITRE ATT&CK (для некоторых угроз отсутствуют возможные сценарии реализации; при обновлении документов, содержащих техники и тактики, программа будет дополняться и обновляться) [8, 9]. Отчет можно редактировать, выводить на печать.

Программное обеспечение включает в себя девять диалоговых окон:

1) начальная страница;
2) определение класса защищенности;
3) определение объектов воздействия;
4) выбор видов риска;
5) негативные последствия после выбора риска;
6) определение нарушителя;
7) выбор источника угрозы;
8) возможность реализации угрозы безопасности информации;
9) завершение работы программы. Формирование и сохранение отчета.

Дизайн приложения позволяет оператору быстро адаптироваться к интерфейсу программного обеспечения. На рис. 2 изображена начальная страница.

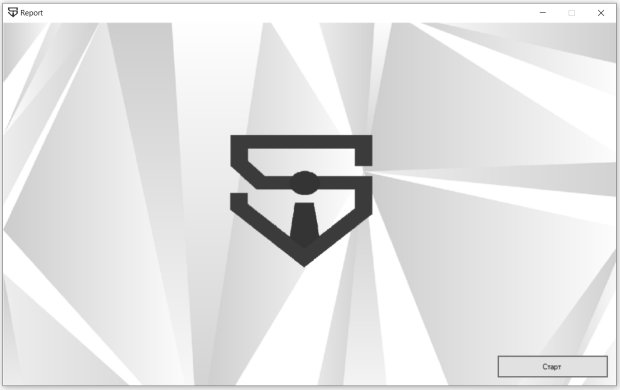

Рис. 2. Главное окно программы

Fig. 2. The main program window

Следующее окно открывается после нажатия кнопки «Старт». В нем необходимо выбрать уровень значимости информации и масштаб системы, как показано на рис. 3. После выбора двух компонентов автоматически подбирается класс защищенности. Если не выбрать один из компонентов, всплывает окно с просьбой о заполнении. Без заполнения всех окон на следующую страницу не перейти. Отчет начинает заполняться сразу после запуска программы.

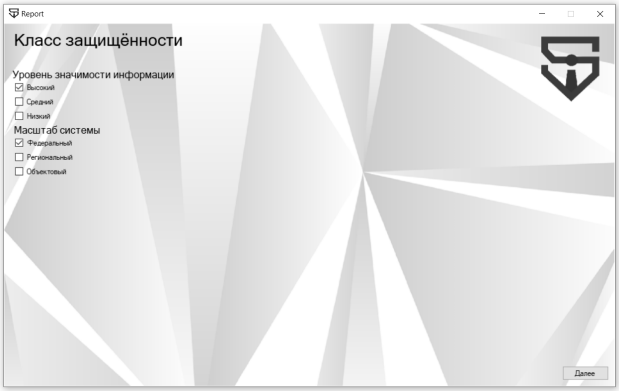

Рис. 3. Определение класса защищенности

Fig. 3. Security class defenition

После перехода на третье окно, которое изображено на рис. 4, приложение предлагает список объектов воздействия, который заранее объединен по классам, с возможностью выбора применения / неприменения конкретного объекта в системе.

От выбора объекта зависит дальнейшая работа программы, поэтому оператору важно на данном этапе не допустить ошибку.

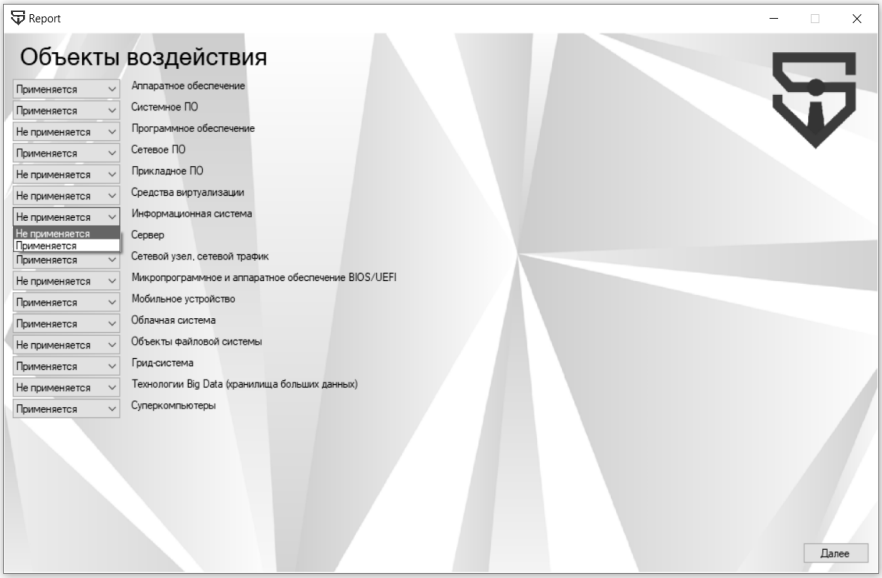

Рис. 4. Выбор объектов воздействия

Fig. 4. Security class definition

На следующем этапе оператору предлагается выбрать виды риска. От выбора видов риска на этом этапе зависит список предложенных возможных типовых негативных последствий. Можно выбрать все три, можно одну, всё зависит от рассматриваемой системы.

Далее предлагается список негативных последствий согласно выбранному риску. Предыдущий и настоящий пункты не влияют на дальнейшую работу программы. Это стандартные пункты при составлении модели угроз для проверки оператором.

В программе на выбор предлагается список видов нарушителей, для которых нужно выбрать категорию и потенциал [4].

Категория делится на три типа:

1) внешний;
2) внутренний (наличие постоянного доступа в контролируемую зону);
3) внутренний (наличие разового доступа в контролируемую зону).

Источник угрозы бывает четырех видов:

1) Н1 – нарушитель, обладающий базовыми возможностями;
2) Н2 – нарушитель, обладающий базовыми повышенными возможностями;
3) Н3 – нарушитель, обладающий средними возможностями;
4) Н4 – нарушитель, обладающий высокими возможностями.

Далее переходим к основной части. Именно это окно формирует предлагаемые на следующем этапе актуальные угрозы. На рис. 5 видим, что окно содержит ранее выбранные объекты воздействия, и для них предлагается выбрать категорию и потенциал нарушителя. Список источников угроз немного урезан. Так, окно 7 содержит всего две характеристики и три потенциала нарушителя, в отличие от окна 6.

После выбора источника угроз формируется список возможных угроз и отображается в следующем окне, реализацию работы можно увидеть на рис. 5. На данном этапе оператор должен выбрать угрозы, актуальные для конкретной системы, и при проведении экспертизы исключить лишние из проверяемой модели угроз.

Оператору предлагается список угроз на основе выбираемых ранее объектов воздействия и источников угроз с указанием, возможна ли угроза, и если нет, то почему.

В данном окне можно увидеть несовершенство работы с Visual Studio. Фоновая картинка растягивается в зависимости от количества подходящих угроз. В будущем данная проблема должна быть исправлена, либо можно разбить список актуальных угроз на несколько окон так, чтобы высвечивалось только определенное количество угроз, которое помещается в стандартное окно.

Время заполнения отчета индивидуально и зависит от списка актуальных угроз, так как при заполнении отчета заполняются и таблицы с тактиками и соответствующими им типовыми техниками, используемыми для построения сценариев реализации угроз безопасности информации по методике ФСТЭК России и матрице MITRE ATT&CK [8, 9]. Каждой тактике соответствует некоторое количество техник – хорошо известных приемов, позволяющих нарушителю выполнить нужное ему действие в рамках решения стоящей перед ним в этот момент тактической задачи.

Рис. 5. Выбор объектов воздействия

Fig. 5. Security class definition

Выбор тактик и техник по методике ФСТЭК России осуществляется по методическому документу «Методика оценки угроз безопасности информации» [4].

Плюс такой таблицы в том, что она структурирована. Техники не повторяются в других тактиках. Отсутствуют пересечения, что позволяет удобно перемещаться по таблице.

Параллельно с этим существуют иные практики по структурированию действий нарушителей кибербезопасности, и самая популярная из них – матрица MITRE ATT&CK. Моделирование угроз в методике ФСТЭК во многом основано не тактиках и техниках MITRE Att&CK, но моделировать угрозы только на основе базы знаний MITRE Att&CK не получится.

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации.

Выбор тактик и техник с помощью матрицы MITRE ATT&CK. В MITRE выделили 12 тактических задач (тактик), которые приходится решать нарушителю и из которых складывается сценарий, в то время как методика ФСТЭК предлагает нам всего 10.

Главными источниками данных в ATT&CK являются публично доступные отчеты об инцидентах и исследованиях угроз компьютерной безопасности. Из них выделяются общие тактики, техники и процедуры. Также используются публично доступные исследования новых техник, схожих с уже известными поведениями, поэтому они регулярно обновляются.

Когда актуальные угрозы для рассматриваемой системы выбраны, программа отсылает оператора на финальный этап. Формирование отчета может занять некоторое время в зависимости от количества угроз.

3. АПРОБАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Разработанное приложение для проведения экспертизы модели угроз безопасности информации информационных систем применяется для быстрого получения результатов и проверки составленной модели угроз.

Приложение применяется во время проведения экспертизы работниками следующих учреждений:

– Управления ФСТЭК России по Сибирскому федеральному округу;
– ООО «Центр информационной безопасности», г. Барнаул;
– ООО «Акстел-Безопасность», г. Новосибирск;
– ООО «СИБ», г. Новосибирск;
– филиала АО «БИТК», г. Воронеж.

Благодаря универсальности программы ее можно использовать как для проведения экспертизы, так и для составления самой модели угроз. В любом случае программа будет служить хорошим помощником и поможет существенно сократить время на выполнение поставленных задач.

ЗАКЛЮЧЕНИЕ

В процессе работы было разработано программное обеспечение для создания модели угроз безопасности информации информационных систем. Данный продукт позволяет существенно сократить временные расходы за счет автоматизации процессов. Также разработанное программное обеспечение уменьшает количество ошибок, связанных с человеческим фактором. Избегать ошибок помогает то, что все данные уже внесены в программу и нельзя пропустить или не указать важные характеристики. Хоть процесс и автоматизирован, исключать оператора из цепочки нельзя.

В ходе работы были решены следующие задачи:

– проведен системный анализ предметной области;
– рассмотрено применение документов ФСТЭК России в области защиты государственных информационных систем;

– исследован и реализован алгоритм по созданию модели угроз для государственных информационных систем;

– разработано программное обеспечение с целью автоматизации создания модели угроз.

В настоящей работе большое внимание уделялось именно реализации алгоритма построения модели угроз и созданию программного обеспечения, так как на данный момент нет аналогов данному приложению, а проверка документов оператором занимает большое количество времени.

Были получены отзывы от пользователей приложения при его тестировании и обнаружены некоторые ошибки на этапе подбора класса защищенности, при фильтрации угроз и в наименовании одной из угроз. Подробно рассмотрим ошибки.

1. Выбор класса защищенности. Проблема связана с человеческим фактором. При написании кода приложения была допущена ошибка, поэтому после заполнения отчета можно было заметить, что класс защищенности выдавался не точно.

Пример: в соответствии с приказом ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» установлен первый класс защищенности (К3).

2. Фильтрация угроз. Так как угрозы по объектам воздействия и по потенциалу нарушителя были рассмотрены в разных таблицах, при наложении одной на другую возникли проблемы, и не все угрозы были учтены правильным образом. Проблема была решена следующим образом: все угрозы были вручную вписаны в код программного обеспечения.

3. Наименование угрозы. Из-за большого объема обрабатываемой информации сработал человеческий фактор и УБИ118 «Угроза перехвата привилегированного процесса» была написана дважды, исключив из списка УБИ119 «Угроза перехвата управления гипервизором». Ошибка заключалась только в неправильном наименовании угрозы, техники и тактики были занесены в код правильно, поэтому устранить проблему было достаточно просто.

Благодаря внедрению приложения в организации и оперативному тестированию этого приложения компетентными сотрудниками ошибки были найдены и исправлены в кратчайшие сроки.

Применение данной программы на практике показало, что существенно сокращается время на создание модели угроз, а соответственно, и проведение экспертизы, так как существуют заготовки, которые помогают не пропустить нужные разделы, и минимизируется количество ошибок, связанных с челове-

ческим фактором. Простой интерфейс приложения помогает с первых секунд использования влиться в работу.

Приложение может использовать любая организация, которая занимается построением или проведением экспертиз модели угроз безопасности информации информационных систем. Программу благодаря ее универсальности используют как для проведения экспертизы, так и для разработки самой модели угроз. Программа служит хорошим помощником и помогает существенно сократить время на выполнение поставленных задач.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и защите информации» // Собрание законодательства Российской Федерации. – 2006. – № 31, ч. 1–2. – Ст. 3448.

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. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

4. Методический документ. Методика оценки угроз безопасности информации: утв. ФСТЭК России 5 февраля 2021 г.

5. Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // Собрание законодательства Российской Федерации. – 2015. – № 28, ч. 4. – Ст. 4241.

6. Методика определения угроз безопасности информации: методический материал. – М.: ФСТЭК, 2021. – 83 с.

7. Методический документ. Меры защиты в государственных информационных системах: утв. ФСТЭК России 11 февраля 2014 г.

8. Банк данных угроз безопасности информации: web-сайт. – URL: https://bdu.fstec.ru/ (дата обращения: 01.06.2023).

9. MITRE ATT&CK: website. – URL: https://attack.mitre.org/ (accessed: 01.06.2023).

10. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008. – 9 с.

11. ГОСТ Р 56545–2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. – М.: Стандартинформ, 2018. – 13 с.

12. ГОСТ Р 51624–2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. – М.: Госстандарт России, 2001.

13. ГОСТ 34.602–89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. – М.: Стандартинформ, 2009. – 13 с.

14. Microsoft. Visual Studio: web-сайт. – URL: https://visualstudio.microsoft.com/ru/ (дата обращения: 01.06.2023).

15. Законы, кодексы и нормативно-правовые акты Российской Федерации: web-сайт. – URL: https://legalacts.ru/doc/FZ-ob-informacii-informacionnyh-tehnologijah-i-o-zawite-informacii/ (дата обращения: 01.06.2023).

16. Консультант Плюс: web-сайт. – URL: http://www.consultant.ru (дата обращения: 01.06.2023).

17. Техэксперт: web-сайт. – URL: http://docs.cntd.ru (дата обращения: 01.06.2023).

18. Федеральная служба по техническому и экспортному контролю: web-сайт. – URL: https://fstec.ru (дата обращения: 01.06.2023).

19. Microsoft. Документация по C#. – URL: https://docs.microsoft.com/ru-ru/dotnet/csharp/ (дата обращения: 01.06.2023).

20. Хабр. О моделировании угроз. – URL: https://habr.com/ru/company/cloud4y/blog/350228/ (дата обращения: 01.06.2023).

21. *Ковалева Н.Н., Холодная Е.В.* Комментарий к Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. – 2006. – 29 июля (№ 165).

22. *Степанов В.А.*, *Андреев Н.Д.* Моделирование угроз безопасности информации по новой методике ФСТЭК, используя средства автоматизации // Информационные технологии. Проблемы и решения. – 2021. – № 4 (17). – С. 95–101.

23. *Дорошенко И.Е., Максудов М.О., Селифанов В.В.* Вопросы описания возможных сценариев угроз при разработке моделей угроз безопасности информации // Интерэкспо Гео-Сибирь. – 2021. – Т. 7, № 1. – С. 16–21.

24. *Стариковская Н.А., Слепухина Ю.В.* Разработка модели угроз для государственной информационной системы // Материалы Афанасьевских чтений. – 2022. – № 2 (39). – С. 36–41.

25. *Татарникова Т.М., Яготинцева Н.В.* Модель обеспечения информационной безопасности ГИС // Научный альманах. – 2016. – № 1-1 (15). – С. 521–523. – EDN: VPSCAN.

26. *Татарникова Т.М., Яготинцева Н.В.* Угрозы информационной безопасности ГИС // Региональная информатика и информационная безопасность. – СПб., 2016. – Вып. 2. – С. 137–142.

27. *Prokushev Y.E., Ponomarenko S.V., Ponomarenko S.A.* Modeling the processes of designing information security systems in state information systems // Computational Nanotechnology. – 2021. – Vol. 8, iss. 1. – P. 26–37.

28. *Борщева Н.В.* Особенности построения модели угроз безопасности информации для государственных информационных систем // Современные проблемы проектирования, производства и эксплуатации радиотехнических систем. – Ульяновск, 2019. – С. 163–166.

29. *Курносов К.В.* Обеспечение безопасности виртуальной инфраструктуры в государственных информационных системах (ГИС) // Информационно-телекоммуникационные системы и технологии: материалы Всероссийской научно-практической конференции. – М., 2014. – С. 92–93.

30. *Розенберг И.Н. Булгаков С.В.* Проектная модель информационной безопасности ГИС // Вестник Московского государственного областного университета. Серия: Естественные науки. – 2010. – № 2. – С. 113–115.

31. Enterprise Matrix: website. – URL: https://attack.mitre.org/matrices/enterprise/ (accessed: 01.06.2023).

32. Enterprise tactics: website. – URL: https://attack.mitre.org/tactics/enterprise/ (accessed: 01.06.2023).

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации. Область научных интересов – защита информации, комплексное обеспечение информационной безопасности. E-mail: sfo1@mail.ru

Звягинцева Полина Александровна, старший преподаватель кафедры информационной безопасности. Область научных интересов – защита информации. E-mail: polinasgugit@mail.ru

Плахотникова Елена Александровна, специалист-эксперт отдела Управления ФСТЭК России по Сибирскому федеральному округу. Область научных интересов – информационная безопасность. E-mail: plahotnikova.elena@mail.ru

DOI: 10.17212/2782-2230-2023-2-52-70

Examination of the information security threats model for information systems *

V.V. Selifanov[1], P.A. Zvyagintseva[2], E.A. Plahotnikova[3]

[1] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, senior lecturer of the Information security Department . E-mail: sfo1@mail.ru*
[2] *Novosibirsk State Technical University, 10 Plakhotnogo Street, Novosibirsk, 630108, Russian Federation, senior lecturer of the Information security Department. E-mail: polinasgugit@mail.ru*
[3] *The office of the Federal service for technical and export control in the Siberian Federal district, 41 Krasny Prospect, Novosibirsk, 630091, Russian Federation, specialist-expert. E-mail: plahotnikova.elena@mail.ru*

The basis of the work is the development of an automated software tool for the examination of information security threat models developed for various information systems that process data for compliance with the requirements of regulatory legal acts and regulatory methodological documentation initiated by the Decree of the Government, the FSS and the FSTEC of Russia.

Keywords: threat model, information system, threat model expertise, threats, information protection

REFERENCES

1. Federal Law of the Russian Federation dated July 27, 2006 No. 149 "On Information, Information Technologies and Information Protection". *Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the Legislation of the Russian Federation*, 2006, no. 31, art. 3448. (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).
3. Order of the FSTEC of Russia of February 11, 2013 N 17 "On approval of requirements for the protection of information not constituting state secrets contained in state information systems". (In Russian).
4. FSTEC of Russia. *Methodological document "Methodology for assessing threats to information security"*. Approved on February 5, 2021. (In Russian).
5. Decree of the Government of the Russian Federation of July 6, 2015 No. 676 "On the requirements for the procedure for the creation, development, commissioning, operation and decommissioning of state information systems and further stor-

* *Received 20 April 2023.*

age of information contained in their databases". *Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the Legislation of the Russian Federation*, 2015, no. 28, art. 4241. (In Russian).

6. *Metodika opredeleniya ugroz bezopasnosti informatsii* [Methodology for determining threats to information security]. Moscow, FSTEC Publ., 2021. 83 p.

7. FSTEC of Russia. *Methodological document "Security measures in state information systems"*. Approved on February 11, 2014. (In Russian).

8. Bank dannykh ugroz bezopasnosti informatsii [Data security threats database]. Website. Available at: www.bdu.fstec.ru (01.06.2023).

9. MITER ATT&CK: website. Available at: www.attack.mitre.org (accessed 01.06.2023).

10. GOST R 50922–2006. *Zashchita informatsii. Osnovnye terminy i opredeleniya* [State Standard R 50922–2006. Protection of information. Basic terms and definitions]. Moscow, Standartinform Publ., 2008. 9 p.

11. GOST R 56545–2015. *Zashchita informatsii. Uyazvimosti informatsionnykh sistem. Pravila opisaniya uyazvimostei* [State Standard R 56545–2015. Information protection. Vulnerabilities in information systems. Rules of vulnerabilities description]. Moscow, Standartinform Publ., 2018. 13 p.

12. GOST R 51624–2000. *Zashchita informatsii. Avtomatizirovannye sistemy v zashchishchennom ispolnenii. Obshchie trebovaniya* [State Standard R 51624–2000. Information security. Automated systems in a secure design. General requirements]. Moscow, Gosstandart Rossii Publ., 2001.

13. GOST 34.602–89. *Informatsionnaya tekhnologiya. Kompleks standartov na avtomatizirovannye sistemy. Tekhnicheskoe zadanie na sozdanie avtomatizirovannoi sistemy* [State Standard 34.602-8. Information technology. Set of standards for automated systems. Technical directions for automated system making]. Moscow, Standartinform Publ., 2009. 13 p.

14. Microsoft. Visual Studio: website. Available at: https://visualstudio.microsoft.com/ru/ (accessed 01.06.2023).

15. Laws, codes and normative-legal acts of the Russian Federation: website. (In Russian). Available at: https://legalacts.ru/doc/FZ-ob-informacii-informacionnyh-tehnologijah-i-o-zawite-informacii/ (accessed 01.06.2023).

16. Consultant Plus: website. (In Russian). Available at: http://www.consultant.ru (accessed 01.06.2023).

17. Techexpert: website. (In Russian). Available at: http://docs.cntd.ru (accessed 01.06.2023).

18. Federal Service for Technical and Export Control: website. Available at: https://fstec.ru (accessed 01.06.2023).

19. Microsoft. C# documentation. (In Russian). Available at: https://docs.microsoft.com/ru-ru/dotnet/csharp/ (accessed 01.06.2023).

20. Habr. About threat modeling. (In Russian). Available at: https://habr.com/ru/company/cloud4y/blog/350228/ (accessed 01.06.2023).

21. Kovaleva N.N., Kholodnaya E.V. Commentary on the Federal Law of July 27, 2006 No. 149-FZ "On Information, Information Technologies and Information Protection". *Rossiiskaya gazeta = Russian newspaper*, 2006, July 29, no. 165. (In Russian).

22. Stepanov V.A., Andreev N.D. Modelirovanie ugroz bezopasnosti informatsii po novoi metodike FSTEK, ispol'zuya sredstva avtomatizatsii [Modeling information security threats using the new FSTEC methodology using automation tools]. *Informatsionnye tekhnologii. Problemy i resheniya = Information Technology*, 2021, no. 4 (17), pp. 95–101. (In Russian).

23. Doroshenko I.E., Maksudov M.O., Selifanov V.V. Voprosy opisaniya vozmozhnykh stsenariev ugroz pri razrabotke modelei ugroz bezopasnosti informatsii [Issues of description of possible scenarios of threats in the development of models of information security threats]. *Interekspo Geo-Sibir' = Interexpo GEO-Siberia*, 2021, vol. 7, no. 1, pp. 16–21. (In Russian).

24. Starikovskaya N.A., Slepukhina Yu.V. Razrabotka modeli ugroz dlya gosudarstvennoi informatsionnoi sistemy [Development of a threat model for the state information system]. *Materialy Afanas'evskih chtenij = Materials Athanasian Readings*, 2022, no. 2 (39), pp. 36–41. (In Russian).

25. Tatarnikova T.M., Yagotinceva N.V. Model' obespecheniya informatsionnoi bezopasnosti GIS [Model of information security GIS]. *Nauchnyi al'manakh = Science Almanac*, 2016, no. 1-1 (15), pp. 521–523. EDN: VPSCAN.

26. Tatarnikova T.M., Yagotinceva N.V. Ugrozy informatsionnoi bezopasnosti GIS [Information security threats GIS]. *Regional'naya informatika i informatsionnaya bezopasnost'* [Regional informatics and information security]. St. Petersburg, 2016, iss. 2, pp. 137–142.

27. Prokushev Y.E., Ponomarenko S.V., Ponomarenko S.A. Modeling the processes of designing information security systems in state information systems. *Computational Nanotechnology*, 2021, vol. 8, iss. 1, pp. 26–37.

28. Borshcheva N.V. Osobennosti postroeniya modeli ugroz bezopasnosti informatsii dlya gosudarstvennykh informatsionnykh sistem [Features of building a model of information security threats for state information systems]. *Sovremennye problemy proektirovaniya, proizvodstva i ekspluatatsii radiotekhnicheskikh system* [Modern problems of design, production and operation of radio engineering systems]. Ul'yanovsk, 2019, pp. 163–166.

29. Kurnosov K.V. [Ensuring the security of virtual infrastructure in state information systems (GIS)]. *Informatsionno-telekommunikatsionnye sistemy i technologii* [Information and telecommunication systems and technologies]. Materials of

the All-Russian scientific and practical conference. Moscow, 2014, pp. 92–93. (In Russian).

30. Rozenberg I.N. Bulgakov S.V. Proektnaya model' informatsionnoi bezopasnosti GIS [Design model of information safety GIS]. *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Estestvennye nauki = Bulletin of the Moscow State Regional University. Series: Natural Sciences*, 2010, no. 2, pp. 113–115.

31. Enterprise Matrix: website. Available at: https://attack.mitre.org/matrices/enterprise/ (accessed 01.06.2023).

32. Enterprise tactics: website. Available at: https://attack.mitre.org/tactics/enterprise/ (accessed 01.06.2023).

Для цитирования:

Селифанов В.В., Звягинцева П.А., Плахотникова Е.А. Экспертиза модели угроз безопасности информации для информационных систем // Безопасность цифровых технологий. – 2023. – № 2 (109). – С. 52–70. – DOI: 10.17212/2782-2230-2023-2-52-70.

For citation:

Selifanov V.V., Zvyagintseva P.A., Plahotnikova E.A. Ekspertiza modeli ugroz bezopasnosti informatsii dlya informatsionnykh sistem [Examination of the information security threats model for information systems]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 2 (109), pp. 52–70. DOI: 10.17212/2782-2230-2023-2-52-70.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 2 (109). – 71–81

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 004 DOI: 10.17212/2782-2230-2023-2-71-81

ИСПОЛЬЗОВАНИЕ МЕТОДОЛОГИИ IDEF0 В РАЗРАБОТКЕ СИСТЕМЫ МОНИТОРИНГА*

Н.Ю. ЦИБЕРМАН[1], В.М. БЕЛОВ[2]

[1] *630087, Российская Федерация, г. Новосибирск, ул. Немировича-Данченко, 136, Новосибирский государственный технический университет, студент кафедры вычислительной техники. E-mail: nciberman@gmail.com*
[2] *630087, Российская Федерация, г. Новосибирск, ул. Немировича-Данченко, 136, Новосибирский государственный технический университет, доктор технических наук, профессор. E-mail: vmbelov@mail.ru*

Существует множество специализированных методологий, предназначенных для моделирования систем и бизнес-процессов. Одной из них является методология IDEF0, актуальность применения которой подтверждается высокой эффективностью использования и рационализации различных процессов, проходящих в сложных системах. В статье рассматривается методология IDEF0, а также ее преимущества и основные понятия. Описывается разработанная с помощью данной методологии функциональная модель системы мониторинга для нахождения уязвимостей в локальных сетях. Модель использовалась для представления процессов системы и их взаимодействия между собой в графическом виде, что позволило оптимально определить основные этапы разработки, локализовать слабые места системы еще на стадии планирования и улучшить понимание того, как должна работать система. В результате была составлена функциональная модель, состоящая из четырех уровней декомпозиции и шести схем.

Ключевые слова: функциональная модель, система мониторинга, IDEF0, моделирование функций, локальная сеть, мониторинг, агент мониторинга, графическая модель, планирование

1. МЕТОДОЛОГИЯ IDEF0

Стандарт IDEF0 был разработан в 1981 году в США департаментом Военно-воздушных сил для автоматизации промышленных предприятий.

IDEF0 (Integration Definition for Function Modeling) – это метод моделирования функций, который используется для анализа и проектирования систем.

* Статья получена 17 мая 2023 г.

Он представляет собой формальную методологию, которая позволяет описывать процессы и функции внутри системы, а также взаимосвязи между ними. Особенностью методологии является ее акцент на соподчиненность объектов. IDEF0 используется в инженерии, бизнес-анализе, управлении проектами и других областях деятельности, где требуется моделирование функций и процессов.

Основные преимущества использования модели.

Наглядность. Модель читаема для лиц, даже незнакомых с моделируемым проектом, и позволяет обнаружить «тонкие места» в проекте.

Простота и скорость создания модели. В сжатые сроки можно создать модель, которая поможет разобраться в том, что происходит в той или иной системе.

Отсутствие ошибок. Стандарт IDEF0 предполагает строгие рамки и правила. Нарушения стандарта становятся сразу заметны.

В основе методологии лежат четыре основных понятия.

Первым из них является понятие функционального блока, который олицетворяет собой некоторую функцию в рамках рассматриваемой системы.

Вторым понятием являются стрелки или дуги, которые соединяют блоки между собой. Направление стрелок имеет свое определенное значение:

- входящее (слева направо) – постановка определенной задачи;
- исходящее (справа налево) – вывод результата деятельности;
- управление (сверху вниз) – представление механизмов управления (инструкции, положения и пр.).
- механизмы (снизу вверх) – выполнение работы (сотрудники, клиенты).

Следующим понятием является декомпозиция – разбиение блока на составляющие его функции. Декомпозиция позволяет представить модель в виде иерархической структуры, что делает ее менее перегруженной.

Последним понятием является глоссарий. Для каждого элемента модели имеется набор соответствующих определений и ключевых слов, который дополняет графическое представление дополнительной информацией.

2. ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ СИСТЕМЫ МОНИТОРИНГА

Далее рассмотрим функциональную модель, которая использовалась при разработке системы, обеспечивающей мониторинг уязвимостей и слабых мест в локальных сетях. Основными функциями системы являются оповещение клиентов о наличии проблем на серверах и предоставление статистики по метрикам за определенный период времени.

Модель будет включать в себя описание основных компонентов системы мониторинга и процессов, выполняемых в рамках системы и связей между ними.

Мониторинг осуществляется следующим образом: на каждом из серверов находятся агенты, собирающие информацию о системе и передающие ее на главный сервер, который сохраняет полученные данные в базу данных. С помощью двух периодических задач в случае недоступности или выхода значений метрик сервера за установленные границы формируется оповещение, которое отображается на веб-странице. При появлении оповещения администраторы, соблюдая установленный SLA, в случае необходимости информируют клиентов и приступают к устранению проблемы. После устранения проблемы составляется краткий отчет и отправляется клиенту.

На первом уровне модели (рис. 1) в качестве основного блока выступает система мониторинга, на вход которой поступают сервера. В качестве управления используются конфигурация систем и SLA. Механизмами являются клиенты и администраторы, обслуживающие систему мониторинга. На выходе получаем отчет о решенной проблеме.

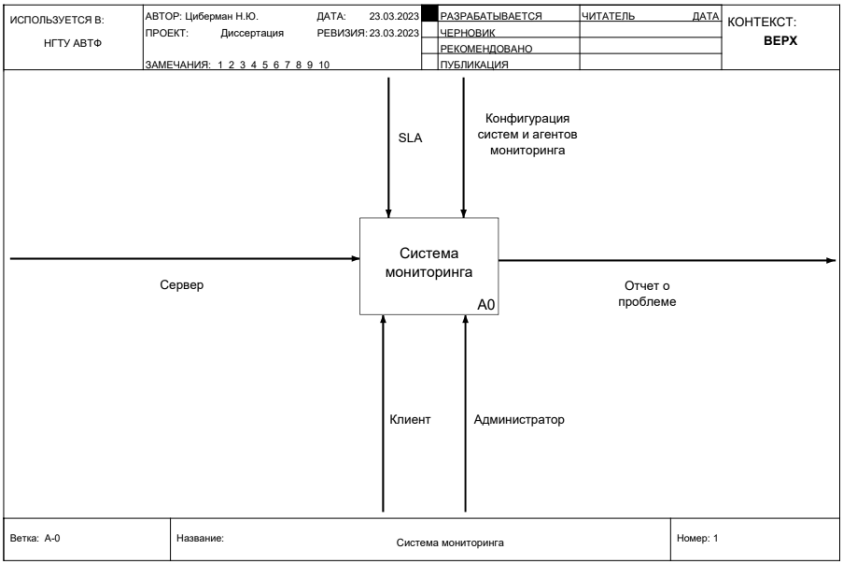

Рис. 1. Первый уровень модели

Fig. 1. The first level of the model

Первый уровень декомпозируется на три блока (рис. 2). В первом блоке выполняется настройка сервера для постановки его на мониторинг. Второй блок отвечает за мониторинг – получение и обработку метрик, создание оповещений и графиков. В последнем блоке описаны процессы решения инцидента.

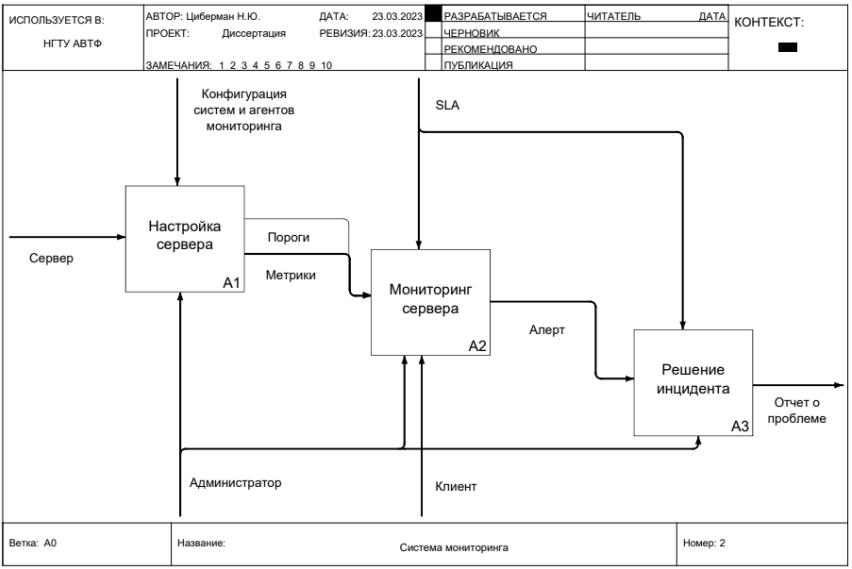

Рис. 2. Декомпозиция системы мониторинга.

Fig. 2. Decomposition of the monitoring system.

В декомпозиции блока A1 находятся функции настройки сервера, которые выполняет администратор (рис. 3). Первый блок – это функция добавления сервера в систему через веб-интерфейс, где указывается имя сервера и IP-адрес. После добавления серверу присваивается уникальный идентификатор и токен, которые используются в конфигурации агента мониторинга. После настройки и запуска агента администратор устанавливает пороги для метрик, указанные клиентом либо на основе конфигурации сервера.

После того как значения метрик и порогов попадают на сервер, они сохраняются в базу данных. Затем значения используются для создания графиков и обрабатываются в периодических задачах, которые создают оповещения (рис. 4).

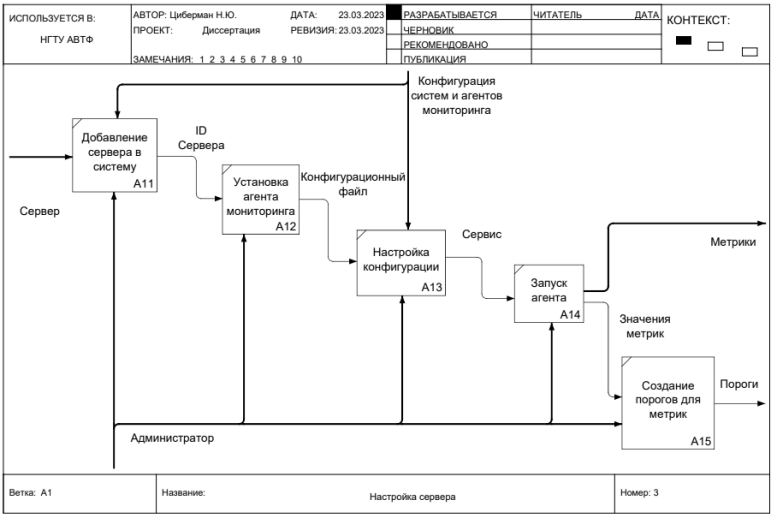

Рис. 3. Декомпозиция настройки сервера

Fig. 3. Decomposition of the server setup

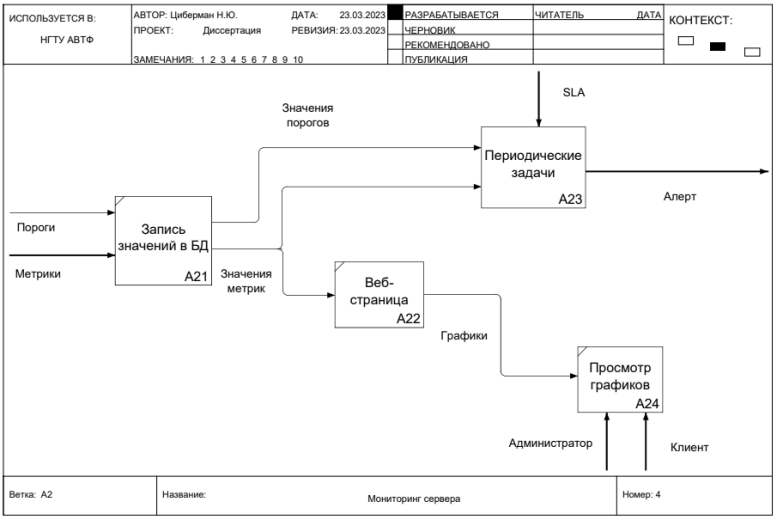

Рис. 4. Декомпозиция блока A2

Fig. 4. Block A2 decomposition

В периодических задачах выполняется проверка выхода значений за пороги и разница текущего времени и времени последних полученных значений метрик (рис. 5). На основе проверок создается оповещение на веб-странице, которое должен принять администратор.

Рис. 5. Декомпозиция периодических задач

Fig. 5. Decomposition of periodic tasks

После принятия оповещения администратор сообщает о проблеме клиенту и приступает к ее устранению, соблюдая установленный SLA (рис. 6).

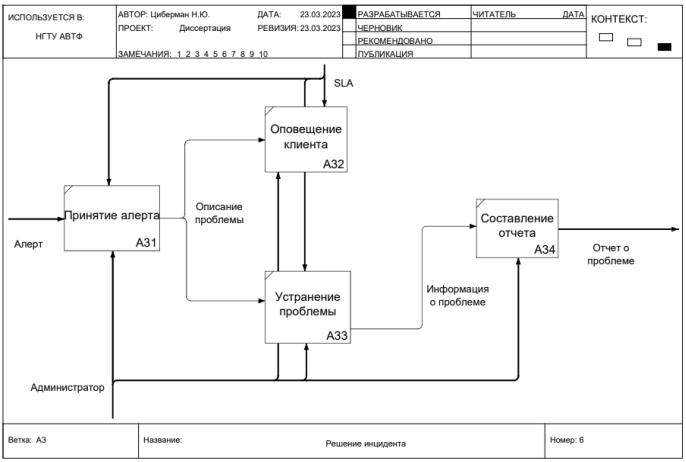

Рис. 6. Декомпозиция решения инцидента

Fig. 6. Decomposition of incident resolution

ЗАКЛЮЧЕНИЕ

Таким образом, методология IDEF0 разбивает сложную систему на более простые компоненты с описанием их взаимодействия. Методология позволяет визуализировать все этапы функциональных процессов проекта, а также улучшает понимание работы системы и идентификацию проблемных мест проектирования. Благодаря использованию IDEF0 разработчики могут получить более качественный результат и сократить время на разработку программного обеспечения.

СПИСОК ЛИТЕРАТУРЫ

1. *Чемисов С.Б.* Применение методологии IDEF0 с целью моделирования бизнес-процессов на предприятии // Проблемы современной экономики. – 2009. – № 4. – С. 446–449.

2. *Заплатников П.В.* Применение нотации IDEF0 для оптимизации бизнес-процессов производственного предприятия // Вестник науки. – 2020. – № 6. – С. 158–163.

3. *Андросюк А.Б.* IDEF0 – инструмент, необходимый для совершенствования бизнес-процессов // Вектор экономики. – 2019. – № 1. – С. 86.

4. *Александров Д.В.* Формализация и развитие методологии IDEF0 для системного моделирования организаций // Горный информационно-аналитический бюллетень. – 2008. – № 2. – С. 76–81.

5. *Шилкина А.Т.* Моделирование процесса формирования системы постоянного улучшения на основе методологии функционального моделирования IDEF0 // Вестник Волжского университета им. В.Н. Татищева. – 2001. – № 2. – С. 222–227.

6. *Дворников А.* IDEF0 как инструмент моделирования процессов // Авант Партнер. – 2005. – № 22. – С. 79.

7. *Владымцев Н.В., Извольская И.В.* Принцип моделирования бизнес-процессов в стандарте IDEF0 // Экономический анализ: теория и практика. – 2008. – № 9. – С. 11–17.

8. *Плаксина И.В., Борисова Д.В.* Особенности проектирования сайта с использованием методологии IDEF0 // Инновационная наука. – 2019. – № 7–8. – С. 32–36.

9. *Карпычев В.Ю.* Функциональное моделирование (IDEF0) как метод исследования блокчейн-технологии // Труды НГТУ им. Р.Е. Алексеева. – 2018. – № 4. – С. 22–32.

10. *Топольник В.Г., Щербакова Д.В.* Моделирование средствами IDEF0 бизнес-процесса предоставления фитнес-услуг // Форум молодых ученых. – 2019. – № 8. – С. 310–317.

11. Automation of strategy using IDEF0 – A proof of concept / G.R. Waissi, M. Demir, J.E. Humble, B. Lev // Operations Research Perspectives. – 2015. – Vol. 2. – P. 106–113.

12. *Spanidis P.-M., Pavloudakis F., Roumpos C.* Introducing the IDEF0 methodology in the strategic planning of projects for reclamation and repurposing of surface mines // Materials Proceedings. – 2021. – Vol. 5. – P. 26. – DOI: 10.3390/materproc2021005026.

13. Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования: рекомендации по стандартизации Р 50.1.028–2001. – М.: Изд-во стандартов, 2002.

14. *Черемных С.В., Семенов И.О., Ручкин В.С.* Структурный анализ систем: IDEF-технологии. – М.: Финансы и статистика, 2001. – 207 с.

15. *Кинзябулатов Р.* IDEF0. Знакомство с нотацией и пример использования. – URL: https://trinion.org/blog/idef0-znakomstvo-s-notaciey-i-primer-ispolzovaniya (дата обращения: 02.06.2023).

Циберман Николай Юрьевич, лаборант кафедры вычислительной техники Новосибирского государственного технического университета. E-mail: nciberman@gmail.com

Белов Виктор Матвеевич, доктор технических наук, профессор Новосибирского государственного технического университета, E-mail: vmbelov@mail.ru

DOI: 10.17212/2782-2230-2023-2-71-81

Using the IDEF0 methodology in monitoring system development*

N.Y. Tsiberman[1], V.M. Belov[2]

[1] *Novosibirsk State Technical University, 136 Nemirovicha-Danchenko Avenue, Novosibirsk, 630087, Russian Federation, student of Computer Engineering Department. E-mail: nciberman@gmail.com*
[2] *Novosibirsk State Technical University, 136 Nemirovicha-Danchenko Avenue, Novosibirsk, 630087, Russian Federation, Doctor of Technical Sciences, Professor E-mail: vmbelov@mail.ru*

There are many specialized methodologies for modeling systems and business processes. One of them is the methodology IDEF0, the relevance of which is confirmed by high efficiency of the use and rationalization of various processes taking place in complex systems. This article discusses the methodology of IDEF0, as well as its advantages and basic concepts. In the second chapter of the paper, a functional model of a monitoring system for finding vulnerabilities in local networks, developed with the help of this methodology, is described. The model was used to represent the system processes and their interaction with each other graphically, which allowed us to optimally determine the main development steps, localize the weaknesses of the system at the planning stage and improve the understanding of how the system should work. As a result, a functional model consisting of four decomposition levels and six schemes was made.

Keywords: functional model, monitoring system, IDEF0, function modeling, local network, monitoring, monitoring agent, graphical model, planning

REFERENCES

1. Chemisov S.B. Primenenie metodologii IDEF0 s tsel'yu modelirovaniya biznes-protsessov na predpriyatii [Application of the IDEF0 methodology for modeling business processes at the enterprise]. *Problemy sovremennoi ekonomiki = Problems of Modern Economics*, 2009, no. 4, pp. 446–449.

2. Zaplatnikov P.V. Primenenie notatsii IDEF0 dlya optimizatsii biznes-protsessov proizvodstvennogo predpriyatiya [Application of IDEF0 notation for optimization of business processes of a production enterprise]. *Vestnik nauki*, 2020, no. 6, pp. 158–163. (In Russian).

3. Androsyuk A.B. IDEF0 – instrument, neobkhodimyi dlya sovershenstvovaniya biznes-protsessov [IDEF0 – a tool required for improvement of business processes]. *Vektor ekonomiki*, 2019, no. 1, p. 86. (In Russian).

4. Aleksandrov D.V. Formalizatsiya i razvitie metodologii IDEF0 dlya sistemnogo modelirovaniya organizatsii [Formalization and development of the IDEF0

* *Received 10 May 2023.*

methodology for system modeling of organizations]. *Gornyi informatsionno-analiticheskii byulleten'= Mining informational and analytical bulletin*, 2008, no. 2, pp. 76–81.

5. Shilkina A.T. Modelirovanie protsessa formirovaniya sistemy postoyannogo uluchsheniya na osnove metodologii funktsional'nogo modelirovaniya IDEF0 [Modeling of process of formation of system of continuous improvement on the basis of methodology of functional modeling IDEF0]. *Vestnik Volzhskogo universiteta im. V.N. Tatishcheva = Vestnik of Volzhsky University after V.N. Tatishchev*, 2001, no. 2, pp. 222–227.

6. Dvornikov A. IDEF0 kak instrument modelirovaniya protsessov [IDEF0 as a process modeling tool]. *Avant Partner*, 2005, no. 22, p. 79. (In Russian).

7. Vladymtsev N.V., Izvol'skaya I.V. Printsip modelirovaniya biznes-protsessov v standarte IDEF0 [Principle of modeling of business-processes in standard IDEF0]. *Ekonomicheskii analiz: teoriya i praktika = Economic Analysis: Theory and Practice*, 2008, no. 9, pp. 11–17.

8. Plaksina I.V., Borisova D.V. Osobennosti proektirovaniya saita s ispol'zovaniem metodologii IDEF0 [Peculiarities of site design using the IDEF0 methodology]. *Innovatsionnaya nauka = Innovation Science*, 2019, no. 7–8, pp. 32–36.

9. Karpychev V.Yu. Funktsional'noe modelirovanie (IDEF0) kak metod issledovaniya blokchein-tekhnologii [Functional modeling (IDEF0) as a method of research on blockchain technology]. *Trudy NGTU im. R.E. Alekseeva = Transactions of NNSTU n.a. R.E. Alekseev*, 2018, no. 4, pp. 22–32.

10. Topolnik V.G., Shcherbakova D.V. Modelirovanie sredstvami IDEF0 biznes-protsessa predostavleniya fitnes-uslug [Modeling tools the IDEF0 business process of providing fitness services]. *Forum molodykh uchenykh*, 2019, no. 8, pp. 310–317. (In Russian).

11. Waissi G.R., Demir M., Humble J.E., Lev B. Automation of strategy using IDEF0 – A proof of concept. *Operations Research Perspectives*, 2015, vol. 2, pp. 106–113.

12. Spanidis P.-M., Pavloudakis F., Roumpos C. Introducing the IDEF0 Methodology in the Strategic Planning of Projects for Reclamation and Repurposing of Surface Mines. *Materials proceedings*, 2021, vol. 5, P. 26. DOI: 10.3390/materproc2021005026.

13. *Continuous acquisition and life-cycle support. Methodology of functional modeling*. Recommendations for standardization P 50.1.028–2001. Moscow, Standards Publ., 2002.

14. Cheremnykh S.V., Semenov I.O., Ruchkin V.S. *Strukturnyi analiz sistem: IDEF-tekhnologii* [Structural analysis of systems: IDEF-technologies]. Moscow, Finansy i statistika Publ., 2001. 207 p.

15. Kinzyabulatov R. IDEF0. Znakomstvo s notatsiei i primer ispol'zovaniya [IDEF0. Acquaintance with notation and example of use]. Available at: https://trinion.org/blog/idef0-znakomstvo-s-notaciey-i-primer-ispolzovaniya (accessed 20.05.2023).

Для цитирования:

Циберман Н.Ю., Белов В.М. Использование методологии IDEF0 в разработке системы мониторинга // Безопасность цифровых технологий. – 2023. – № 2 (109). – С. 71–81. – DOI: 10.17212/2782-2230-2023-2-71-81.

For citation:

Tsiberman N.Yu., Belov V.M. Ispol'zovanie metodologii IDEF0 v razrabotke sistemy monitoringa [Using the IDEF0 methodology in monitoring system development]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 2 (109), pp. 71–81. DOI: 10.17212/2782-2230-2023-2-71-81.

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.