

**УЧРЕДИТЕЛИ**

**ФГАОУ ВО «ЮЖНО-УРАЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ООО «ЮЖНО-УРАЛЬСКИЙ
ЮРИДИЧЕСКИЙ ВЕСТНИК»**

ПРЕДСЕДАТЕЛЬ**РЕДАКЦИОННОГО СОВЕТА****ЧУВАРДИН О. П.,**

руководитель Управления
Федеральной службы
по техническому и экспортному
контролю России по Уральскому
федеральному округу

ГЛАВНЫЙ РЕДАКТОР**СОКОЛОВ А. Н.,**

к. т. н., доцент, зав. кафедрой
«Защита информации»,
Южно-Уральский государственный
университет (национальный
исследовательский университет)
(г. Челябинск)

ВЫПУСКАЮЩИЙ**РЕДАКТОР****СОГРИН Е. К.****ВЁРСТКА****ШРЕЙБЕР А. Е.****КОРРЕКТОР****ФЁДОРОВ В. С.****РЕДАКЦИОННЫЙ
СОВЕТ:****БАРАНКОВА И. И.,**

д. т. н., профессор, зав. кафедрой
«Информатика и информацион-
ная безопасность», Магнитогор-
ский государственный техниче-
ский университет им. Г. И. Носова
(г. Магнитогорск);

ВАСИЛЬЕВ В. И.,

д. т. н., профессор, профессор
кафедры «Вычислительная
техника и защита информации»,
Уфимский государственный
авиационный технический
университет (г. Уфа);

ВОЙТОВИЧ Н. И.,

д. т. н., профессор, зав. кафедрой
«Конструирование и производ-
ство радиоаппаратуры»,
Южно-Уральский государственный
университет (национальный
исследовательский университет)
(г. Челябинск);

ГАЙДАМАКИН Н. А.,

д.т.н., профессор, профессор
Учебно-научного центра «Инфор-
мационная безопасность»,
Уральский федеральный универ-
ситет им. первого президента
России Б.Н. Ельцина (г. Екатеринбу-
рг);

ДИК Д. И.,

к. т. н., доцент кафедры
«Безопасность информацион-
ных и автоматизированных
систем», Курганский государ-
ственный университет
(г. Курган);

ЗАХАРОВ А. А.,

д.т.н., профессор, зав. базовой
кафедрой «Безопасность
информационных технологий
умного города», Тюменский
государственный университет
(г. Тюмень);

ЗЫРЯНОВА Т. Ю.,

к. т. н., доцент, зав. кафедрой
«Информационные технологии
и защита информации»,
Уральский государственный
университет путей сообщения
(г. Екатеринбург);

МЕЛЬНИКОВ А. В.,

д. т. н., профессор, директор
Югорского научно-исследова-
тельского института информа-
ционных технологий
(г. Ханты-Мансийск);

МИНБАЛЕЕВ А. В.,

д.ю.н., доцент, ведущий научный
сотрудник сектора «Информа-
ционное право и международ-
ная информационная безопас-
ность», Институт государства и
права РАН (г. Москва);

ПОРШНЕВ С. В.,

д.т.н., профессор, директор
Учебно-научного центра
«Информационная безопас-
ность», Уральский федеральный
университет им. первого
президента России
Б.Н. Ельцина (г. Екатеринбург);

РУЧАЙ А.Н.,

к. ф.-м. н., доцент, заведующий
кафедрой «Компьютерная
безопасность и прикладная
алгебра», Челябинский государ-
ственный университет
(г. Челябинск);

ХОРЕВ А. А.,

д. т. н., профессор, зав. кафе-
дрой «Информационная безопас-
ность», Национальный исследо-
вательский университет
«Московский институт
электронной техники»
(г. Москва, г. Зеленоград);

ШАБУНИН С. Н.,

д.т.н., профессор, зав. кафедрой
«Радиоэлектроника и телеком-
муникации», Уральский
федеральный университет
им. первого президента России
Б.Н. Ельцина (г. Екатеринбург).

**Подписной индекс 73852
в каталоге «Почта России»**

Журнал зарегистрирован Федераль-
ной службой по надзору в сфере
связи, информационных технологий
и массовых коммуникаций.

Свидетельство
ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский
юридический вестник»**

Адрес редакции и издателя: Россия,
454080, г. Челябинск, пр. Ленина, д. 76.
Тел./факс (351) 267-97-01.

Электронная версия журнала
в Интернете:
**www.info-secur.ru,
e-mail: urvest@mail.ru**

Journal of the Ural Federal District.

Information security

№ 3(37) / 2020



ISSN 2225-5435

FOUNDER

**SOUTH URAL STATE UNIVERSITY
SOUTH URAL LEGAL NEWSLETTER**

CHAIRMAN OF THE EDITORIAL BOARD

CHUVARDIN O. P.,

Head of Department Federal Service
for Technical and Export Control of
Russia for the Urals Federal District

CHIEF EDITOR

SOKOLOV A.N.,

Ph.D., Associate Professor, Head
of Department "Information
Protection", South Ural State
University (National Research
University) (Chelyabinsk city)

PRODUCING EDITOR

SOGRIN E. K.

LAYOUT

SHRABER A. E.

PROOFREADING

FEDOROV V. S.

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal
service in the field of communication,
information technology and mass
communications.

Certificate
PI No. ΦC77-65765 dd. 05/20/2016

**Publisher: ООО «South Ural Legal
Newsletter»**

Editorial and publisher address: Russia,
454080, Chelyabinsk, Lenin Avenue, 76
Phone / fax (351) 267-97-01.

**Electronic version of the magazine
in the Internet:**

**www.info-secur.ru,
e-mail: urvest@mail.ru**

EDITORIAL COUNCIL:

BARANKOVA I. I.,

Doctor of Technical Sciences,
Professor, Head of Department
"Informatics and Information
Security", Magnitogorsk State
Technical University named after
G.I. Nosova (Magnitogorsk city);

VASILYEV V. I.,

Doctor of Technical Sciences,
Professor, Professor of the
Department "Computer Science and
Information Protection", Ufa State
Aviation Technical University
(Ufa city);

VOITOVICH N. I.,

Doctor of Technical Sciences,
Professor, Head of Department
"Design and production of radio
equipment", South Ural State
University (National Research
University) (Chelyabinsk city);

GAYDAMAKIN N. A.,

Doctor of Technical Sciences,
Professor, Professor of the
Information Security Training and
Research Center of the Ural Federal
University named after the first
President of Russia B.N.Yeltsin
(Ekaterinburg city);

DIK D. I.,

Ph.D., Associate Professor of
Department "Security of information
and automated systems", Kurgan
State University (Kurgan city);

ZAHAROV A. A.,

Doctor of Technical Sciences,
Professor, Head Basic Department of
"Security information technologies
smart city", Tyumen State University
(Tyumen city);

ZYRYANOVA T. Y.,

Ph.D., Associate Professor, Head of
Department "Information
Technologies and Information
Protection", Ural State
University ways of communication
(Ekaterinburg city);

MELNIKOV A. V.,

Doctor of Technical Sciences,
Professor, Director Ugra Research
Institute of Information Technologies
(Khanty-Mansiysk city);

MINBALEEV A. V.,

Doctor of Law, Associate Professor,
Leading Researcher of the
"Information Law and International
Sector Information Security",
Institute of State and Law Russian
Academy of Sciences (Moscow city);

PORSHNEV S. V.,

Doctor of Technical Sciences,
Professor, Director of the Training
and Scientific Center "Information
Security", Ural Federal University
named after the first President of
Russia B.N.Yeltsin
(Ekaterinburg city);

RUCHAY A. N.,

Ph.D., Associate Professor, Head of
the Department "Computer Security
and Applied Algebra", Chelyabinsk
State University (Chelyabinsk city);

HOREV A. A.,

Doctor of Technical Sciences,
Professor, Head of Department of
"Information Security", National
Research University "Moscow
Institute of Electronic Technology"
(Moscow, the city of Zelenograd);

SHABUNIN S. N.,

Doctor of Technical Sciences,
Professor, Head of Department
"Radioelectronics and
Telecommunications", Ural Federal
University named after the first
President of Russia B.N.Yeltsin
(Ekaterinburg city).

В НОМЕРЕ

ИССЛЕДОВАНИЕ И ПРОЕКТИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ

**ВОЙТОВИЧ Н. И., ЕРШОВ А. В.,
ЖДАНОВ Б. В., ЮНГАЙТИС Е. М.**

Поведение информационного параметра
глиссадного радиомаяка системы посадки
воздушных судов в широком секторе углов
места. 5

ПЛОХОВ С. Н., ШАБУНИН С. Н.

Влияние взаимодействия элементов
антенно-фидерного тракта радиолокатора
на шумовые характеристики канала
приема. 20

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

КУЦ Д. В., ПОРШНЕВ С. В.

Особенности применения полномочной
модели разграничения доступа
в современных средствах защиты
информации от несанкционированного
доступа 27

РУЧАЙ А. Н.

Разработка избирательной
мультиметрической аутентификации .. 34

МЕТОДЫ АНАЛИЗА ДАННЫХ

ДУХАН Е. И., ЗАХАРКИН Г. Ф., ДУХАН А. Е.

Методика обучения нейронных сетей,
используемых в блоке принятия решения
сигнализационных средств
обнаружения 42

ЯПАРОВА Н. М., ГАВРИЛОВА Т. П.

Численный метод определения
температурного поля линейного объекта
при внешнем тепловом воздействии 49

ОРГАНИЗАЦИОННО- ТЕХНИЧЕСКАЯ И ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

АНФИНОГЕНОВ М. В., АНТЯСОВ И. С.

Эволюция систем защиты информации
в видеоиграх. 59

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

**РАГОЗИН А. Н., ПОРТНОВ А. В.,
ЛЫСОВ С. С., ПРЫТКОВ Н. С.**

Формирование высокоинформативного
цифрового образа сигнала
автоматизированной системы управления
с использованием технологий время-
частотного представления и двумерной
цифровой фильтрации 69

ГРУЗДЕВА Л. М.

Исследование проблем защиты объектов
транспортной инфраструктуры от угроз
хищения информации 81

RESEARCH AND DESIGN OF TECHNICAL FACILITIES

**VOYTOVICH N. I., ERSHOV A. V.,
ZHDANOV B. V., IUNGAITIS E. M.**

Behavior of the information parameter
of the glide path beacon of the landing system
in a wide sector of angles 5

PLOHOV S. N., SHABUNIN S. N.

Influence of interaction between elements
of the radar antenna-feeder network
on the noise characteristics of the reception
channel.....20

INFORMATION TECHNOLOGY AND COMPUTER SECURITY

KUTS D. V., PORSHNEV S. V.

The features of mandatory access control
model in modern unauthorized access data
protection tools.....27

RUCHAY A. N.

Development of new elective multibiometric
authentication34

METHODS OF DATA ANALYSIS

**DUKHAN E. I., ZAKHARKIN G. F.,
DUKHAN A. E.**

Training methods for neural networks used
in the decision-making block of signaling
detection tools.....42

YAPAROVA N. M., GAVRILOVA T. P.

Numerical method for determining
temperature field of a linear object under
external thermal influence49

ORGANIZATIONAL, TECHNICAL AND LEGAL PROTECTION OF INFORMATION

ANFINOGENOV M. V., ANTYASOV I. S.

Evolution of information security systems
in video games59

TOPICAL PROBLEMS OF CYBERSECURITY

**RAGOZIN A. N., PORTNOV A. V., LYSOV S. S.,
PRYTKOV N. S.**

Formation of a highly informative digital signal
image of an automated control system
using time-frequency representation
and two-dimensional digital filtering
technologies.....69

GRUZDEVA L. M.

Research of problems of protection of transport
infrastructure objects from threats
of information theft81



ПОВЕДЕНИЕ ИНФОРМАЦИОННОГО ПАРАМЕТРА ГЛИССАДНОГО РАДИОМАЯКА СИСТЕМЫ ПОСАДКИ ВОЗДУШНЫХ СУДОВ В ШИРОКОМ СЕКТОРЕ УГЛОВ МЕСТА

Статья посвящена проблеме защиты информации, формируемой глиссадным радиомаяком формата ГРМГ для обеспечения инструментального захода воздушных судов на посадку. Для обеспечения безопасного захода радиомаячная система посадки формирует в пространстве траекторию снижения – глиссаду. Целостность системы посадки призвана обеспечить развитая многоуровневая система контроля путём непрерывного контроля положения заданной глиссады и крутизны индицируемого параметра глиссады. Однако, при летных испытаниях глиссадного радиомаяка (ГРМ) иногда выявляют ложную глиссаду в зоне действия системы посадки, которая естественно нарушает ее целостность. В статье показана причина этого явления – нарушение кратности высот подвеса излучающих элементов антенной решётки ГРМ. Приведены данные летных измерений зоны глиссады на аэродроме в предгорной местности. Экспериментальные результаты подтверждают найденные теоретические закономерности в поведении информационного параметра глиссадного радиомаяка в широком секторе углов. Предложены рекомендации для сохранения целостности системы посадки.

Ключевые слова: ГРМ, целостность, информационный параметр ГРМ, угол глиссады, ложная глиссада.

BEHAVIOR OF THE INFORMATION PARAMETER OF THE GLIDE PATH BEACON OF THE LANDING SYSTEM IN A WIDE SECTOR OF ANGLES

The article is devoted to the problem of information protection generated by a glide path beacon of the PRMG format for providing instrumental approach of aircraft for landing. To ensure a safe approach, the radio beacon landing system forms a descent trajectory in space - a glide path. A developed multilevel control system is designed to ensure the integrity of the landing system by continuous monitoring of the position of a given glide path and the steepness of the indicated glide path parameter. However, during flight tests of a glide path beacon (GPB), a false glide path is sometimes detected in the area of the landing system, which naturally violates its integrity. The article shows the reason for this phenomenon - a violation of the multiplicity of the heights of the suspension of the radiating elements of the GPB antenna array. Flight measurements data of the glide path zone at the airfield in the foothills are given. The experimental results confirm the theoretically found regularities in the behavior of the information parameter of the glide path beacon in a wide sector of angles. Recommendations are proposed for maintaining the integrity of the landing system

Keywords: *Glide Path Beacon, integrity, Glide Path Beacon information parameter, glide path angle, false glide path.*

Статистика аварий, поломок самолетов и катастроф в авиации говорит о том, что около 60% авиационных происшествий происходит при заходе на посадку и посадке самолета [1]. Причиной авиационных происшествий может быть человеческий фактор, неблагоприятные погодные условия или технические проблемы с самолетом либо проблемы с информацией, формируемой радиомаячной системой посадки. Пилоту принять правильное решение в нештатной ситуации, когда, что-то пошло не так - чрезвычайно сложно, у него стрессовое состояние, дефицит времени и ограниченная показаниями бортового оборудования информация.

На тридцать третьей Ассамблеи ИКАО была названа главная причина всех авиационных происшествий при заходе на посадку и посадке: «Неспособность распознать экипажем воздушного судна необходимости ухода на второй круг и невыполнение этого маневра».

Естественно стремление разработчиков [2] и персонала, эксплуатирующего радиомаячные системы посадки воздушных судов, обеспечить пилота или автопилот безопасной информацией о траектории захода на посадку.

В глиссадных радиомаяках «нулевой зоны» [3, 4] применена двухэлементная антенная решетка излучающих элементов (антенн), разнесенных по высоте. В настоящей статье представлен анализ влияния ошибки в установке нижней антенны на поведение зоны глиссады. Анализ предшествует подробное изложение принципа работы глиссадного радиомаяка формата ПРМГ [3, 4]. Это сделано потому, что в известных литературных источниках и методической литературе [5-8] нет такого материала. Вначале выполнен анализ параметров ГРМ, как это обычно делается, в предположении идеальной проводимости подстилающей поверхности. Предположение идеальной проводимости позволя-

ет оперировать простыми соотношениями, которые, тем не менее, дают высокую точность в расчете основных параметров ГРМ в реальной ситуации.

Затем, выполнен анализ с учетом того, что подстилающая поверхность представляет собой границу раздела двух сред: воздух-почва. Предположено, что в случае реальной подстилающей поверхности (во втором случае) нижняя антенна ГРМ смещена относительно номинальной высоты вверх на величину, равную длине волны. Исследовано поведение зоны в этом случае. Приведены данные летных измерений зоны глиссады на аэродроме в предгорной местности. Эксперименталь-

ходом, подстроечный фазовращатель, первую и вторую антенны. Выходы первого и второго генераторов прямоугольных колебаний соединены с сигнальными входами переключателя. Выход третьего генератора прямоугольных колебаний соединен с параллельно включенными управляющим входом переключателя и с управляющим входом дискретного управляемого фазовращателя. Первый выход регулируемого делителя последовательно соединен с подстроечным фазовращателем и первой (нижней) антенной. Второй выход соединен с дискретным управляемым фазовращателем, выход которого соединен со второй антенной.

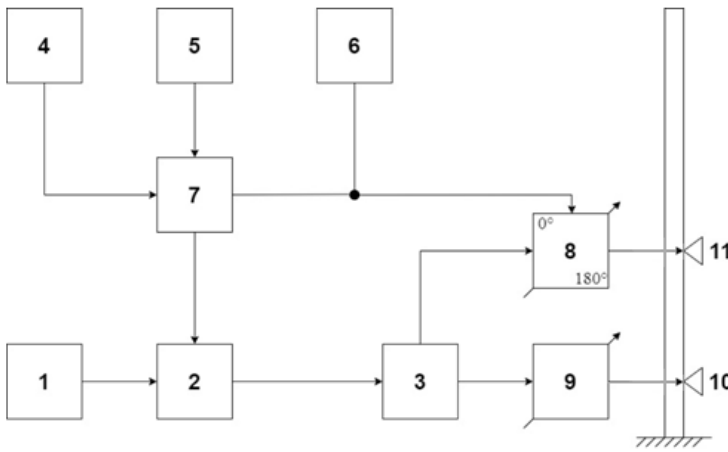


Рис.1. Структурная схема глиссадного радиомаяка формата ПРМГ

1– генератор высокочастотных колебаний, 2– ключ, 3– регулируемый делитель мощности, 4 – первый генератор прямоугольных колебаний, 5– второй генератор прямоугольных колебаний, 6 – третий генератор прямоугольных колебаний, 7–переключатель, 8–дискретный управляемый фазовращатель, 9–подстроечный фазовращатель, 10–первая антенна, 11– вторая антенна

ные результаты подтверждают закономерности в поведении информационного параметра глиссадного радиомаяка в широком секторе углов. В заключение дана рекомендация по установке нижней антенны.

Принцип работы глиссадного радиомаяка формата ПРМГ

Структурная схема ГРМ формата ПРМГ.

ГРМ (рис.1) содержит последовательно соединенные генератор высокочастотных колебаний, ключ и регулируемый делитель мощности на два направления, первый, второй и третий генераторы прямоугольных колебаний, переключатель с первым и вторым сигнальными входами, управляющим входом и выходом, дискретный управляемый фазовращатель с двумя фазовыми состояниями, отличающимися друг от друга на 180° , с сигнальным входом, управляющим входом и вы-

соты подвеса относительно поверхности Земли h_1 и h_2 первой и второй антенн равны $h_1 = \frac{\lambda}{4 \sin \theta_{21}}$ и $h_2 = \frac{\lambda}{2 \sin \theta_{21}}$, где λ – длина волны, θ_{21} – угол глиссады. В результате излучения сигнала первой (второй) антенной в пространстве формируется диаграмма направленности $F_1(\theta)$, $(F_2(\theta))$, (рис.2).

Формирование навигационной информации

ГРМ работает следующим образом (рис.2). Гармонические колебания с несущей частотой ω от высокочастотного генератора поступают на сигнальный вход первого ключа, на управляющий вход которого поступают две чередующиеся последовательности прямоугольных колебаний: с частотой 2100 Гц с выхода первого генератора прямоугольных колебаний и с частотой 1300 Гц с выхода

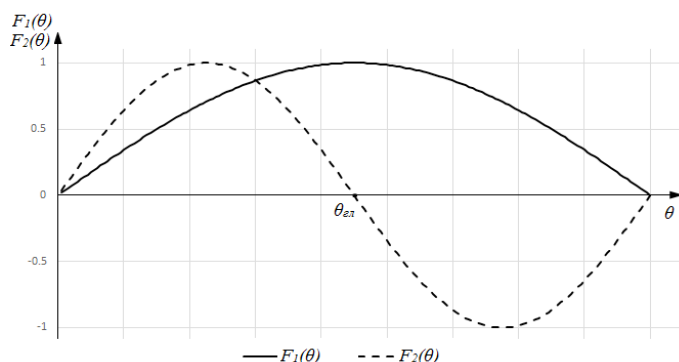


Рис.2. Амплитудные диаграммы направленности первой (нижней) $F_1(\theta)$ и второй (верхней) $F_2(\theta)$ антенн

второго генератора прямоугольных колебаний. Смена прохождения колебаний с частотами 2100 Гц и 1300 Гц осуществляется под управлением третьего генератора с частотой 12,5 Гц, сигналы которого одновременно поступают на управляющие входы переключателя и дискретного управляемого фазовращателя. В течение одного полупериода коммутации (в течение 0,04 сек.) через переключатель следует периодический сигнал прямоугольной формы, длительность импульса и длительность паузы которого в периоде равны друг другу («меандр»), с частотой 2100 Гц, а течение второго полупериода коммутации (в течение последующих 0,04 сек.) следует сигнал в форме «меандр» с частотой 1300 Гц.

гулируемого делителя сигнал поступает на дискретный управляемый фазовращатель, с выхода которого поступает на вторую антенну. С выхода генератора третьего генератора управляющие сигналы одновременно поступают и на переключатель, и на управляющий вход дискретного управляемого фазовращателя. Прохождение сигналов с частотой «меандра» 2100 Гц выполняется в течение одного полупериода колебания генератора с частотой 12,5 Гц. По окончании первого полупериода скачкообразно изменяется на половину длины волны электрическая длина пути дискретного управляемого фазовращателя для прохождения высокочастотного сигнала, модулированного с частотой «меандра» 1300 Гц.

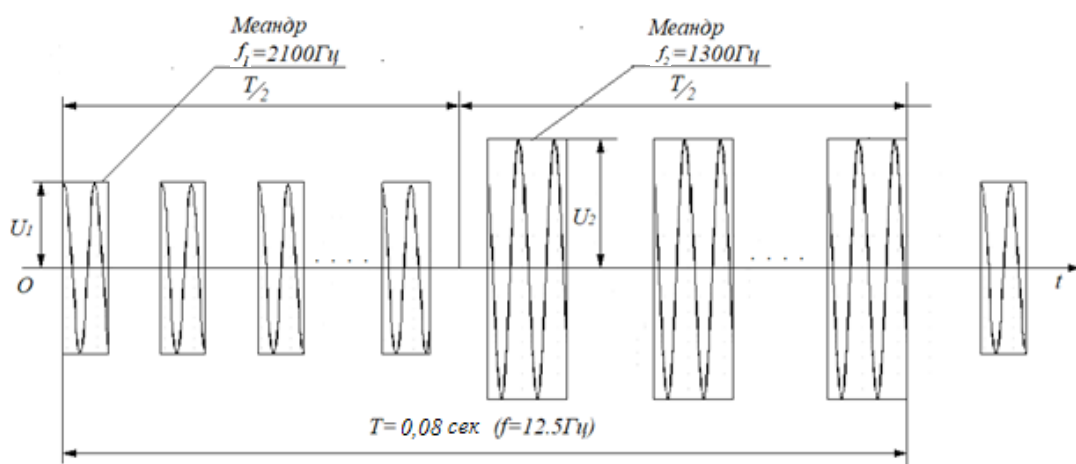


Рис. 3. Огибающая сигнала ПРМГ

Высокочастотный сигнал, модулированный последовательно сигналами в форме «меандр» с частотой 2100 Гц и 1300 Гц (рис.3), с выхода первого ключа поступает на вход регулируемого делителя. С первого выхода регулируемого делителя сигнал поступает через подстроечный фазовращатель на первую (нижнюю) антенну. Со второго выхода ре-

В каждый из полупериодов колебания с частотой 12,5 Гц высокочастотные колебания излучаются и первой и второй антеннами. В первом полупериоде обе антенны излучают синфазные высокочастотные сигналы, модулированные «меандром» с частотой 2100 Гц. В окружающем пространстве формируется амплитудная диаграмма направленности $F_{2100}(\theta)$ (рис.4).

$$F_{2100}(\theta) = |\dot{F}_1(\theta) + a\dot{F}_2(\theta)| \quad (1)$$

где: a – соотношение амплитуд сигналов в первой и второй антеннах, устанавливаемое регулируемым делителем мощности.

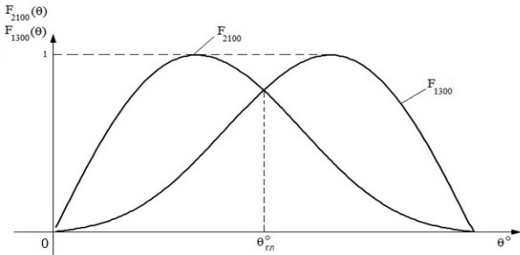


Рис.4. Амплитудные диаграммы направленности для сигналов 2100 Гц $F_{2100}(\theta)$ и 1300 Гц $F_{1300}(\theta)$

Во втором полупериоде излучаются сигналы, модулированные «меандром» с частотой 1300 Гц. При этом сигналы в первой и второй антеннах противофазны между собой. В результате в пространстве формируется амплитудная диаграмма направленности $F_{1300}(\theta)$ (рис.4).

$$F_{1300}(\theta) = |\dot{F}_1(\theta) - a\dot{F}_2(\theta)| \quad (2)$$

Точка пересечения диаграмм направленности $F_{2100}(\theta)$ и $F_{1300}(\theta)$ определяет положение угла глissады $\theta_{\text{гл}}$. При этом ниже угла глissады ($\theta < \theta_{\text{гл}}$) преобладает сигнал, модулированный «меандром» с частотой 2100 Гц. Выше угла глissады ($\theta_{\text{гл}} < \theta$) преобладает сигнал, модулированный «меандром» с частотой 1300 Гц.

Теоретические исследования

Из соотношений (1) и (2), в частом случае идеальной проводимости подстилающей поверхности, следует, что угол глissады $\theta_{\text{гл}}$ равен углу места θ при котором функция $F_2(\theta)$ обращается в нуль $F_2(\theta_{\text{гл}}) = 0$. При этом величина угла глissады $\theta_{\text{гл}}$ не зависит от поведения функции $F_1(\theta)$. Предпочтительно, чтобы функция $F_1(\theta)$ при $\theta = \theta_{\text{гл}}$ принимала максимальное значение.

Воспользуемся далее соотношением, определяющим зону глissады $KPC(\theta)$, полагая, что ГРМ расположен над горизонтальной плоскостью. Тогда для вычисления $KPC(\theta)$ воспользуемся соотношением (3).

$$KPC(\theta) = \frac{|\dot{E}_1(\theta) + a\dot{E}_2(\theta)| - |\dot{E}_1(\theta) - a\dot{E}_2(\theta)|}{|\dot{E}_1(\theta) + a\dot{E}_2(\theta)| + |\dot{E}_1(\theta) - a\dot{E}_2(\theta)|} \quad (3)$$

$$\dot{E}_1(\theta) = e^{ikh_1 \sin \theta} + R(\theta)e^{-ikh_1 \sin \theta} \quad (4)$$

$$\dot{E}_2(\theta) = e^{ikh_2 \sin \theta} + R(\theta)e^{-ikh_2 \sin \theta} \quad (5)$$

h_1 (h_2) – высота подвеса нижней (верхней) антенны относительно подстилающей поверхности;

$$\dot{R}(\theta) = \frac{\sin \theta - \sqrt{\dot{\epsilon} - \cos^2 \theta}}{\sin \theta + \sqrt{\dot{\epsilon} - \cos^2 \theta}} \quad (6)$$

$\dot{R}(\theta)$ – коэффициент отражения Френеля от подстилающей поверхности $\dot{\epsilon}$ – комплексная диэлектрическая проницаемость почвы.

Подстилающая поверхность – идеальная проводящая плоскость

Рассмотрим вначале предельный случай, когда подстилающая поверхность представляет собой идеально проводящую плоскость. В этом случае коэффициент отражения $\dot{R}(\theta)$ равен минус единице. Пусть высоты верхней и нижней антенн отличаются строго в 2 раза.

$$E_1(\theta) = 2\sin(kh\sin\theta) \quad (7)$$

$$E_2(\theta) = 2\sin(2kh\sin\theta) \quad (8)$$

Пусть $h_2 = 2h_1 = 2h$. Тогда

$$KPC(\theta) = 2a\cos(kh\sin\theta) \quad (9)$$

Тогда при $a \leq 0,5$ из (1):

Функция $E_2(\theta)$ обращается в ноль при условии

$$2kh\sin\theta_n = n\pi \quad n = 0, 1, 2, \dots \quad (10)$$

Угол глissады $\theta_{\text{гл}}$ соответствует $n = 1$

$$\sin\theta_{\text{гл}} = \frac{\lambda}{4h} \quad (11)$$

Найдем крутизну S зоны глissады (характеристики ГРМ) при $\theta = \theta_{\text{гл}}$:

$$S = \frac{dKPC(\theta)}{d\theta} \Big|_{\theta=\theta_{\text{гл}}} = -2a\sin(kh\sin\theta_{\text{гл}}) \cdot kh\cos\theta_{\text{гл}} = -2akh\cos\theta_{\text{гл}} \quad (12)$$

Или, учитывая (11):

$$S = -a\pi\text{ctg}\theta_{\text{гл}} \quad (13)$$

В соответствии с нормативными документами [9, 10, 11], границы полусектора зоны выше и ниже линии глissады должны устанавливаться относительно линии глissады в пределах:

- ниже линии глissады $(0,12 \pm 0,2)\theta_{\text{гл}}$,
- выше линии глissады $(0,12^{+0,02}_{-0,05})\theta_{\text{гл}}$.

Крутизна $S \left(\frac{\%}{\text{град}} \right)$ характеристики глissадного радиомаяка должна быть равна $\frac{16,5\%}{K\theta_{\text{гл}}}$. Коэффициент K может принимать значение от 0,1 до 0,14 ниже линии глissады и от 0,07 до 0,14 выше линии глissады.

$$S(\theta) \Big|_{\theta=\theta_{\text{гл}}} = \frac{0,165}{K\theta_{\text{гл}}} \quad 0,1 \leq K \leq 0,14 \quad (14)$$

$$a \cdot \pi \cdot \text{ctg}\theta_{\text{гл}} = \frac{0,165}{K\theta_{\text{гл}}} \quad 0,1 \leq K \leq 0,14 \quad (15)$$

$$a \cdot \pi \cdot \text{ctg}\theta_{\text{гл}} = \frac{0,165}{K\theta_{\text{гл}}} \quad 0,1 \leq K \leq 0,14 \quad (16)$$

Учитывая то, что в радианной мере $\theta_{2l} \ll 1$, воспользуемся приближенным соотношением

$$\frac{\operatorname{tg} \theta_{2l}}{\theta_{2l}} \approx 1 \quad (17)$$

Тогда:

$$a = \frac{0,165}{K\pi} \quad 0,375 \leq a \leq 0,525 \quad (18)$$

При номинальном же значении коэффициента $K = 0,12$ величина $a = 0,44$.

Далее будем полагать, что в ГРМ регулируемым делителем мощности установлен коэффициент $a = 0,44$.

Заметим, что при $2h_1 = h_2 = h$ функция $KPC(\theta) = a \frac{\sin(2\kappa h \sin \theta)}{\sin(\kappa h \sin \theta)}$ в точке $\theta = 2\theta_{2l}$ имеет неопределенность вида $\frac{0}{0}$, которая в пределе раскрывается по правилу Лопиталья как величина. Функция $KPC(\theta)$ непрерывна и при $\theta = 2a_{2l}$ имеет максимальное значение, равное $2a$.

σ_2 – проводимость почвы.

Судя по графикам на рис.14 Рек. МСЭ-R P.527-4 19 в дециметровом диапазоне длин волн реальная часть ε' относительной диэлектрической проницаемости почвы в зависимости от ее влажности изменяется в пределах от 3 до 8. Судя по графикам на рис.1.16 в [12] мнимая часть диэлектрической проницаемости для влажной почвы равна примерно 0,01, а для сухой – примерно 0,001. Поэтому мнимой частью диэлектрической проницаемости в сравнении с действительной в дециметровом диапазоне можно пренебречь.

Диэлектрическую проницаемость почвы будем полагать величиной вещественной (в пределах от 3 до 8)

Поведение амплитудных и фазовых диаграмм направленности

На рис. 5 и рис. 6 приведены амплитудные и фазовые диаграммы направленности нижней и верхней антенн.

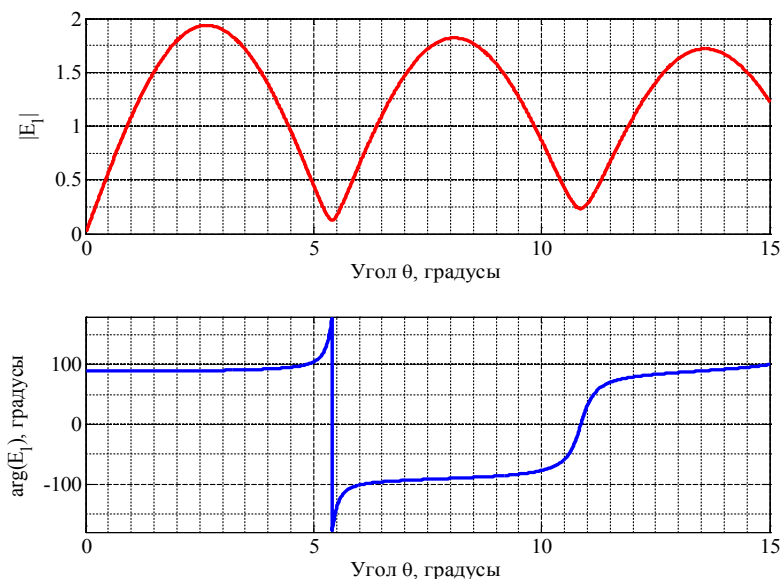


Рис. 5. Амплитудная и фазовая диаграммы направленности нижней антенны

Подстилающая поверхность – граница двух диэлектриков

Параметры почвы в диапазоне дециметровых волн. В диапазоне дециметровых волн почву можно рассматривать как диэлектрик. Действительно,

$$\dot{\varepsilon} = \varepsilon' - i \frac{\sigma_2}{\omega \varepsilon_0}$$

$\varepsilon' = \frac{\varepsilon_a}{\varepsilon_0}$ – относительная диэлектрическая проницаемость почвы,

ε_a – абсолютная диэлектрическая проницаемость среды,

ε_0 – электрическая постоянная вакуума,

Заметим, что фазовые диаграммы направленности в действительности представляют непрерывные монотонно растущие функции. С целью упрощения построения графиков зависимость фазы от угла места построена с точностью до 360° . Это упрощение придает графикам фазовых диаграмм направленности обманчивый вид – вид разрывных функций.

С учетом реальных свойств подстилающей поверхности коэффициент отражения Френеля отличен от минус единицы. Поэтому при углах места θ_n , удовлетворяющих условию $2\kappa h \sin \theta_n = n\pi$ $n = 0, 1, 2, \dots$, уровни в ми-

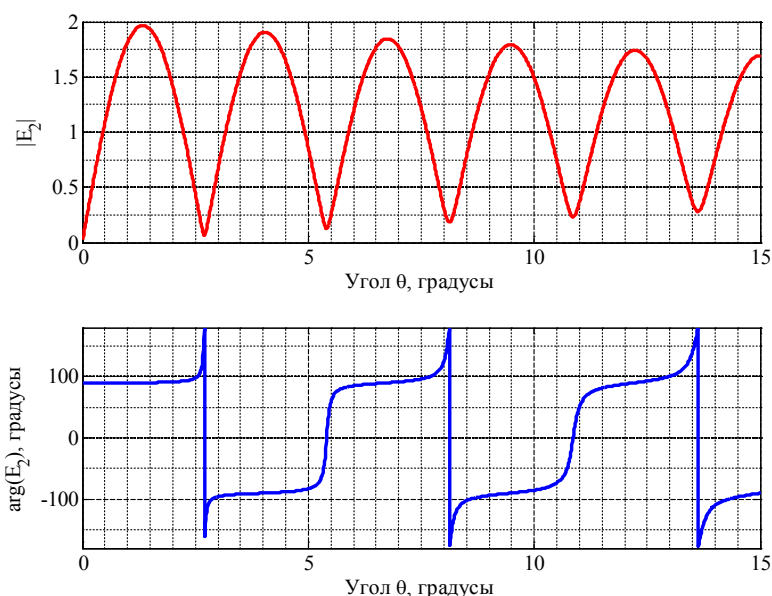


Рис. 6. Амплитудная и фазовая диаграммы направленности верхней антенны

нимумах диаграмм направленности имеют конечные значения. При этом в функции $KPC(\theta)$ при $0 < \theta_n$ исчезает неопределенность вида $\frac{0}{0}$.

На рис. 7 приведена зависимость $KPC(\theta)$ в предположении, что относительная диэлектрическая проницаемость почвы равна 4.

Это область углов, в которой еще можно рассматривать экспериментальные записи токов на пленке шлейфного осциллографа при выполнении горизонтального полета, как обычно, на высоте 300 м в направлении оси ВПП.

Как видно из графиков на рис. 7, в случае идеально проводящей подстилающей по-

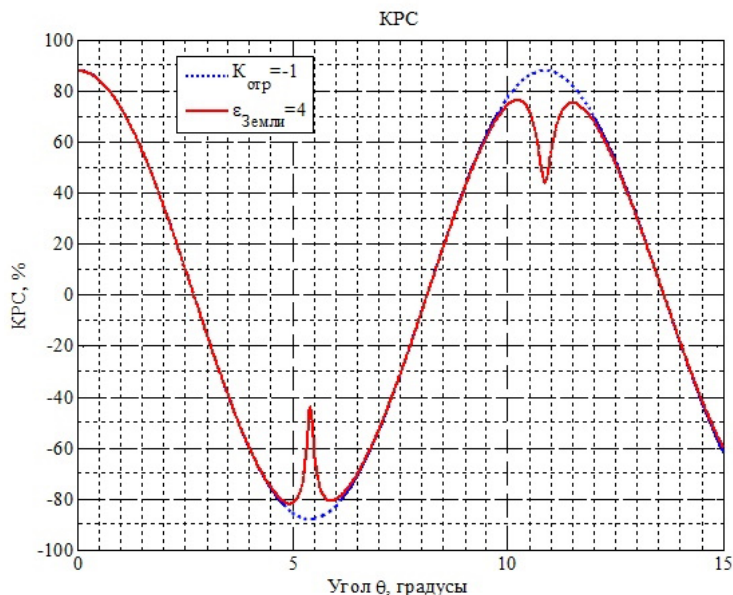


Рис. 7. Зависимость КРС от угла места

Поведение КРС в зависимости от угла θ при $2h_1 = h_2$

С целью выявления общих закономерностей в поведении функции $KPC(\theta)$ в зоне глиссады и за ее пределами вычисления выполнены в диапазоне углов места θ , превышающих угол глиссады более чем в пять раз.

верхности функция представляет собой почти косинусоидальную зависимость. Более точно, осциллирующую зависимость, в которой угловые координаты точек с нулевыми уровнями, соотносятся как

$$\frac{\sin \theta_{n+1}}{\sin \theta_n} = \frac{n+1}{n} \quad n = 1, 2, \dots \quad (19)$$

Или, учитывая при малых углах приближенное равенство $\sin \theta_n \approx \theta_n$, угловые координаты точек с нулевыми уровнями, соотносятся как

$$\frac{\theta_{n+1}}{\theta_n} = \frac{n+1}{n} \quad n = 1, 2, \dots \quad (20)$$

т.е. как целые числа.

При учете параметров почвы как диэлектрика с относительной диэлектрической проницаемостью, равной 4, наблюдается различие в поведении функции $KPC(\theta)$ в окрестности углов глиссады, примерно равных $2\theta_{2\lambda}$ и $4\theta_{2\lambda}$. В некоторой окрестности каждого из этих углов график функция $KPC(\theta)$ выглядит как график кривой конического сечения с закруглением малого радиуса. В этих точках функция уклоняется от минимального значения, равного минус $2a$, при $\theta \approx 2\theta_{2\lambda}$ и максимального значения, равного плюс $2a$, примерно на одну и ту же величину. Величина уклонения такова, что абсолютная величина в этих точках не менее, чем 41,5%.

Это означает, что если бортовой приемник способен работать при той напряженности поля, которая наблюдается в минимумах ДН нижней антенны, соответствующих рассматриваемым углам, то на экспериментальной записи токов индикации эти уклонения не будут отражаться.

Поведение КРС в зависимости от угла θ при $2h_1 \neq h_2$

Предположим теперь, что требование установить соотношение высот равным 2:1 нарушено. Обратимся снова к (3).

Пусть, например, нижняя антенна установлена по высоте $h_{1+\lambda}$ с ошибкой в одну длину волны $h_{1+\lambda} = h_1 + \lambda$. Тогда зависимость KPC от угла θ примет вид, представленный на рис. 8. Вычисления выполнены для ГРМ с углом глиссады $\theta_{2\lambda} = 2,7^\circ$.

На графике $KPC(\theta)$ рис. 8 отмечены угловые координаты характерных точек зоны: угла глиссады, полусекторов зоны ($2,38^\circ$ и $3,02^\circ$), $KPC = 41,5\%$ ($\theta = 1,77^\circ$) и $KPC = -41,5\%$ ($\theta = 3,36^\circ$). Угол глиссады не изменился. Однако, поведение функции $KPC(\theta)$ при $h_{1+\lambda} = h_1 + \lambda$ резко отличается от поведения при соотношении высот, равным 2:1. В зоне действия ГРМ наблюдается ложная глиссада под углом $4,57^\circ$. В верхней части сектора зоны KPC имеет положительный знак, недопустимый для этой части зоны. При ошибке в установке нижней антенны выше положенной высоты на одну длину волны (примерно 30 см) зона глиссады не удовлетворяет требованиям, предъявляемым ГОСТ к зоне ГРМ второй категории (а также к ГРМ первой категории).

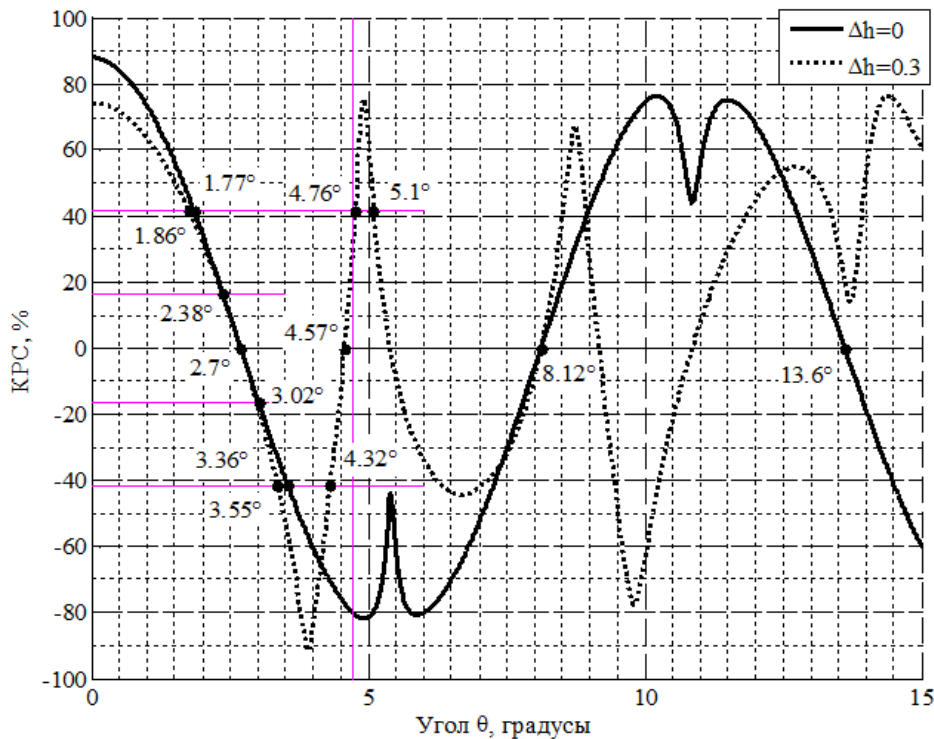


Рис. 8. Зависимость КРС от угла места при номинальной высоте подвеса нижней антенны и при смещенной вверх на одну длину волны

Экспериментальные результаты

Экспериментальные результаты получены в переходный период от осени к зиме. В это время мерзлая земля в зоне, существенной для отражения электромагнитных волн, излучаемых ГРМ, была покрыта тонким слоем снега ($\approx 5-8$ см). Измерения выполнены с помощью воздушного судна-лаборатории (ВСЛ), оборудованного аппаратурой летного контроля.

Принятые на борту воздушного судна высокочастотные сигналы ГРМ подвергаются преобразованию. Упрощенная схема блок-схема бортового приемника показана на рис. 9. Высокочастотные сигналы усиливаются в приемно-усилительном каскаде. Усиленные сигналы поступают на детектор. На выходе детектора тоновые сигналы выделяются полосовыми фильтрами и подвергаются выпрямлению. Разность и сумма выпрямленных тоновых токов формируют информационный сигнал: Коэффициент Разнослышимости Сигналов.

На рис. 10 приведена требуемая норма-

тивными документами зависимость информационного параметра от угла места $KPC(\theta)$ и соответствующая ему величина тока индикации $I(\theta)$.

На рис. 10 по горизонтали откладывается нормированный угол места $\frac{\theta}{\theta_{21}}$. В качестве нормы выбран угол глиссады θ_{21} . По вертикали откладывается величина KPC в процентах и ток индикации I в μA . Вертикальными прямыми указаны границы зоны действия ГРМ в вертикальной плоскости: нижняя граница, равная $0,45\theta_{21}$ и верхняя граница, равная $1,75\theta_{21}$. Горизонтальными прямыми указаны границы полусектора: граница верхней части полусектора, равная плюс $0,165 KPC$ и граница нижней части полусектора, равная минус $0,165 KPC$, и соответствующие им токи индикации плюс $125 \mu A$ и минус $125 \mu A$, соответственно. Кроме того, горизонтальными прямыми указаны границы монотонного изменения информационного параметра и соответствующие им токи $I = \pm 315 \mu A$.

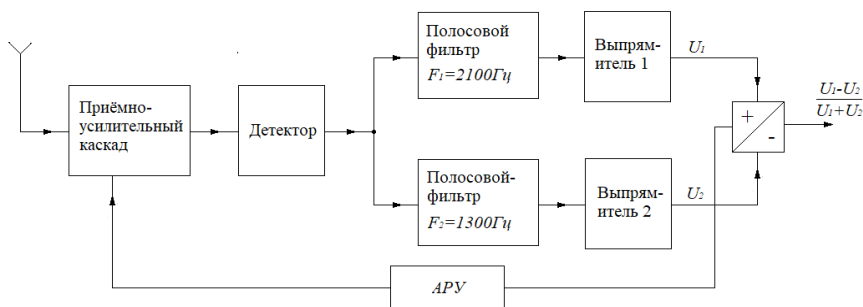


Рис. 9. Упрощенная блок-схема бортового приемника-измерителя КРС

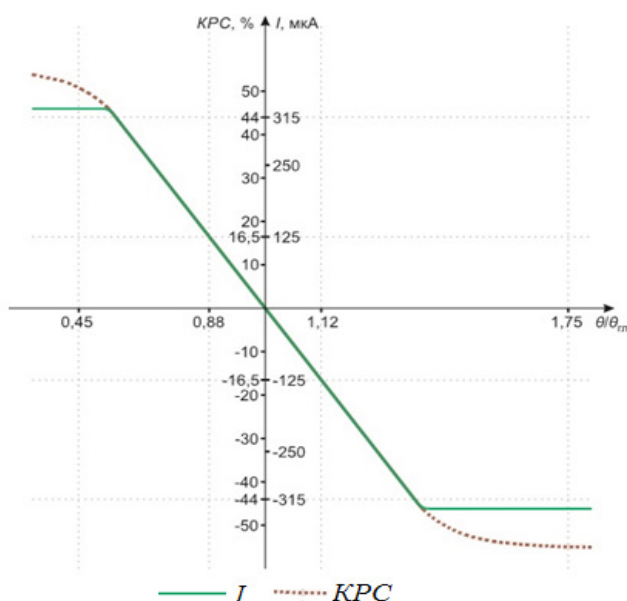


Рис. 10. Зависимость КРС и тока индикации от нормированного угла места, КРС, I

В пределах полусектора $|KPC| \leq 16,5\%$ должна наблюдаться линейная зависимость тока индикации от угла отклонения от глissады. За пределами полусектора ток индикации должен монотонно увеличиваться по абсолютной величине до указанной границы $I = \pm 315 \mu\text{KA}$. За пределами указанного участка монотонного изменения функции $KPC(\theta)$ не должен по абсолютной величине быть меньше $315 \mu\text{KA}$ вплоть до углов $0,45\theta_{2л}$ и $1,75\theta_{2л}$. Это требование условно показано на рис. горизонтальными пунктирными линиями.

Выполнялись стандартные заходы [13]. Заметим, что измерениями по заходам по нулю глissады, по верхнему и по нижнему полусекторам было установлено следующее. На основном и противоположном направлениях границы полусектора выше и ниже линии глissады установлены в пределах $(0,12 \pm 0,2)\theta_{2л}$.

На рис. 11 приведена зависимость тока индикации, равного току, поступающему на пилотажный прибор, и зависимость тока устройства траекторной записи (УТЗ) при горизонтальном полете ВСЛ на высоте 300 м по основному направлению захода самолетов на посадку на аэродром, а на рис.12 – при полете по противоположному направлению, соответственно.

Рисунки отличаются друг от друга разным горизонтальным масштабом. В левой части каждого рисунка приведены записи калибровки тока индикации I в $\frac{\mu\text{KA}}{\text{мм}}$ и тока калибровки УТЗ $\frac{\mu\text{KA}}{\text{град}}$.

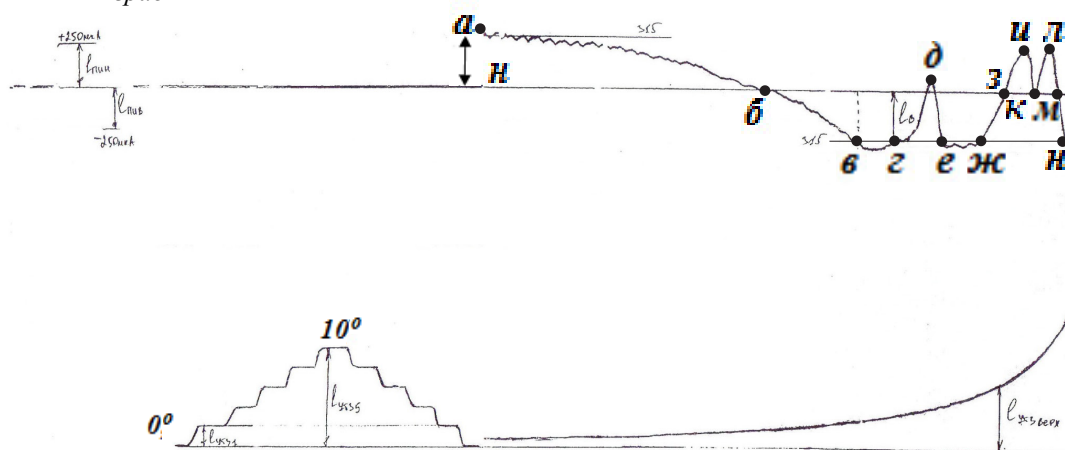


Рис. 11. Ток индикации и ток УТЗ при полёте на высоте 300 м в основном направлении

По графику тока УТЗ (нижняя кривая на рис.11, 12) можно определить угол точки наблюдения ВСЛ относительно горизонта в си-

стеме координат с началом на позиции УТЗ. В верхней части рисунка приведена зависимость тока индикации. На графиках буквами, **а – н** отмечены характерные точки. Угловые координаты характерных точек на графике зависимости тока индикации при полете по основному направлению и в обратном направлении указаны в таблицах 1 и 2, соответственно.

Рассмотрим поведение тока индикации от расстояния в сечении при полете на высоте 300 м на основном направлении. Обратимся к рис. 11 и таблице 1.

На графике на рис.11 буквами **а-н** обозначены характерные точки зависимости тока $I(\mu\text{KA})$ от расстояния. В таблице указаны угловые координаты характерных точек.

В третьей строке таблицы указано отношение угловой координаты каждой точки к углу глissады.

На графике буквой **а** отмечена точка ($\theta_a = 1,87^\circ$), до которой ток индикации при отклонении от глissады вниз возрастает до величины плюс $315 \mu\text{KA}$. Точка **б** ($\theta_b = 2,67^\circ$) – точка перехода кривой тока индикации через нуль. Это означает, что точка **б** находится непосредственно на глissаде. Угол глissады равен $2,67^\circ$. Точкой **в** ($\theta_v = 4,28^\circ$) отмечена точка, до которой ток индикации при отклонении от глissады вверх возрастает по абсолютной величине до величины $315 \mu\text{KA}$. Заметим, что на отрезке $\theta_a < \theta < \theta_v$ с ростом угла места ток индикации монотонно убывает от величины плюс $315 \mu\text{KA}$ в точке **а** до нулевого значения в точке **б** ($\theta_b = 2,67^\circ$) на глissа-

де и далее до минус $315 \mu\text{KA}$ в точке **в** под углом места θ_v ($\theta_v = 4,28^\circ$).

Точка **з** ($\theta_z = 8,02^\circ$) и точка **м** ($\theta_m = 13,37^\circ$)

Угловые координаты характерных точек на записи тока индикации на основном направлении посадки

Точки	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п
θ_v	1,87	2,67	4,28	4,8	5,35	5,88	6,95	8,02	9,09	10,7	12,3	13,37	15	5,3	5,4
θ_v / θ_{21}	0,7	1	1,4	1,8	2	2,2	2,6	3	3,4	4	4,6	5	5,6	1,98	2,02

– это точки, соответствующие углу, равному $3\theta_{21}$ и $5\theta_{21}$, соответственно. На отрезке от точки **в** до точки **ж** график функции тока имеет форму близкую к горизонтальной прямой с возвышением по середине отрезка. Возвышение имеет форму сечения конуса с закругленным наконечником. Вершина возвышения (точка **д**, $\theta_o = 5,35^\circ$) приходится на угол, равный удвоенному углу глиссады. Максимальное значение тока в точке **д** ($\theta_o = 5,35^\circ$) равно плюс $75 \mu\text{A}$.

На участке между двумя максимумами в точках **и** ($\theta_u = 9,09^\circ$) и **л** ($\theta_l = 12,3^\circ$) наблюдается углубление в форме сечения конуса с закругленным наконечником. Минимум углубления приходится на угол $\theta_k = 10,7^\circ$, равный по величине примерно. Минимальное значение тока в минимуме углубления равно нулю.

Особенностью рассматриваемой зависимости является то, что в промежутке $(\theta_{21}, 3\theta_{21})$ существует две точки в окрестности точки **д** с нулевым значением КРС. Одна из них точка **о** ($\theta_o = 5,08^\circ$) находится на промежутке $(\theta_{21}, 2\theta_{21})$. Однако точку **о** нельзя считать, лежащей на ложной глиссаде, так как ее координата, равная $5,08^\circ$, больше координаты границы зоны действия ГРМ в вертикальной плоскости, равной $1,75\theta_{21} = 4,7^\circ$.

Таким образом, характеристика ГРМ на основном направлении соответствует требованиям, предъявляемым к характеристикам ГРМ второй категории.

Рассмотрим теперь поведение тока индикации в сечении при полете на высоте 300м по обратному направлению. Обратимся теперь к рис.12 и табл. 2.

На графике буквой **а** отмечена точка

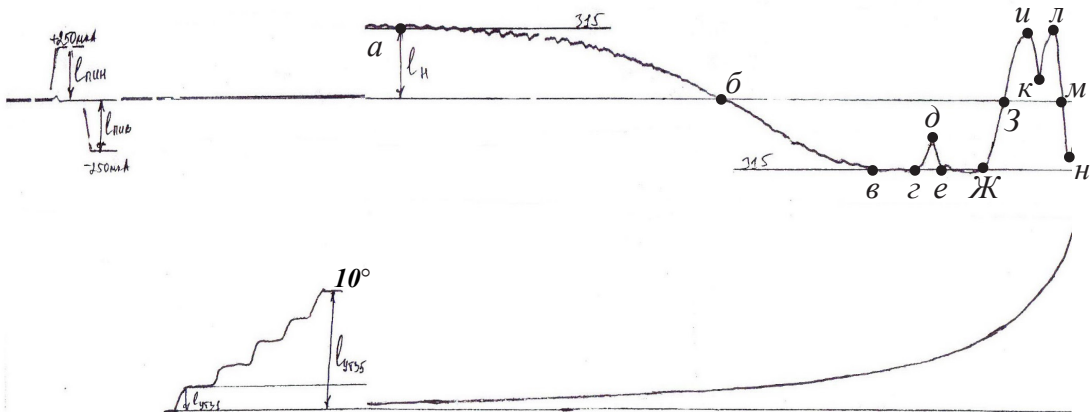


Рис. 12. Ток индикации и ток УТЗ при полёте на высоте 300 м на противоположном направлении

Таблица 2

Угловые координаты характерных точек на записи тока индикации на противоположном направлении посадки

Точки	а	б	в	г	д	е	ж	з	и	к	л	м	н
θ_v	1,91	2,72	4,55	5,23	5,45	5,91	7,41	8,18	10,45	10,9	12,5	13,64	15,9
θ_v / θ_{21}	0,7	1	1,67	1,92	2	2,17	2,72	3	3,84	4	4,6	5	5,66

($\theta_a = 1,91^\circ$), до которой ток индикации при отклонении от глissады вниз возрастает до величины плюс ($\theta_a = 1,91^\circ$), 315 мкА . Точка δ ($\theta_\delta = 2,72^\circ$) – это точка перехода кривой тока индикации через нуль. Следовательно, точка δ – это точка непосредственно на глissаде. Угол глissады равен $2,72^\circ$. Точкой ϵ ($\theta_\epsilon = 4,55^\circ$) отмечена точка, до которой ток индикации при отклонении от глissады вверх возрастает по абсолютной величине до 315 мкА . Заметим, что на отрезке $\theta_a < \theta < \theta_\epsilon$ с ростом угла места ток индикации монотонно убывает от величины плюс 315 мкА в точке a до нулевого значения в точке δ ($\theta_\delta = 2,72^\circ$) на глissаде и далее до минус 315 мкА в точке ϵ под углом места θ_ϵ ($\theta_\epsilon = 4,55^\circ$). Точка $з$ ($\theta_з = 8,18^\circ$) и точка $м$ ($\theta_м = 13,64^\circ$) – это точки, в которых ток индикации равен нулю, в этих точках $\theta_з = 3\theta_{\delta}$ и $\theta_м = 5\theta_{\delta}$, соответственно. На отрезке от точки ϵ до точки $ж$ ($\theta_ж = 7,41^\circ$) график функции тока имеет форму близкую к отрезку горизонтальной прямой с возвышением по середине отрезка. Возвышение имеет форму сечения конуса с закруглением. Вершина возвышения (в точке ∂ , $\theta_\partial = 5,45^\circ$) приходится на угол, равный удвоенному углу глissады. Величина тока в точке ∂ ($\theta_\partial = 5,45^\circ$) равна минус 60 мкА .

На участке между двумя максимумами в точках $и$ $\theta_и = 10,45^\circ$ и $\theta_н = 12,5^\circ$ наблюдается углубление остроконечной формы. Минимум приходится на угол $\theta_к = 11,36^\circ$, равный четырем углам глissады. Величина тока на дне углубления равна плюс 100 мкА .

Как видно, характеристика ГРМ отличается от идеальной характеристики, соответствующей соотношению высот верхней и нижней антенн строго 2:1, лишь тем, что в зависимости $KPC(\theta)$ в окрестности двойного угла глissады наблюдается минимум. Однако, область с величинами КРС $< 41,5\%$, находится выше угла, равного $1,75\theta_{гн}$.

При отклонении от линии глissады вверх $KPC(\theta)$ возрастает до угла $1,75\theta_{гн}$ не менее чем на $41,5\%$. При отклонении от линии глissады вниз возрастает до величины $41,5\%$ под углом до угла $0,65\theta_{гн}$. И далее остается неизменной до угла $0,3\theta_{гн}$ (на рис не показано).

Таким образом, характеристика ГРМ на противоположном направлении также полностью соответствует требованиям, предъявляемым к характеристикам ГРМ второй категории.

Примечание. На данных осциллограммах

нет отметок дальнего и ближнего маркерных радиомаяков, которые позволяют более точно скорректировать координаты самолета в процессе измерения характеристик радиомаяков.

Обсуждение результатов

В статье представлено подробное изложение принципа работы глissадного радиомаяка, поскольку в известной журнальной и методической литературе принцип работы ранее не был детально представлен. Далее, в обычно используемом предположении идеальной проводимости подстилающей поверхности в виде горизонтальной плоскости найдены соотношения для вычисления параметров зоны глissады. При этом зависимость КРС от угла места описывается косинусоидальной функцией от обобщенного угла $khs \sin \theta$. Оказывается, что для формирования номинальной крутизны зоны отношение a амплитуды тока в верхней антенне к амплитуде тока в нижней антенне должно быть равным $0,44$. Именно при этом значении a выполнен теоретический анализ и в том случае, когда подстилающая поверхность имеет реальные параметры.

В дециметровом диапазоне диэлектрическую проницаемость почвы можно с достаточной для практики точностью считать величиной вещественной. Учет реальных параметров почвы показывает, что в интерференционных минимумах уровень амплитудной ДН имеет хотя и небольшое, но все-таки конечное значение. При расчете зависимости КРС от угла места исчезает неопределенность вида $0/0$, характерная при идеальной проводимости подстилающей поверхности для угла места, равного удвоенному значению угла глissады. Одновременно с этим исчезает строго косинусоидальная зависимость КРС от угла места. График зависимости КРС при $2h_1 = h_2$ в окрестности углов, равных четному количеству угла глissады, приобретает вид, известный в литературе как вид кривой конического сечения с закруглением малого радиуса (вид "клювика"). Однако, эти отличия от косинусоидальной зависимости при летных измерениях при строго выдержанном соотношении высот 2:1 не могут быть замечены, а КРС при этом по абсолютной величине больше $41,5\%$ и, стало быть, не выходит за пределы ограничений.

Отличия КРС от косинусоидальной зависимости усугубляются со случайным или преднамеренным введением ошибки в уста-

новку нижней антенны ($2h_1 = h_2$). Так при ошибке в одну длину волны на границе зоны ГРМ формируется ложная глиссада. Ниже удвоенного угла глиссады формируется неверная информация о нахождении точки наблюдения относительно глиссады. Тем не менее, асимметрия зоны, определяемая по показаниям КРС на уровне плюс 16,5% и на уровне минус 16,5% пренебрежимо мала. Практически показания на этих уровнях сохранились неизменными. В связи с этим следует сделать важное замечание. При вводе ГРМ в эксплуатацию и в период плановых проверок (два раза в год) обнаруженную в процессе летных настроек ГРМ асимметрию зоны пытаются устранить изменением высоты подвеса нижней антенны. Как видно из приведенного примера, по крайней мере в случае строго плоской подстилающей поверхности, изменением высоты подвеса нижней антенны устранить асимметрию зоны глиссады не представляется возможным. А приобрести неприятности в виде ложной глиссады возможно.

Поэтому, целесообразно при вводе ГРМ в эксплуатацию установить соотношение высот подвеса верхней и нижней антенн как возможно точно в соотношении 2:1.

Летные измерения характеристик ГРМ подтвердили найденные теоретически зако-

номерности в поведении зависимости $KPC(\theta)$.

Найденные закономерности в поведении зависимости $KPC(\theta)$ полезно применять при летной настройке ГРМ при выводе ГРМ в эксплуатацию.

Выводы

Учет подстилающей поверхности как границы раздела двух диэлектрических сред: воздух-почва, объясняет особенности поведения характеристики ГРМ в окрестности двойного угла глиссады. График зависимости КРС при $2h_1 = h_2$ в окрестности углов, равных четному числу угла глиссады, приобретает вид, известный в литературе как вид кривой конического сечения с закруглением малого радиуса («вид клювика».)

При ошибке в установке высоты подвеса нижней антенны порядка одной длины волны может в зоне глиссады, может формироваться ложная глиссада.

С целью сохранения целостности системы посадки необходимо при вводе ГРМ в эксплуатацию установить соотношение высот подвеса верхней и нижней антенн как можно точно в соотношении 2:1.

Анализ поведения тока индикации в широком секторе углов на основе найденных закономерностей оказывается полезным для выполнения летной настройки ГРМ.

Литература

1. Галенко В. Некоторая статистика катастроф при заходе на посадку и посадке (AVIASAFETY.RU) (по базе данных Международного консультативно-аналитического агентства «Безопасность полетов»). – URL: <https://aviator.guru> (дата обращения 17.09.2020 г.).
2. Шатраков Ю.Г. Безопасность полетов. – URL: <https://topwar.ru> (дата обращения 05.10.2020 г.).
3. Пахолков Г.А., Кашинов В.В., Соломоник М.Е., Шатраков Ю.Г. Угломерные радиотехнические системы посадки: (Прогнозирование точностных характеристик) — М.: Транспорт, 1982. – 159 с.
4. Посадочная радиомаячная группа дециметрового диапазона ПРМГ 76УМ. – URL: www.polyot.ru/products/24 (дата обращения 25.09.2020 г.).
5. Воробьев В.В., Киселев А.М., Поляков В.В. Системы управления летательных аппаратов: учебник для курсантов-слушателей вузов ВВС. Под ред. В.В.Воробьева. – М.: Изд. ВВИА им. проф. Н.Е. Жуковского. – 2008. – 203 с.
6. Микоян С.А., Корбут А.Г. Заход на посадку по приборам. – М.: Военное издательство Министерства обороны СССР. – 1979. – 48 с.
7. Радиомаячные системы посадки и системы VOR: Учебное пособие. / Сост.: А.В. Хафизов – Кировград: ГЛАУ. – 2009. – 83 с.
8. Павлов Ю.В. Глиссадный радиомаяк: Учебное пособие / Ю.В. Павлов. М.: ВВИА им. проф. Н.Е. Жуковского. – 1960. – 52 с.
9. Системы радиомаячные дециметрового диапазона второй категории инструментального захода самолетов на посадку. Общие технические требования. Основные параметры. ГОСТ 15827 – 70
10. Системы инструментального захода самолетов на посадку радиомаячные. Термины и определения. ГОСТ 26121 –84. М.: Госкомитет СССР по стандартам.
11. Нормы годности к эксплуатации аэродромов экспериментальной авиации (НГЭА ЭА). Приказ

Минпромторга РФ от 30.12.2009 № 1215 «Об утверждении нормативных методических документов, регулирующих функционирование и эксплуатацию аэродромов экспериментальной авиации». Зарегистрировано в Минюсте РФ 5 апреля 2010 г. Регистрационный № 16822.

12. Электрические характеристики земной поверхности. ИТУ: Международный союз электросвязи. Серия Р. Распространение радиоволн. Рекомендация МСЭ-R P.527-4(06/2017).

13. Васильева Е.Ф. Методика летной проверки радиомаячных систем посадки и навигации с помощью аппаратуры летного контроля АСЛК-75 / Е.Ф. Васильева (ред.). – ВВС, 1995. – 212 с.

References

1. Galenko V. Nekotoryaya statistika katastrof pri zakhode na posadku i posadke (AVIASAFETY.RU) (po baze dannykh Mezhdunarodnogo konsul'tativno-analiticheskogo agentstva «Bezopasnost' poletov»). – URL:[https://aviator.guru\(data obrashcheniya 17.09.2020 g.\)](https://aviator.guru(data obrashcheniya 17.09.2020 g.)).

2. Shatrakov YU.G. Bezopasnost' poletov. – URL:[https://topwar.ru \(data obrashcheniya 05.10.2020 g.\)](https://topwar.ru (data obrashcheniya 05.10.2020 g.)).

3. Pakholkov G.A., Kashinov V.V., Solomonik M.Ye., Shatrakov YU.G. Uglomernyye radiotekhnicheskiye sistemy posadki: (Prognozirovaniye tochnostnykh kharakteristik) — М.: Transport, 1982. – 159 s.

4. Posadochnaya radiomayachnaya gruppa detsimetrovogo diapazona PRMG 76UM. – URL:[www.polyot.ru/products/24 \(data obrashcheniya 25.09.2020 g.\)](http://www.polyot.ru/products/24 (data obrashcheniya 25.09.2020 g.)).

5. Vorob'yev V.V., Kiselev A.M., Polyakov V.V. Sistemy upravleniya letatel'nykh apparatov: uchebnik dlya kursantov-slushateley vuzov VVS. Pod red. V.V.Vorob'yeva. – М.: Izd. VVIA im. prof. N.Ye. Zhukovskogo. – 2008. – 203 s.

6. Mikoyan S.A., Korbut A.G. Zakhod na posadku po priboram. – М.: Voennoye izdatel'stvo Ministerstva oborony SSSR. – 1979. – 48 s.

7. Radiomayachnyye sistemy posadki i sistemy VOR: Uchebnoye posobiye. / Sost.: A.V. Khafizov – Kirovograd: GLAU. – 2009. – 83 s.

8. Pavlov YU.V. Glissadnyy radiomayak: Uchebnoye posobiye / YU.V. Pavlov. М.: VVIA im. prof. N.Ye. Zhukovskogo. – 1960. – 52 s.

9. Sistemy radiomayachnyye detsimetrovogo diapazona vtoroy kategorii instrumental'nogo zakhoda samoletov na posadku. Obshchiye tekhnicheskiye trebovaniya. Osnovnyye parametry. GOST 15827 – 70.

10. Sistemy instrumental'nogo zakhoda samoletov na posadku radiomayachnyye. Terminy i opredeleniya. GOST 26121 – 84. М.: Goskomitet SSSR po standartam.

11. Normy godnosti k ekspluatatsii aerodromov eksperimental'noy aviatsii (NGEA EA). Prikaz Minpromtorga RF ot 30.12.2009 № 1215 «Ob utverzhdenii normativnykh metodicheskikh dokumentov, reguliruyushchikh funktsionirovaniye i ekspluatatsiyu aerodromov eksperimental'noy aviatsii». Zaregistrirvano v Minyuste RF 5 aprelya 2010 g. Registratsionnyy № 16822.

12. Elektricheskiye kharakteristiki zemnoy poverkhnosti. ITU: Mezhdunarodnyy soyuz elektrosvyazi. Seriya R. Rasprostraneniye radiovoln. Rekomendatsiya MSE-R P.527-4(06/2017).

13. Vasil'yeva Ye.F. Metodika letnoy proverki radiomayachnykh sistem posadki i navigatsii s pomoshch'yu apparatury letnogo kontrolya ASLK-75 / Ye.F. Vasil'yeva (red.). – VVS, 1995. – 212 s.

ВОЙТОВИЧ Николай Иванович, доктор технических наук, профессор, заведующий кафедрой конструирования и производство радиоаппаратуры, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: voytovichni@mail.ru

VOYTOVICH Nikolay Ivanovich, Doctor of Technical Sciences, Professor, Head of the Department of Design and Production of Radio Equipment, South Ural State University (National Research University). 76, Lenin prospect, Chelyabinsk, 454080, Russia. E-mail: voytovichni@mail.ru

ЖДАНОВ Борис Викторович, кандидат технических наук, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: boris.z@inbox.ru

ZHDANOV Boris Victorovich, PhD in Engineering sciences, South Ural State University (National Research University). 76, Lenin prospect, Chelyabinsk, 454080, Russia. E-mail: boris.z@inbox.ru

ЕРШОВ Алексей Валентинович, кандидат технических наук, Южно-Уральский государ-

ственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: eav@list.ru

ERSHOV Aleksey Valentinovich, PhD in Engineering sciences, South Ural State University (National Research University). 76, Lenin prospect, Chelyabinsk, 454080, Russia. E-mail: eav@list.ru

ЮНГАЙТИС Екатерина Михайловна, младший научный сотрудник, ООО «КОНСТРУКТОРСКОЕ БЮРО «ЭКРАН» имени М.А. Шильмана». 454080, г. Челябинск, ул. Энтузиастов, дом 26Б; аспирант, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: jungaitis92@gmail.ru

IUNGAITIS Ekaterina Mikhailovna, junior researcher, LLC "DESIGN BUREAU" EKRAN "named after M.A. Shilman". Building 26B, st. Enthusiasts, Chelyabinsk, 454080, Russia; postgraduate, South Ural State University (National Research University). 76, Lenin prospect, Chelyabinsk, 454080, Russia. E-mail: jungaitis92@gmail.ru

ВЛИЯНИЕ ВЗАИМОДЕЙСТВИЯ ЭЛЕМЕНТОВ АНТЕННО– ФИДЕРНОГО ТРАКТА РАДИОЛОКАТОРА НА ШУМОВЫЕ ХАРАКТЕРИСТИКИ КАНАЛА ПРИЕМА

В статье рассматривается влияние эффектов взаимодействия передающей и приемной антенн радара миллиметрового диапазона, а также прямого прохождения сигнала передатчика на вход приемника по внутренним цепям СВЧ микросхемы на уровень декоррелированного фазового шума. Показано, что при определенных величине связи между антеннами, времени задержки распространения сигнала по путям дополнительного приема, коэффициенте шума приемника и уровне фазового шума несущей передатчика на частоте отстройки, равной частоте полезного сигнала, на выходе преобразователя приемника мощность шума по дополнительному каналу приема и собственные шумы приемника становятся соизмеримы. За счет дополнительного канала приема создаются условия, приводящие к уменьшению приведенного к входу приемника отношения сигнал/шум и ограничению дальности действия радиолокатора. При расчете использованы данные для коэффициента шума приемника и спектральной плотности фазового шума синтезатора микросхемы приемо–передатчика миллиметрового диапазона AWR1243 фирмы Texas Instruments в диапазоне от 77 до 81 ГГц. Рассматривается влияние диэлектрического антенного укрытия на коэффициент связи передающей и приемной антенн, и, как следствие, на спектральную плотность мощности шума на входе приемника. Показаны зависимости спектральной плотности декоррелированного фазового шума за счет дополнительных каналов связи в сравнении с собственными шумами приемника.

Ключевые слова: фазовый шум, радар, приемник, передатчик, коэффициент шума приемника, линейная частотная модуляция, миллиметровые волны.

INFLUENCE OF INTERACTION BETWEEN ELEMENTS OF THE RADAR ANTENNA–FEEDER NETWORK ON THE NOISE CHARACTERISTICS OF THE RECEPTION CHANNEL

The influence of the interaction effects of the transmitting and receiving antennas of a millimeter-range radar, as well as the direct transmission of the transmitter signal to the receiver input via the internal circuits of the microwave chip on the level of the decorrelated phase noise is under consideration. It is shown that for a certain amount of interaction between the antennas, the delay time of signal propagation along the paths of additional reception, the receiver noise factor and the level of phase noise of the carrier frequency of the transmitter at the detuning frequency equal to the frequency of the useful signal, the output noise power of the receiver converter by the additional receiving channel and the receiver's own noise become comparable. Due to the additional noise reception channel, the signal-to-noise ratio decreases and the range of the radar action decreases as well. The calculation uses data for the noise factor of the receiver and the spectral density of the phase noise of the synthesizer of the AWR1243 millimeter-wave transceiver chip from Texas Instruments in the frequency range from 77 till 81 GHz. The effect of a dielectric antenna shelter on the coupling between the transmitting and receiving antennas, and on the spectral noise power density at the receiver input, is considered. The dependences of the spectral density of the decorrelated phase noise due to additional communication channels in comparison with the receiver's own noise are shown.

Keywords: phase noise, radar, receiver, transmitter, noise factor, linear frequency modulation, millimeter waves.

Скрытность работы радиотехнических систем, помимо применения шумоподобных сигналов, обеспечивается уменьшением уровня излучаемой мощности. Однако для сохранения тактико-технических характеристик радиолокационных датчиков охранных систем и радаров транспортных систем безопасности, в том числе при воздействии средств преднамеренного подавления [1], актуальной становится задача реализации предельной чувствительности приемника. Повышение чувствительности приемника связано с минимизацией уровня системных помех, из которых для радиолокационных систем с линейной частотной модуляцией (ЛЧМ) основной является наводка сигнала

передатчика на входе приемника. В связи с этим актуальным при разработке схемотехнических решений при построении РЛС является изучение методов расчета и измерения уровня таких помех и их влияния на шумовые характеристики канала приема.

Уровень электромагнитного шума на входе радиоприемника существенно влияет на эффективность обнаружения объектов радиолокационными комплексами. В первую очередь помехи ограничивают дальность действия систем. Обычно рассматривают внешние помехи, обусловленные природными и промышленными источниками электромагнитного излучения, и внутренние шумы, в первую очередь создаваемые элементами

входных цепей и первыми каскадами малошумящих усилителей радиоприемников. Заданное соотношение сигнал/шум достигается увеличением коэффициента усиления антенн и излучаемой мощности. Однако в ряде ситуаций подобные действия не дают ожидаемого результата.

Рассмотрим радиолокатор, использующий ЛЧМ излучаемого сигнала. Обобщенная схема такого локатора показана на рис. 1. Отраженный от объекта сигнал, принимаемый антенной A_{RX} и поступающий на вход приемника, в идеальных условиях подобен излученному сигналу с некоторой задержкой, зависящей от дальности до объекта, и при ненулевой радиальной взаимной скорости он приобретает дополнительный частотный сдвиг, обусловленный эффектом Доплера.

Паразитные связи между передатчиком и смесителем, а также антеннами передатчика A_{TX} и приемника A_{RX} приводят к появлению дополнительных каналов приема зондирующего сигнала. Таким образом, на входе смесителя присутствуют как полезный сигнал, так и задержанные в пределах конструктива радара копии сигнала передатчика. Хотя время задержки этих сигналов мало, по уровню они существенно превосходят полезный сигнал и при некоторых условиях, которые будут рассмотрены ниже, могут оказать существенное влияние на энергетические параметры радиоканала и в частности на соотношение сигнал/шум.

Такой шум называется декоррелированным фазовым шумом [2].

При определенных граничной величине связи между антеннами, времени задержки распространения сигнала по путям дополнительного приема, коэффициенте шума приемника и уровне фазового шума несущей передатчика на частоте отстройки, равной частоте полезного сигнала, на выходе преобразователя приемника мощность шума по дополнительному каналу приема и собственные шумы приемника становятся соизмеримы. Таким образом, за счет дополнительного канала приема создаются условия, приводящие к уменьшению приведенного к входу приемника отношения сигнал/шум и тем самым к ограничению дальности действия радиолокатора. Следует отметить, что это ограничение не может быть преодолено за счет увеличения мощности передатчика, так как одновременно будет пропорционально увеличиваться мощность шума, создаваемая за счет дополнительного канала приема сигнала передатчика. В силу своей компактности, автомобильные радары миллиметрового диапазона, работающие как на большом расстоянии (Long-Range Radar), так и системы безопасности малой дальности (Short-Range Radar) имеют антенно-фидерную часть, выполненную в основном по микрополосковой технологии. На этой же плате размещается интегральная микросхема, например, AWR1243 фирмы Texas Instruments (рис. 2).

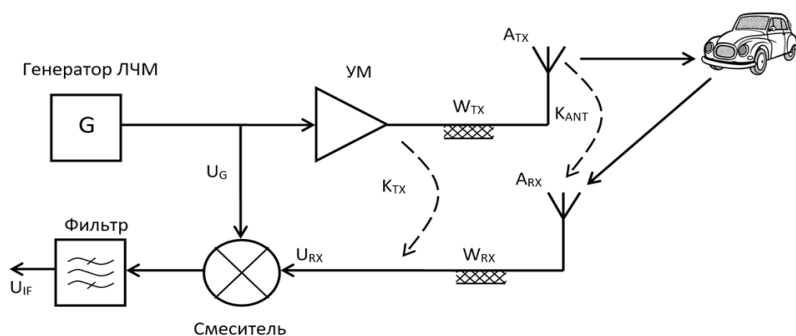


Рис. 1. Обобщенная схема преобразования сигналов в ЛЧМ радаре

Преобразование смесителем приемника сигнала, являющегося копией опорного колебания, при наличии в нем фазовых флуктуаций и при условии неполного совпадения по времени (т.е. при его задержке относительно опорного колебания) приводит к возникновению шума со спектральным составом, совпадающим с информационной полосой полезного выходного сигнала смесителя.

Она имеет 3 передатчика и 4 приемника, работающие в диапазоне частот 76–81 ГГц. Микрополосковые антенны формируют широкую диаграмму направленности в горизонтальной плоскости и относительно узкую в вертикальной плоскости. Показанная топология соответствует SRR радару.

Отмеченные выше эффекты проникновения паразитных сигналов на вход приемника,

ухудшающие соотношение сигнал/шум, влияют на предельную дальность обнаружения радара. В связи с этим актуальным является анализ параметров дополнительного канала распространения сигнала в конструкции приемо-передатчика радара.

Декоррелированный фазовый шум является результатом преобразования в смесителе приемника задержанного сигнала передатчика и в явной форме не присутствует на входе приемника. Однако, этот шум, также как и собственные шумы приемника, измеренные на промежуточной частоте, может быть пересчитан к входу приемника с учетом коэффициента передачи смесителя и установленных перед ним каскадов.

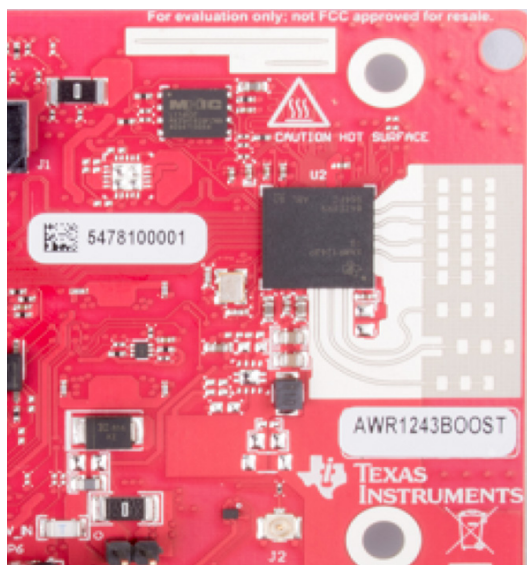


Рис. 2. Топология антенно-фидерной системы радара миллиметрового диапазона

Исходя из приведенной на Рис.1 схемы преобразования сигналов в радиоканале автомобильного радара, и в предположении, что преобразователь приемника имеет единичный коэффициент передачи для полезного сигнала, отношение сигнал/шум, приведенное к входу приемника, будет определяться выражением:

$$\left(\frac{P_C}{P_{\text{ш}} \right)_{\text{вх}}} = \frac{P_C}{(N_{\text{RX}} + L_{\text{TX}} + L_{\text{Ant}})F}, \quad (1)$$

где P_C – мощность полезного сигнала на входе приемника;

$N_{\text{RX}} = N_0 K_{\text{ш}}$ – спектральная плотность мощности собственных шумов приемника, приведенная к его входу (при условии его согласования с источником сигнала);

$K_{\text{ш}}$ – коэффициент шума приемника;

$N_0 = k T_0$ – спектральная плотность мощ-

ности шума нешумящего приемника, приведенная к его входу и при условии его согласования по сопротивлению с источником сигнала;

$k = 1,38 \cdot 10^{-23}$ Дж/К – постоянная Больцмана; $T_0 = 290$ К;

L_{TX} – спектральная плотность декоррелированного фазового шума, возникающего на выходе смесителя при прямом прохождении сигнала передатчика на вход приемника по цепи микросхемы, приведенная к входу приемника;

L_{Ant} – спектральная плотность декоррелированного фазового шума, возникающего на выходе смесителя при прохождении сигнала передатчика на вход приемника по цепи антенн, приведенная к входу приемника;

F – шумовая полоса канала приема.

На практике для системы с ЛЧМ, как следует из [2], [3], выполняется следующее соотношение для спектральных плотностей мощности шума, приведенных к входу приемника:

$$L_{\text{TX}} \ll N_{\text{RX}}. \quad (2)$$

В [2] приведено расчетное выражение, применимое к системам с ЛЧМ, для оценки спектральной плотности мощности декоррелированного фазового шума на выходе преобразователя приемника:

$$L_{\text{IF}}(f) = L_{\text{TX}}(f) \cdot 4 \sin^2(\pi f \tau), \quad (3)$$

где обозначено IF (Intermediate Frequency) – разностная (промежуточная) частота;

τ – время задержки сигнала по цепи выход синтезатора передатчика – вход смесителя;

$L_{\text{IF}}(f)$, $L_{\text{TX}}(f)$ – спектральные плотности фазового шума соответственно на выходах передатчика и смесителя приемника;

f – частота отстройки от несущей частоты генератора.

Параметр $L_{\text{TX}}(f)$ и параметр τ в выражении (3) предполагаются частотно-независимыми для заданных рабочих частот ЛЧМ сигнала. Расчет АЧХ и ФЧХ цепи связи между антеннами (частотной зависимости коэффициента $S_{21}(\omega)$ матрицы рассеяния), сделанный с помощью программы AWR Design Environment, а затем расчет группового времени запаздывания для антенной цепи показывает, что это условие во всем диапазоне частот строго не выполняется. Поэтому далее предполагается, что полученные с помощью формулы (3) данные строго применимы для расчета отношения сигнал/шум по формуле (1) только для ЛЧМ сигнала, спектр которого расположен в частотном диапазоне со слабой зависимостью $\tau(\omega)$ от частоты. С учетом

этих замечаний и принятых выше условий преобразования сигналов, показанных в схеме на Рис. 1, для фазового шума, приведенного к входу приемника и определяемого прохождением задержанного сигнала передатчика через электромагнитную связь антенн выражение (3) примет вид:

$$L_{\text{Ant}}(\omega, f) = K_{\text{ANT}}(\omega) L_{\text{TX}}(f) \cdot 4 \sin^2[\pi f \tau(\omega)], \quad (4)$$

где f – фиксированное значение отстройки от несущей, для которой определяется величина $L_{\text{TX}}(f)$;

$K_{\text{ANT}}(\omega)$ – модуль комплексного коэффициента передачи сигнала с выхода передатчика на вход приемника по цепи связи между антеннами.

Задержка огибающей высокочастотного колебания в линейном четырехполюснике и его ФЧХ связаны известным соотношением [4]:
 $\tau(\omega) = -d\Phi(\omega)/d\omega$,

где $\Phi(\omega)$ – фаза комплексного коэффициента передачи четырехполюсника (здесь им является цепь, состоящая из антенн передатчика, приемника и конструктивных элементов связи между ними).

Как следует из выражения (1), декоррелированный фазовой шум $L_{\text{Ant}}(f)$ при его соизмеримости с уровнем собственного шума приемника $N_0 K_{\text{ш}}$ необходимо учитывать при расчете отношения сигнал/шум, приведенного к входу приемника. Равенство $L_{\text{Ant}}(f) = N_0 K_{\text{ш}}$, при котором отношение сигнал/шум уменьшается на 3 дБ, определяет границу существенного влияния параметра $L_{\text{Ant}}(f)$ на предельную дальность обнаружения радара. При превышении $L_{\text{Ant}}(f)$ уровня собственного шума приемника теряет смысл увеличение мощности передатчика с целью увеличения отношения сигнал/шум.

Пример расчета уровня декоррелированного фазового шума по формуле (4) с учетом связи между антеннами передатчика и приемника приведен ниже. При расчете использованы данные для коэффициента шума и спектральной плотности фазового шума синтезатора микросхемы приемо-передатчика миллиметрового диапазона AWR1243 в диапазоне 77...81 ГГц [5]:

Коэффициент шума приемника 15 дБ;

Спектральная плотность мощности фазового шума сигнала передатчика при отстройке от несущей на 1 МГц – 93 дБн/Гц;

Мощность передатчика 13 дБм.

На основании приведенных параметров микросхемы AWR1243 для частоты отстройки $f = 1$ МГц получим спектральную плотность

мощности собственных шумов приемника, приведенную к его входу, $N_{\text{RX}} = -159$ дБм/Гц, спектральную плотность декоррелированного фазового шума, возникающего на выходе смесителя при прямом прохождении сигнала передатчика на вход приемника по цепи микросхемы, приведенную к входу приемника $L_{\text{TX}} = -80$ дБм/Гц.

В разработанном макете на материале Rogers R3003 толщиной 0,127 мм микрополосковая антенная система соединяется с выходом передатчика и входом приемника с помощью копланарных линий W_{TX} и W_{RX} . Их длина составила $l = 25$ мм, погонное затухание на рабочей частоте $\alpha = 35$ дБ/м, фазовая скорость в фидерных линиях $v = 1,73 \cdot 10^8$ м/с. С учетом этих данных и при условии согласования с антеннами по сопротивлению линии передачи внесут дополнительное затухание в цепь связи между приемником и передатчиком $A_i = 2l\alpha$, что составляет 1,8 дБ, и дополнительную задержку сигнала $\tau_i = 2l/v$, равную 0,29 нс.

На рис. 3 показана частотная зависимость коэффициента передачи между приемной и передающей антеннами с учетом потерь и фазовой задержки в соединительных линиях. Графики представлены для антенн, излучающих в открытое пространство, и антенн, находящихся под диэлектрическим укрытием толщиной 3,3 мм из диэлектрика с относительной проницаемостью $\epsilon = 3,0$.

Наличие антенного укрытия, хотя и оптимизированного на максимальный коэффициент усиления антенны, вызывает заметный рост взаимного влияния приемной и передающей антенн. За счет сложной картины распространения электромагнитных волн под антенным укрытием время задержки сигнала испытывает существенные изменения. Это, в свою очередь, заметно влияет на спектральную плотность декоррелированного фазового шума, возникающего на выходе смесителя при прохождении сигнала передатчика на вход приемника по цепи антенн, приведенную к входу приемника (рис. 4).

На приведенных графиках $N_{\text{ш RX}}$ соответствует собственному тепловому шуму приемника, графики L_{Ant} с укрытием и без укрытия показывают частотную зависимость спектральной плотности декоррелированного фазового шума, возникающего на выходе смесителя при прохождении сигнала передатчика на вход приемника по цепи антенн, приведенную к входу приемника, для антенной системы радара без диэлектрического

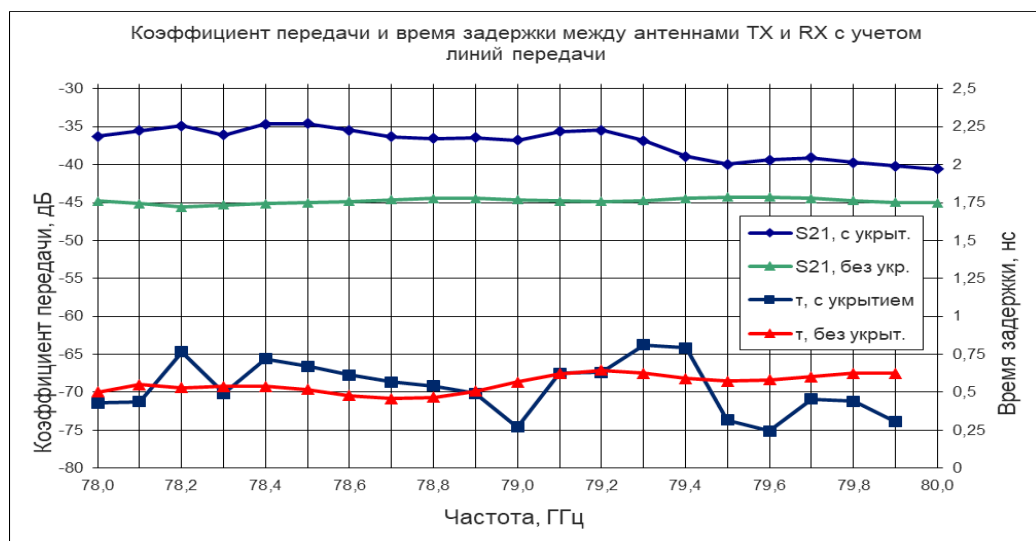


Рис. 3. Частотная зависимость коэффициентов передачи и группового времени запаздывания сигнала по цепи, образованной приемной и передающей антеннами с учетом потерь (1,8 дБ) и задержки (0,29 нс) в согласованных с ними линиях передачи

укрытия и при его наличии. Графики построены для спектральной плотности декоррелированного фазового шума, возникающего на выходе смесителя при прямом прохождении сигнала передатчика на вход приемника по цепи микросхемы, приведенной к входу приемника $L_{TX} = -80$ дБм/Гц. Частота отстройки от несущей составляет 1 МГц.

Проведенный анализ позволил сделать следующие выводы.

1. Антенное укрытие оказывает влияние на модуль и фазу коэффициента передачи цепи связи между антеннами приемника и передатчика. В полосе частот 78...80 ГГц связь между антеннами на некоторых участках рабочей полосы увеличивается на 10 дБ по сравнению с системой без укрытия. Искажение ФЧХ приводит к увеличению задержки до 0,75 нс (с учетом за-

держки в линиях подключения, равной 0,29 нс). По этим причинам уровень декоррелированного фазового шума в некоторых ограниченных областях заданного частотного диапазона становится соизмерим с уровнем собственных шумов приемника. Если доля этих областей в полной полосе сигнала мала, существенного влияния на отношение сигнал/шум приемника радара антенное укрытие оказывать не должно.

2. Расчет показывает, что задержка сигнала по цепи связи между антеннами и в линиях их подключения к приемо-передатчику в рассматриваемом примере оказываются соизмеримыми (около 0,3 нс). Поэтому одним из методов уменьшения уровня фазового шума (что может потребоваться при наращивании мощности передатчика) является сокращение длин линий подключения антенн.

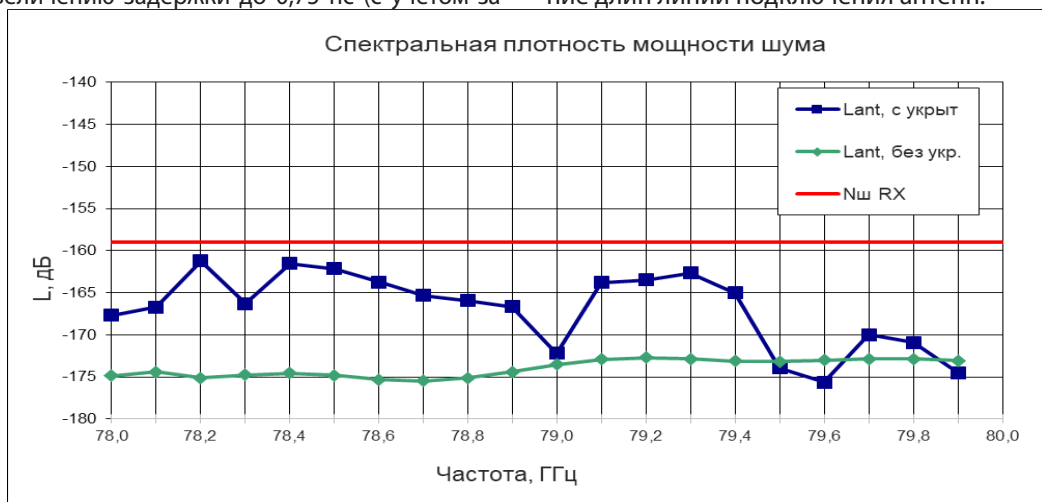


Рис. 4. Частотная зависимость спектральной плотности мощности шума, приведенной к входу согласованного с антенной приемника

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации в рамках соглашения № 075-11-2019-052 от 13.12.2019 с Научно-производственным объединением автоматики имени академика Н.А. Семихатова (АО «НПО автоматики») по комплексному проекту «Создание высокотехнологичного производства высокочастотного радара, предназначенного для использования в составе ин-

теллектуальных систем помощи водителю, систем автоматического управления беспилотных транспортных средств и систем интеллектуального земледелия» при участии ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина» (ФГАОУ ВО «УрФУ») в части выполнения научно-исследовательских, опытно-конструкторских и технологических работ.

Литература

1. Савашинский И.И., Астрцов Д.В. Скрытное устройство радиоэлектронного подавления измерителей скорости движения транспортных средств и методы радиоэлектронной защиты // Вестник УрФО. Безопасность в информационной сфере. – 2018. - № 2(28). – С. 11 – 15.
2. Siddiq K., Hobden M. K., Pennock S. R., Watson R. J. Phase Noise in FMCW Radar Systems // Transactions on Aerospace and Electronic Systems. 2019. – N 1(55). – P. 70 – 81.
3. Melzer A., Starzer F., Jäger H., Huemer M. On-Chip Delay Line for Extraction of Decorrelated Phase Noise in FMCW Radar Transceiver MMICs // Proceedings of the 23rd Austrian Workshop on Microelectronics (Austrochip 2015). 2015. – P. 31 – 35.
4. Баскаков С.И. Радиотехнические цепи и сигналы. – М.: Высшая школа, 1983. – 536 с.
5. AWR1243 Single-Chip 77– and 79–GHz FMCW Transceiver // Texas Instruments. 2019. [Электронный ресурс]. URL: <https://www.ti.com>.

References

1. Savashinskiy I. I., Astrecov D. V. Skrytnoe ustroystvo radioelektronnogo podavleniya izmeritelei skorosti dvizheniya transportnykh sredstv i metody radioelektronnnoi zashchity [Vehicles speed measurement systems radio–electronic repression secretive device and radio–electronic protection methods] // Vestnil UrFO. Bezopasnost v informatsionnoi sfere [Journal of the Ural Federal District Information Security]. – 2018. - N2(28). – P. 11 – 15.
2. Siddiq K., Hobden M. K., Pennock S. R., Watson R. J. Phase Noise in FMCW Radar Systems // Transactions on Aerospace and Electronic Systems. 2019. – N 1(55). – P. 70 – 81.
3. Melzer A., Starzer F., Jäger H., Huemer M. On-Chip Delay Line for Extraction of Decorrelated Phase Noise in FMCW Radar Transceiver MMICs // Proceedings of the 23rd Austrian Workshop on Microelectronics (Austrochip 2015). 2015. – P. 31 – 35.
4. Baskakov S. I. Radiotekhnicheskies tsepi i signaly [Radio technical Circuits and Signals] – M.: Vysshiaia shkola, 1983. – 536 p.
5. AWR1243 Single-Chip 77– and 79–GHz FMCW Transceiver // Texas Instruments. 2019. URL: <https://www.ti.com>.

ПЛОХОВ Сергей Николаевич, ведущий инженер департамента радиоэлектроники и связи Уральского федерального университета. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: s.n.plohov@urfu.ru

ШАБУНИН Сергей Николаевич, доктор технических наук, доцент, заведующий кафедрой радиоэлектроники и телекоммуникаций Уральского федерального университета. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: s.n.shabunin@urfu.ru

PLOHOV Sergey Nikolayevich, Leading Engineer of the Department of radio electronics and communications, Ural Federal University. 620002, Ekaterinburg, Mira Str., 19. E-mail: s.n.plohov@urfu.ru

SHABUNIN Sergey Nikolayevich, Doctor of Technical Sciences, Associate Professor, Head of the Department of radio electronics and telecommunications, Ural Federal University. 620002, Ekaterinburg, Mira Str., 19. E-mail: s.n.shabunin@urfu.ru



ОСОБЕННОСТИ ПРИМЕНЕНИЯ ПОЛНОМОЧНОЙ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА В СОВРЕМЕННЫХ СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В статье рассмотрены особенности эксплуатации полномочной модели разграничения доступа в средствах защиты информации (СЗИ) от несанкционированного доступа (НСД), влияющие на её эффективность. Проведен анализ некоторых недостатков средств защиты и возможные сценарии, позволяющие нарушителю получить доступ к данным в обход действующей модели. Предложены меры по противодействию НСД и способы их применения, обеспечивающие устранение обнаруженных недостатков СЗИ. Сделан обоснованный вывод о необходимости целенаправленного анализа политик настройки СЗИ от НСД и, при необходимости, их пересмотра в сторону ужесточения.

Ключевые слова: разграничение доступа, СЗИ от НСД, несанкционированный доступ, Secret Net Studio, Страж NT, полномочная модель, мандатная модель, уязвимость, защитные механизмы, альтернативные потоки данных, аппаратный модуль доверенной загрузки, безопасный режим ОС.

THE FEATURES OF MANDATORY ACCESS CONTROL MODEL IN MODERN UNAUTHORIZED ACCESS DATA PROTECTION TOOLS

This article describes the features of mandatory access control model in unauthorized access data protection tools, which can affect its efficiency. Also, some flaws of unauthorized access data protection tools and possible scenarios of unauthorized access bypassing these tools are analyzed. The countermeasures and methods of its application, eliminating detected flaws are offered. The conclusions about necessity of analyze of unauthorized access data protection tools policies and revision of its severeness, if it is necessary, were made.

Keywords: access control, SZI from NSD, unauthorized access, Secret Net Studio, Guardian NT, authoritative model, mandatory model, vulnerability, protective mechanisms, alternative data streams, hardware trusted boot module, safe mode OS.

При работе с данными, требующими полномочного разграничения доступа, применяются те или иные защитные механизмы, которые призваны обеспечить доступность защищаемых файлов и каталогов только для пользователей, работающих в системе с уровнем допуска, соответствующим метке доступа защищаемого ресурса. Используемые при этом защитные механизмы являются компонентами операционной системы (ОС) или частью специального программного обеспечения (СПО). Полномочная модель разграничения доступа реализована, например, в отечественной ОС специального назначения Astra Linux [1], а также в отечественных средствах защиты от НСД (например, Secret Net Studio [2], Dallas Lock [3], Страж NT [4] и др.).

Однако оказывается, что в ряде случаев даже правильно настроенная модель разграничения доступа не способна обеспечить надёжную и эффективную защиту от НСД к данным пользователя, не обладающего необходимыми полномочиями, поскольку защитные механизмы как дискреционной, так и полномочной системы разграничения доступа могут быть нарушены с помощью специальных действий, предпринятых со стороны пользователя. В этой связи разработка подходов,

обеспечивающих надёжную защиту от НСД, является актуальной.

В статье обсуждается способ защиты от НСД, основанный на комплексном использовании механизмов безопасности ОС и средств защиты.

Для обоснования актуальности темы исследования, на примере Secret Net Studio, рассмотрим некоторые компьютерные системы и сценарии поведения злоумышленника, в которых современные сертифицированные средства защиты от НСД, представленные в соответствующем сегменте рынка СПО, оказываются неэффективными.

1. Компьютер, в котором отсутствует аппаратный модуль доверенной загрузки, или он был извлечён злоумышленником. Здесь злоумышленник имеет возможность реализовать загрузку ОС с внешнего носителя (параметр UEFI в BIOS), что даёт неограниченный доступ к незашифрованным данным, хранящимся на жестком диске, так как все атрибуты безопасности файлов и каталогов в случае неактивной системы защиты будут игнорироваться. Это становится возможным, поскольку используемый для защиты доступа к BIOS и изменению его настроек пароль оказывается достаточно просто сбросить [5].

Более эффективным решением для обсуждаемой системы является механизм защиты диска, реализованный в ряде СЗИ от НСД, суть которого заключается в модификации системных структур диска (например, MBR и/или BR). В этом случае злоумышленник не может получить доступ к файлам и каталогам, так как загружаемая ОС не может распознать на диске разделы и файловые системы на них. Однако злоумышленник имеет возможность сделать побайтную копию всего жесткого диска и далее восстановить данные с образа жесткого диска, используя автоматизированные утилиты, например, RStudio или Easy Recovery.

Отметим, что интеграция аппаратного модуля доверенной загрузки с СЗИ от НСД, не позволяющая злоумышленнику пройти аутентификацию в ОС при извлеченной плате защиты, не исключает возможность загрузки с внешнего носителя.

В этой связи, по-видимому, единственной по настоящему эффективной защитой является шифрование критичных данных на жестком диске, что делает доступ и/или съём информации с диска бесполезным.

2. Получение злоумышленником прав локального администратора компьютерной системы, которые он может получить несколькими способами. Во-первых, при наличии физического доступа к системе и возможности загрузки с внешнего носителя злоумышленник может сбросить пароль на встроенной учётной записи администратора или на любой другой учётной записи с правами администратора, а так же назначить полномочия администратора системы любой учётной записи. Более того, злоумышленник способен скопировать файлы базы учётных данных пользователей Windows и выполнить подбор пароля по хэшу, хранящемуся в этой базе, и тем самым узнать пароль администратора системы, не сбрасывая его. Во-вторых, злоумышленник может использовать уязвимость системного или прикладного ПО, которое своевременно не было обновлено. Для этого используются вредоносные программы, содержащие данные или исполняемый код, которые способны воспользоваться одной или несколькими уязвимостями используемого ПО на локальном или удаленном компьютере (эксплойты) и получить права администратора компьютерной системы. Получив права администратора, злоумышленник становится спо-

собным управлять защитными механизмами СЗИ от НСД, включать и отключать модули защиты (отметим, что ряд СЗИ от НСД имеют механизм самозащиты с сервисным паролем, который не позволит отключить или удалить СЗИ администратором, не знающим данный пароль). В случае развёртывания средства защиты с централизованным управлением, о манипуляциях злоумышленника по отключению средства защиты станет известно на сервере при анализе журналов событий СЗИ от НСД. Однако, имея права администратора системы, существует возможность обращаться к защищаемым ресурсам напрямую, в обход механизмов защиты, и соответственно, без ведения записей в журналах СЗИ. Для этого злоумышленник может использовать специализированное ПО, обеспечивающее прямой доступ к диску – так называемые HEX-редакторы или шестнадцатеричные редакторы.

Для подтверждения данного утверждения рассмотрим модель компьютерной системы, в которой используется одно из популярных сегодня СЗИ от НСД Secret Net Studio 8. В изучаемой системе авторами были созданы три пользователя: User1, User2 и Администратор. Пользователь User1 имел максимальный уровень допуска – «строго конфиденциально», пользователь User2 – «не конфиденциально» и права администратора. Пользователь User1 создал файл text.txt, в котором разместил текст следующего содержания: «Строго конфиденциальное содержимое файла» и присвоил значению метки доступа к файлу «строго конфиденциально». Рабочее окно шестнадцатеричного редактора, в котором пользователь User2, имеющий права администратора и работающий в режиме «не конфиденциально», представлено на рис. 1.

Из рис. 1 видно, что в шестнадцатеричном редакторе оказалось доступным содержимое файла с меткой доступа «строго конфиденциально». При этом в журналах используемого СЗИ от НСД имеется запись о факте запуска пользователем User2 шестнадцатеричного редактора, однако, каких-либо записей о факте доступа к защищенному конфиденциальному файлу с помощью использованного редактора каких-либо записей обнаружить не удалось.

Исключить возникновение описанной ситуации можно, если использовать специальную настройку изолированной программной среды, включающую в себя составление спи-

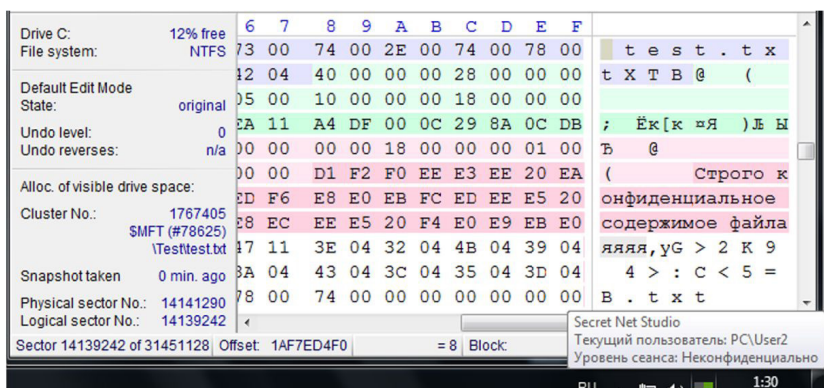


Рис. 1. Демонстрация доступа к содержимому файла с максимальным уровнем конфиденциальности

ска процессов, которые данный субъект может порождать [6]. В этой ситуации субъект (пользователь компьютерной системы) не сможет запустить стороннее ПО. Также целесообразно использовать двухфакторную аутентификацию, так как в данном случае, даже зная пароль локального администратора, злоумышленник не сможет пройти аутентификацию.

3. Загрузка компьютерной системы в безопасном режиме. В безопасном режиме компоненты системы защиты компьютерной системы не загружаются, что позволяет злоумышленнику получать доступ к закрытой информации (рис. 2).

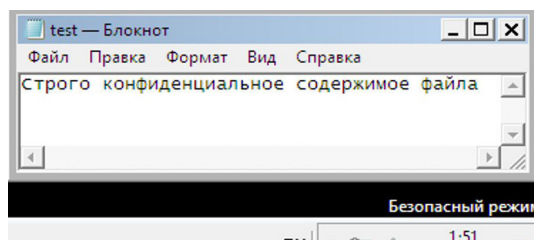


Рис. 2. Доступ к строго конфиденциальному файлу из безопасного режима

С нашей точки зрения, наиболее эффективное решение, позволяющее избежать обсуждаемой ситуации, состоит в запрещении запуска системы в безопасном режиме, которая реализуется редактированием некоторых разделов реестра ОС Windows. Отметим, что штатными механизмами администрирования ОС реализовать данное решение затруднительно.

4. Использование недостатков собственно СЗИ от НСД, к которым следует отнести ряд особенностей работы полномочной системы разграничения доступа, которыми может воспользоваться злоумышленник для извлече-

ния части содержимого строго конфиденциального документа и далее его сохранении с понижением метки конфиденциальности. Проиллюстрируем данный недостаток следующим примером. В модели компьютерной системы установлено одно из популярных на рынке СЗИ от НСД (например, Secret Net Studio 8), полномочная модель которого позволяет создавать неконфиденциальные папки в неконфиденциальных расположениях в строго конфиденциальном режиме. Здесь злоумышленник, имеющий права доступа «строго конфиденциально» может открыть обсуждавшийся выше файл test.txt и скопировать его содержание, далее создать неконфиденциальную папку в неконфиденциальном разделе и вставить в ее название содержимое файла test.txt, имеющего метку конфиденциальности «строго конфиденциально» (рис. 3).

Из рис. 3 видно, что злоумышленнику с уровнем допуска в системе «строго конфиденциально», работающему в строго конфиденциальном режиме, удалось вставить в название неконфиденциальной папки, расположенной в неконфиденциальном расположении, и сохранить содержимое строго конфиденциального текстового документа. Разумеется, возможность такой операции ограничено 256 символами имени папки. Однако данное ограничение не снимает описанных выше проблем безопасности информации. Кроме того, злоумышленник вместо одной папки может создать множество папок данного типа. Также обойти ограничение в 256 символов злоумышленник может путём использования командной строки и записи скопированного текста из строго конфиденциального документа в альтернативный поток данных неконфиденциального каталога (рис. 4).

Из рис. 4 видно, что в неконфиденциаль-

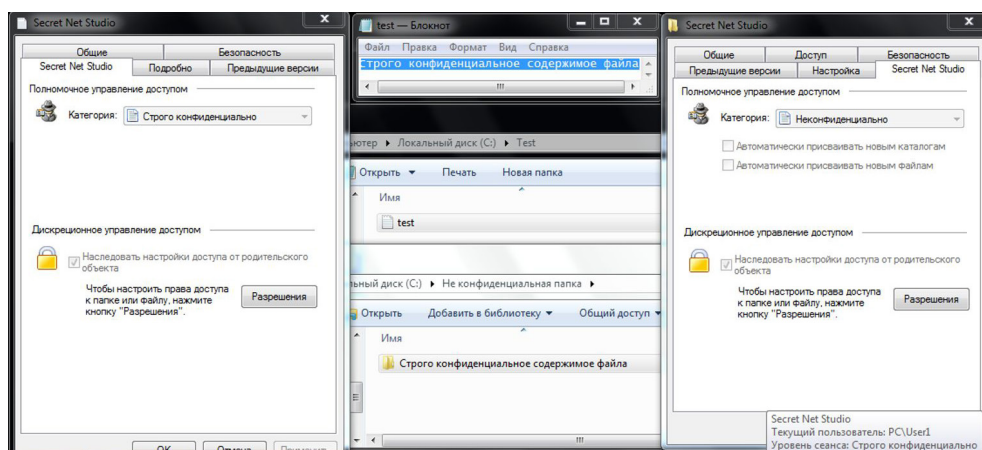


Рис. 3. Возможность понижения категории данных в строго конфиденциальном режиме работы

ном каталоге действительно удастся создать альтернативный поток данных с именем ADS объёмом 45 байт, содержащий текст строго конфиденциального документа. При этом объём записываемого текста ограничен только возможностями командной строки. Данный каталог впоследствии может быть скопирован в неконфиденциальном режиме работы на носитель с файловой системой NTFS без потери данных в альтернативном потоке. При копировании или перемещении файла из одного NTFS-раздела в другой NTFS-раздел потоки сохраняются, и ОС никак не сигнализирует об их присутствии [7]. Кроме того, другой пользователь, работающий в неконфиденциальном режиме, может вывести содержимое альтернативного потока данных на экран (рис. 5).

Для пользователей данного СЗИ мы рекомендуем ограничить с помощью дискреционной модели создание и переименование папок в любых директориях (включая корневую), кроме тех, на которые реализовано перенаправление. В этом случае утечка информации вышеописанным способом будет исключена. Однако это может вызвать сбои в работе прикладного и системного ПО. Кроме этого, в целях обеспечения безопасности, пользователям необходимо запрещать доступ к командной строке и к запуску командных файлов «bat».

В целом, принимая во внимание вышеизложенное, мы считаем, что полномочная модель разграничения доступа будет работать эффективно, и СЗИ от НСД будут обеспечи-

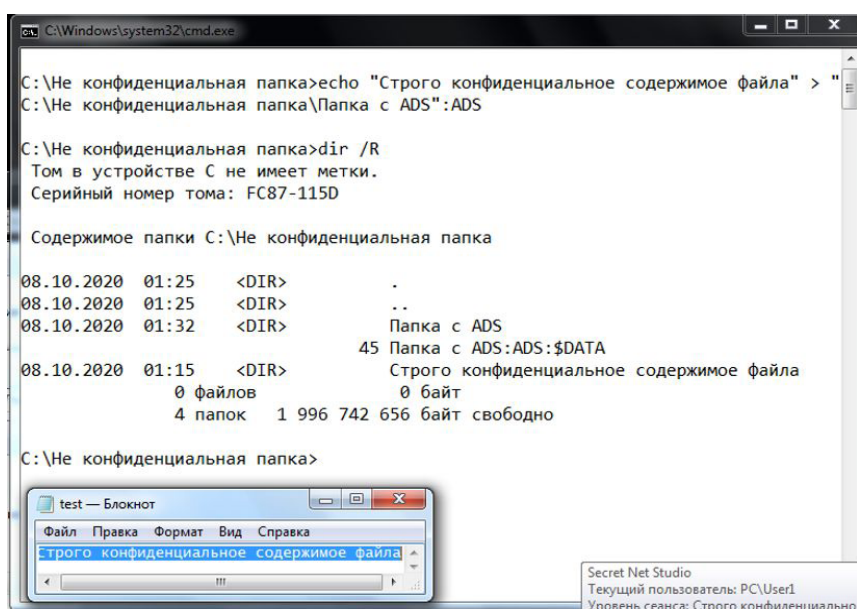


Рис. 4. Сохранение данных в альтернативном потоке

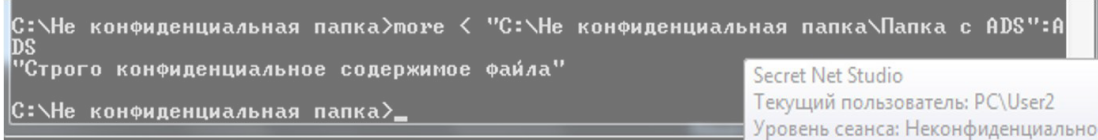


Рис. 5. Доступ к ADS в не конфиденциальном режиме

вать надёжную защиту данных только в случае использования комплексного, грамотного и неформального подхода к реализации защитных механизмов СЗИ. Для этого настройку средства защиты необходимо проводить с учётом специфики данного СЗИ от НСД, ОС, а также аппаратной части компью-

терной системы, на которой оно применяется. Для исключения возможности несанкционированного доступа к данным во многих случаях требуется пересмотреть требования, применяемые при настройке средств защиты информации в компьютерных системах, в сторону их ужесточения.

Литература

1. Операционная система специального назначения «Astra Linux Special Edition» Руководство администратора. Часть 1. [Электронный ресурс] URL: <https://astralinux.ru/products/astra-linux-special-edition/documents-astra-se/rukovodstvo-administratora-chast-1-astra-se.pdf>
2. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Локальная защита. [Электронный ресурс] URL: <https://www.securitycode.ru/upload/iblock/6fe/Руководство администратора. Настройка и эксплуатация. Локальная защита.pdf>
3. Система защиты информации от несанкционированного доступа Dallas Lock 8.0 Руководство по эксплуатации. [Электронный ресурс] URL: <https://www.dallaslock.ru/upload/medialibrary/cp/documents/С ИК5 2017/RU.48957919.501410-02 92 Руководство по эксплуатации.pdf>
4. Страж NT. Система защиты информации от несанкционированного доступа. Руководство администратора. [Электронный ресурс] URL: https://guardnt.ru/doc/gnt_40_admin_guide.pdf
5. Духан Е.И., Синадский Н.И., Хорьков Д.А. Применение программно-аппаратных средств защиты компьютерной информации: учебное пособие. — 3-е изд., перераб. и доп. — Екатеринбург: УрФУ, 2013. — 240 с.
6. Проскурин, В.Г. Защита в операционных системах: учеб. пособие для вузов / В.Г. Проскурин. — М.: Горячая линия – Телеком, 2014. — 193 с.: ил.
7. Анализ и восстановление данных на носителях с файловой системой NTFS: учебное пособие / Н. И. Синадский; научный редактор канд. техн. наук, доц. В.В. Бакланов. Екатеринбург: ГОУ ВПО УГТУ–УПИ, 2007. — 136 с.

References

1. Operacionnaja sistema special'nogo naznachenija «Astra Linux Special Edition» Rukovodstvo administratora. Chast' 1. [Jelektronnyj resurs] URL: <https://astralinux.ru/products/astra-linux-special-edition/documents-astra-se/rukovodstvo-administratora-chast-1-astra-se.pdf>
2. Sredstvo zashhity informacii Secret Net Studio. Rukovodstvo administratora. Nastrojka i jekspluatacija. Lokal'naja zashhita. [Jelektronnyj resurs] URL: <https://www.securitycode.ru/upload/iblock/6fe/Rukovodstvo administratora. Nastrojka i jekspluatacija. Lokal'naja zashhita.pdf>
3. Sistema zashhity informacii ot nesankcionirovannogo dostupa Dallas Lock 8.0 Rukovodstvo po jekspluatácii. [Jelektronnyj resurs] URL: <https://www.dallaslock.ru/upload/medialibrary/cp/documents/S ИК5 2017/RU.48957919.501410-02 92 Rukovodstvo po jekspluatácii.pdf>
4. Strazh NT. Sistema zashhity informacii ot nesankcionirovannogo dostupa. Rukovodstvo administratora. [Jelektronnyj resurs] URL: https://guardnt.ru/doc/gnt_40_admin_guide.pdf
5. Duhan E.I., Sinadskij N.I., Hor'kov D.A. Primenenie programmno-apparatnyh sredstv zashhity komp'juternoj informacii: uchebnoe posobie. — 3-e izd., pererab. i dop. — Ekaterinburg: UrFU, 2013. — 240 s.
6. Proskurin, V.G. Zashhita v operacionnyh sistemah: ucheb. posobie dlja vuzov / V.G. Proskurin. — M.: Gorjachaja linija – Telekom, 2014. — 193 s.: il.
7. Analiz i vosstanovlenie dannyh na nositeljah s fajlovoj sistemoj NTFS: uchebnoe posobie / N. I. Sinadskij; nauchnyj redaktor kand. tehn. nauk, doc. V.V. Baklanov. Ekaterinburg: GOU VPO UGTU–UPI, 2007. — 136 s.

КУЦ Дмитрий Владимирович, старший преподаватель Учебно-научного центра «Информационная безопасность» Уральского федерального университета имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: d.v.kutc@urfu.ru

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» Уральского федерального университета имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: s.v.porshnev@urfu.ru

KUTS Dmitry Vladimirovich, senior teacher of the Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: d.v.kutc@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Full Professor, Head of Unit, Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: s.v.porshnev@urfu.ru

РАЗРАБОТКА ИЗБИРАТЕЛЬНОЙ МУЛЬТИБИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Данная работа посвящена разработке избирательной мультibiометрической аутентификации. Новизна работы заключается в разработке нового подхода к мультibiометрической аутентификации. В зависимости от доступности и удобства использования датчиков, от устойчивости к атакам, от болезней или травм пользователей могут быть выбраны любые биометрические характеристики, такие как ритм пароля, голос, динамическая подпись, графический пароль и т.д. В работе представлены результаты разработки избирательной мультibiометрической аутентификации на основе нового подхода.

Ключевые слова: биометрия, мультibiометрия, мультibiометрическая аутентификация, биометрические технологии, управление доступом, информационная безопасность.

Ruchay A. N.

DEVELOPMENT OF NEW ELECTIVE MULTIBIOMETRIC AUTHENTICATION

The purpose of this work is the development of elective multibiometric authentication. The novelty of the work is to develop a new approach to multibiometric authentication. Depending on the availability and usability of sensors, from resistance to attacks, from diseases or injuries of users, any biometric characteristics can be selected, such as password rhythm, voice, dynamic signature, graphic password, etc. The paper presents the results of the development of elective multibiometric authentication based on a new approach.

Keywords: biometrics, multibiometrics, multibiometric authentication, biometric technologies, access control, managing permissions.

1. Введение

В биометрических системах аутентификации на основе одной биометрической характеристике существуют следующие проблемы [1]:

- Шум в считываемых данных (скопление грязи на датчике, деформированные и зашумленные данные, изменившийся под влиянием холода голос, возможное изменение радужной оболочки глаза под влиянием оч-

ков, изменившиеся под влиянием освещенности характеристики лица).

- Не уникальность (внутриклассовые вариации и межклассовое сходство).

- Не универсальность (невозможность использования биометрических характеристик, низкое качество и непротиворечивость полученных биометрических данных, взаимодействие пользователя с датчиком).

- Атаки с обманом.

Разработчики и исследователи обычно предлагают системы аутентификации, использующие одну биометрическую характеристику и один датчик [2], что создает проблемы в использовании и угрозы в безопасности [3]. Однако современные тенденции заставляют использовать другой подход – мультибиометрическую аутентификацию [4], основное преимущество которой состоит в повышении безопасности [5].

Мультибиометрическая аутентификация позволяет использовать несколько биометрических характеристик и датчиков, которые могут быть интегрированы на разных уровнях и могут использоваться в различных сочетаниях [6]. Биометрические характеристики могут обрабатываться различными методами или комбинироваться для мультибиометрической аутентификации. Решение может быть принято на основе объединенного решающего правила, что повышает надежность.

Мультибиометрическая аутентификация имеет высокую безопасность, надежность и защиту от атак [4], для чего используются множество биометрических данных, множество биометрических образцов, множество правил принятия решений, множество методов нормализации или методов извлечения признаков. Однако повышение безопасности и надежности с помощью мультибиометрической аутентификации приводит к дополнительным требованиям к скорости обработки, к неудобствам пользователей и к проблемам с конфиденциальностью. Поэтому при разработке мультибиометрической аутентификации необходимо найти разумный компромисс между надежностью, безопасностью, вычислительными затратами и удобством пользователя. Этот компромисс можно достичь с помощью динамического управления безопасностью и надежностью на основе автоматических или полуавтоматических методов. Однако в работах очень мало внимания уделяется архитектуре, разработке, оценке надежности, безопасности и производительности в подходах динамического изменения безопасности. В разделе 2 данной статьи представлены различные подходы мультибиометрической аутентификации.

В этой статье был разработан подход избирательной мультибиометрической аутентификации, в котором динамически изменяется уровень безопасности путем выбора

различных параметров и биометрических характеристик. Предлагаемый подход к избирательной мультибиометрической аутентификации подробно описан в Разделе 3 данной статьи. В рамках предложенного подхода для управления доступом в помещении можно использовать аутентификацию на основе голоса, ритма пароля, клавиатурного подчерка или графического пароля [7, 8]. В другом случае аутентификация может быть выполнена на основе ритма пароля или подписи. Для аутентификации в мобильных устройствах можно применять ритм пароля, подпись или графический пароль. На контрольно-пропускных пунктах может использоваться аутентификация только на основе подписи.

2. Мультибиометрическая аутентификация

Мультибиометрическая аутентификация может использоваться для решения различных аспектов управления безопасностью, основная цель которой является повышение безопасности [4, 5].

Ниже приведены различные подходы к созданию мультибиометрических систем [1]:

- мультимодальность (для идентификации пользователя используется более одной биометрической характеристики).
- мультиалгоритмичность (к одному биометрической характеристики применяется несколько различных подходов для извлечения признаков и алгоритмов сопоставления).
- многоэкземпляльность (используется несколько экземпляров одной биометрической характеристики).
- мультисенсорность (информация одной и той же биометрии, полученной с разных сенсоров, объединяется в одну).
- мультивыборность (для регистрации и распознавания используются несколько образцов одной и той же биометрической характеристики).

Мультимодальность может быть реализовано в трех разных режимах [1]:

- Последовательный режим (каскадный режим) – каждая модальность проверяется перед исследованием следующей.
- Параллельный режим – считанные / захваченные данные из нескольких модальностей используются одновременно, а затем результаты объединяются для принятия окончательного решения.
- Иерархический режим – отдельные классификаторы объединяются в иерархию или древовидную структуру.

В мультибиометрической аутентификации существуют следующие различные уровни слияния: на уровне решения, итоговой оценки, характеристик и образцов. Для универсальности должны учитываться всевозможные подходы к реализации мультибиометрии с помощью слияния.

Существует три стратегии мультибиометрического слияния [9]:

- Пользовательская нормализация для мультибиометрического слияния. Например, в зависимости от качества входных образцов предлагаемый алгоритм разумно выбирает подходящий способ слияния для оптимальной эффективности [10].

- Критерий устойчивости для ранжирования пользователей по их эффективности. Он обеспечивает стабильно хорошую эффективность на разных базах данных, несмотря на отсутствие обучающих образцов. Коэффициент Фишера, коэффициент F и d -prime приведены в качестве примеров критериев в [9].

- Избирательная стратегия слияния. Поскольку не все биометрические характеристики должны быть работоспособными для каждой попытки, или необходимо выполнять аутентификацию независимо от устройств или попыток, в этом случае мы должны динамически выбирать соответствующий метод слияния.

В работе [11] была исследована схема динамического слияния динамических оценок для мультиалгоритмического распознавания путем включения качества данных.

В работе [12] авторы предлагают метод последовательного слияния, который использует тест-статистику отношения правдоподобия в сочетании с классификатором машины опорных векторов для учета ошибок. В зависимости от качества входных биометрических данных предлагаемый алгоритм динамически выбирает между различными классификаторами и правилами слияния для распознавания человека по выбранной биометрии.

В статье [13] представлены методы мультибиометрического слияния на ранговом уровне. Предлагаемые методы предлагаются для повышения эффективности схем слияния на уровне рангов при наличии слабых классификаторов или входных изображений низкого качества.

Мультибиометрическая аутентификация должна быть очень гибкой, чтобы учитывать различные требования и ограничения поль-

зователей. При этом она должна решать проблему отсутствия биометрических характеристик в результате низкого качества данных или невозможности предъявления, которая может быть решена с помощью использования других доступных биометрических характеристик. Кроме того, важно соблюдать требование необходимого уровня безопасности, что требует разработки различных динамических избирательных правил и методов мультибиометрического слияния.

В статье [14] описан эксперимент с несколькими простыми методами мультибиометрического слияния. Авторы [15] предложили интересный подход, который включает проведение непрерывной аутентификации. Этот подход требует длительного физического присутствия пользователя и поэтому не подходит для некоторых приложений и ситуаций.

В статье [16] предлагается использовать несколько уровней безопасности для мультибиометрической аутентификации с тремя биометрическими характеристиками (лицо, движение губ, голос). Когда требуемый уровень безопасности низкий, тогда достаточно принять решение на основании двух из трех биометрических характеристик. С другой стороны, для приложений с высоким уровнем безопасности требуется использования всех трех биометрических характеристик. Однако этот подход не позволяет изменять динамически уровень безопасности. Вместо этого администратор принимает решение, в котором должны использоваться конкретные зафиксированные биометрические характеристики.

В работе [17] предлагается сценарий динамического управления доступом в здании с разделением на разные зоны (это могут быть разные этажи или номера комнат) и определенные права доступа для каждого пользователя. Решение доступа в конкретной зоне также могут зависеть от решений, уже принятых в других зонах. Кроме того, количество биометрических характеристик, требуемых в каждой зоне, и различные правила могут варьироваться.

Другим аспектом разработки избирательной мультибиометрической аутентификации является обеспечение желаемой надежности и эффективности, а также выполнения пользовательских предпочтений, ограничений, удобства пользователей и возрастных изменений [18]. Уровень безопасности мультибио-

метрической аутентификации также должен быть скорректирован в зависимости от возможных атак, что требует динамических подходов изменения уровня безопасности.

В работе [19] представлен новый подход к адаптивному комбинированию нескольких биометрических характеристик для динамического обеспечения желаемого уровня безопасности. Работа [19] ориентирована на повышение эффективности и безопасности, хотя одна из ключевых проблем данного подхода связана с правильным выбором биометрических характеристик.

Таким образом, эта данная статья направлена на разработку подхода, в котором адаптивно выбирается набор биометрических характеристик из доступных для обеспечения желаемого уровня безопасности.

3. Избирательная мультибиометрическая аутентификация

В этой статье, в отличие от всех предыдущих работ [20], предлагается новый подход к разработке избирательной мультибиометрической аутентификации, где используется различные критерии выбора параметров и способов мультибиометрической аутентификации. Схема предлагаемой избирательной мультибиометрической аутентификации представлена на рис. 1, на котором показаны основные этапы избирательной мультибиометрической аутентификации, основанной на ритме пароля, голоса, динамической подписи и графического пароля. Этот подход можно использовать и с другими биометрическими характеристиками.

Самым важным блоком для данной схемы является блок полуавтоматических настроек, который выполняет перевод всех настроек и параметров, заданных администратором и пользователем на этапе обучения. В качестве параметров выступает полуавтоматический выбор: последовательности предоставления биометрической характеристики, сам набор биометрических характеристик, устройства ввода (сенсора), метода параметризации, метода сравнения, метода комбинации решения. Здесь под полуавтоматическим выбором понимается выбор метода слияния в виде заранее заданных жестких правил и критериев.

Перечислим базовые критерии и правила [20]:

1. Наличие необходимых устройств ввода (сенсоров);
2. Уровень безопасности (количество необходимых биометрических характеристик);

3. Выбор очередности предоставления биометрических характеристик;

4. Результат предыдущих попыток аутентификации;

5. Особенности данной зоны (комнаты, устройств);

6. Особенности пользователей и их предпочтения, возрастные ограничения;

7. Время прохождения аутентификации;

8. Степень угроз и вероятности атак на устройства ввода (сенсор);

9. Качество предоставляемых биометрических образцов.

Блок полуавтоматических настроек после задания всех настроек и параметров полуавтоматическим способом может выбрать необходимую решающую функцию в блоке комбинация решения $f_1(m1, m2, m3), \dots, f_k(m1, \dots, m4)$, где $m1, m2, m3, m4$ – результат сравнения каждой биометрической характеристики в отдельности, и выбрать необходимый порог принятия решения. В предлагаемом подходе параметры для гарантирования определенного уровня безопасности автоматически не подбираются, эта задача стоит для дальнейших исследований.

В предлагаемой нами избирательной мультибиометрической аутентификации есть 4 биометрических характеристики (голос, динамическая подпись, ритм пароля, графическое распознавание). Всевозможные подмножества из этих биометрий могут быть: $\{1, 2, 3, 4\}, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}$.

Каждый из 16 подмножеств описывает один из вариантов выбора биометрических характеристик в избирательной мультибиометрической аутентификации. Опишем алгоритм выбора комбинации биометрических характеристик в зависимости от уровня безопасности.

Пусть набор используемых биометрических характеристик определяется как $\{p_1, p_2, p_3, p_4\}$, где p_i – индекс использования биометрической характеристики i . Мы предполагаем, что критерии, влияющие на p_i , независимы, поэтому

$$p_i = \prod_{j=1}^k p_i^j,$$

где p_i^j – оценка фактора использования биометрической характеристики i с критерием j .

В данной работе были предложены следующие критерии j для каждой биометрической

ской характеристики i для предлагаемой избирательной мультибиометрической аутентификации:

1. $p^1 = \{0,1\}$ – коэффициент наличия необходимых входных датчиков, когда входной датчик доступен $p^1 = 1$, и когда входной датчик недоступен $p^1 = 0$.

2. $p^2 = [1,10]$ – коэффициент необходимого уровня безопасности. Администратор устанавливает этот коэффициент для каждой биометрической характеристики i . Например, для голосовой аутентификации $p^2 = 10$, для других биометрических характеристик (динамическая подпись, ритм пароля, графическое распознавание) соответственно $p^2 = 3,9,6$.

3. $p^3 = [1,10]$ – коэффициент использования атак на датчик. Администратор устанавливает эту вероятность для каждой биометрической характеристики i . Например, для голоса $p^3 = 3$ из-за высокого риска атак подделки, для других биометрических характеристик (динамическая подпись, ритм пароля,

горитм слияния для оптимальной эффективности [10, 11, 13].

5. $p^5 = [3,10]$ – коэффициент результата предыдущих попыток аутентификации. Этот коэффициент динамически оценивается. Например, $p^5 = d$, если последние d попытки не прошли аутентификацию.

6. $p^6 = [1,10]$ – коэффициент защищенности помещения (оборудования). Администратор устанавливает этот коэффициент для каждой биометрической характеристики i .

7. $p^7 = [0,1]$ – коэффициент предпочтений пользователя. Администратор устанавливает этот коэффициент для каждого пользователя. Например $p^7 = 0$, из-за возрастных ограничений или отсутствия биометрической характеристики, иначе $p^7 = 1$.

8. $p^8 = [0,10]$ – коэффициент времени на аутентификацию. Например $p^8 = 3$, для голоса из-за длительного процесса, для других биометрических характеристик (динамическая подпись, ритм пароля, графическое распознавание) соответственно $p^8 = 9,7,6$.

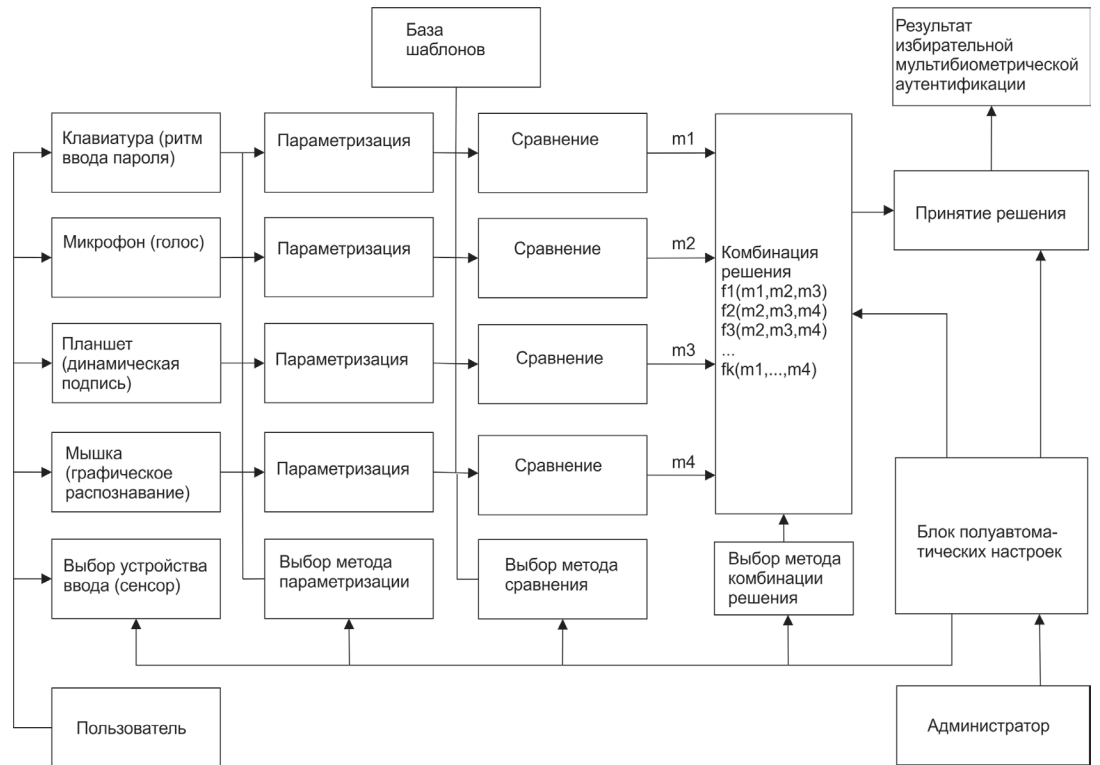


Рис. 1. Схема избирательной мультибиометрической аутентификации

графическое распознавание) соответственно $p^3 = 9,7,6$.

4. $p^4 = [0,1]$ – коэффициент качества биометрических образцов. В зависимости от качества входных выборок предлагаемый алгоритм динамически выбирает подходящий ал-

Опишем алгоритм выбора подмножества элементов для предложенной избирательной мультибиометрической аутентификации:

1. Оценим все значения $\{p_1, p_2, p_3, p_4\}$ для всех критериев p^i .

2. Сравним p_i с порогом $\alpha > 0$. Если

$p_i < \alpha$, то исключаем биометрию p_i . Администратор устанавливает порог α .

3. После того, как значения были оценены $\{p_1, p_2, p_3, p_4\}$, мы сортируем p_i .

4. Выбираем первые t , которые соответствуют высоким показателям p_i выбранной биометрической характеристики. Администратор устанавливает параметр t .

В предлагаемой нами избирательной мультибиометрической аутентификации в зависимости от доступности и удобства использования датчиков, от устойчивости к атакам, от болезней или травм пользователей могут быть выбраны любые биометрические характеристики, такие как ритм пароля, голос, динамическая подпись, графический пароль и т.д.

4. Заключение

В работе был разработан новый подход для избирательной мультибиометрической аутентификации. В этом подходе в отличие всех предыдущих работ предлагается различные критерии полуавтоматического выбора метода слияния и параметров мультибиометрической аутентификации. Однако существуют направления для дальнейшего развития избирательного подхода мультибиометрической аутентификации: применение других биометрических характеристик, обеспечение большей универсальности, увеличение эффективности и производительности, реализация динамического выбора параметров системы, в частности, метода слияния для гарантированного уровня безопасности.

Литература

1. Gad, R., El-Fishawy, N., El-Sayed, A., Zorkany, M.: Multi-Biometric Systems: A State of the Art Survey and Research Directions. *International Journal of Advanced Computer Science and Applications*, 2015, 6(6), P. 128–138.
2. Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., Senior, A. W.: *Guide to biometrics*. Springer-Verlag, New-York, 2003.
3. Dunstone, T., Yager, N.: *Biometric system and data analysis: design, evaluation, and data mining*. Springer, Boston, Ma, 2009.
4. Ross, A. A., Nandakumar, K., Jain A. K.: *Handbook of multibiometrics*. Springer, New York, 2006.
5. Bhanu, B., Govindaraju, V.: *Multibiometrics for Human Identification*. Cambridge University Press, Cambridge, 2011.
6. Sesin, E. M., Belov, V. M.: Personal identification system based on integration organization of several biometric characteristics of the person. *Proceedings of Tomsk State University of Control Systems and Radioelectronics* 2012, 2(25), 2, P. 175–179.
7. Асеев Г.Д., Рагозин А.Н. Определение минимального набора входных данных для корректной аутентификации по клавиатурному почерку с использованием нейронной сети // *Вестник УрФО. Безопасность в информационной сфере*. 2017. № 3(25). С. 19-23.
8. Иванов А.И., Сомкин С.А., Андреев Д.Ю., Малыгина Е.А. О многообразии метрик, позволяющих наблюдать реальные статистики распределения биометрических данных «нечетких экстракторов» при их защите наложением гаммы // *Вестник УрФО. Безопасность в информационной сфере*. 2014. № 2 (12). С. 16-23.
9. Poh, N., Ross, A., Lee, W., Kittler, J.: A user-specific and selective multimodal biometric fusion strategy by ranking subjects. *Pattern Recognition* 2013, 46, P. 3341–3357.
10. Vatsa, M., Singh, R., Noore, A.: Context Switching Algorithm for Selective Multibiometric Fusion. *Pattern Recognition and Machine Intelligence* 5909, Springer, 2009. P. 452–457.
11. Fathima, A., Vasuhi, S., Treesa, T., Babu, N.T., Vaidehi, V.: Person Authentication System with Quality Analysis of Multimodal Biometrics. *WSEAS transactions on information science and applications*.
12. Vatsa, M., Singh, R., Noore, A., Ross, A.: On the Dynamic Selection of Biometric Fusion Algorithms. *IEEE transactions on information forensics and security* 2010, 5(3). P. 470–479.
13. Abaza, A., Ross, A.: Quality Based Rank-Level Fusion in Multibiometric Systems. *Proc. of 3rd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2009.
14. Kittler, J., Hatef, M., Duin, R. P. W., Matas, J.: On combining classifiers. *IEEE Trans. Patt. Anal. Machine Intell.* 1998, 20. P. 226–239.
15. Sim, T., Zhang, S., Janakiraman, R., Kumar, S.: Continuous verification using multimodal biometrics. *IEEE Trans. Patt. Anal. Machine Intell.* 2007, 29(4), P. 687–700.
16. Frischholz, R. W., Deickmann, U.: BioID: a multimodal biometric identification system. *IEEE Comput.* 2000, 33(2).

17. Bradlow, E. T., Everson, P. J.: Bayesian inference for the beta-binomial distribution via polynomial expansions. *J. Comput. Graphical Statistics*, 2002, 11(1). P. 200–207.
18. Poh, N., Wong, R., Kittler, J., Roli, F.: Challenges and research directions for adaptive biometric recognition systems. *Proc. ICB, Alghero, Italy*. 2009.
19. Kumar, A., Kanhangad, V. Zhang, D.: A new framework for adaptive multimodal biometrics management. *IEEE Transactions on Information Forensics and Security*. 2010, (5). P. 92–102.
20. Ручай А.Н., Кузнецов В.В., Мельников А.В., Вохминцев А.В. Разработка централизованной системы избирательной мультибиометрической аутентификации // Информационные технологии и вычислительные системы. №1. 2016. С. 106-116.
21. Ruchay A. An elective multibiometric authentication // *CEUR Workshop Proceedings*, vol. 1710, 2016. P. 292-302.

References

1. Gad, R., El-Fishawy, N., El-Sayed, A., Zorkany, M.: Multi-Biometric Systems: A State of the Art Survey and Research Directions. *International Journal of Advanced Computer Science and Applications*, 2015, 6(6), P. 128–138.
2. Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., Senior, A. W.: *Guide to biometrics*. Springer-Verlag, New-York, 2003.
3. Dunstone, T., Yager, N.: *Biometric system and data analysis: design, evaluation, and data mining*. Springer, Boston, Ma, 2009.
4. Ross, A. A., Nandakumar, K., Jain A. K.: *Handbook of multibiometrics*. Springer, New York, 2006.
5. Bhanu, B., Govindaraju, V.: *Multibiometrics for Human Identification*. Cambridge University Press, Cambridge, 2011.
6. Sesin, E. M., Belov, V. M.: Personal identification system based on integration organization of several biometric characteristics of the person. *Proceedings of Tomsk State University of Control Systems and Radioelectronics* 2012, 2(25), 2, P. 175–179.
7. Asyayev G.D., Ragozin A.N. Opredeleniye minimalnogo nabora vkhodnykh dannykh dlya korrektnoy autentifikatsii po klaviaturnomu pocherku s ispolzovaniyem neyronnoy seti // *Vestnik UrFO. Bezopasnost v informatsionnoy sfere*. 2017. № 3(25). S. 19-23.
8. Ivanov A.I., Somkin S.A., Andreyev D.Yu., Malygina E.A. O mnogoobrazii metrik. pozvolyayushchikh nablyudat realnyye statistikiraspredeleniya biometricheskikh dannykh "nechetkikh ekstraktorov" pri ikh zashchite nalozheniyem gammy // *Vestnik UrFO. Bezopasnost v informatsionnoy sfere*. 2014. № 2 (12). S. 16-23.
9. Poh, N., Ross, A., Lee, W., Kittler, J.: A user-specific and selective multimodal biometric fusion strategy by ranking subjects. *Pattern Recognition* 2013, 46, P. 3341-3357.
10. Vatsa, M., Singh, R., Noore, A.: Context Switching Algorithm for Selective Multibiometric Fusion. *Pattern Recognition and Machine Intelligence* 5909, Springer, 2009. P. 452–457.
11. Fathima, A., Vasuhi, S., Treesa, T., Babu, N.T., Vaidehi, V.: Person Authentication System with Quality Analysis of Multimodal Biometrics. *WSEAS transactions on information science and applications*.
12. Vatsa, M., Singh, R., Noore, A., Ross, A.: On the Dynamic Selection of Biometric Fusion Algorithms. *IEEE transactions on information forensics and security* 2010, 5(3). P. 470–479.
13. Abaza, A., Ross, A.: Quality Based Rank-Level Fusion in Multibiometric Systems. *Proc. of 3rd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2009.
14. Kittler, J., Hatef, M., Duin, R. P. W., Matas, J.: On combining classifiers. *IEEE Trans. Patt. Anal. Machine Intell.* 1998, 20. P. 226–239.
15. Sim, T., Zhang, S., Janakiraman, R., Kumar, S.: Continuous verification using multimodal biometrics. *IEEE Trans. Patt. Anal. Machine Intell.* 2007, 29(4), P. 687–700.
16. Frischholz, R. W., Deickmann, U.: BioID: a multimodal biometric identification system. *IEEE Comput.* 2000, 33(2).
17. Bradlow, E. T., Everson, P. J.: Bayesian inference for the beta-binomial distribution via polynomial expansions. *J. Comput. Graphical Statistics*, 2002, 11(1). P. 200–207.
18. Poh, N., Wong, R., Kittler, J., Roli, F.: Challenges and research directions for adaptive biometric recognition systems. *Proc. ICB, Alghero, Italy*. 2009.
19. Kumar, A., Kanhangad, V. Zhang, D.: A new framework for adaptive multimodal biometrics management. *IEEE Transactions on Information Forensics and Security*. 2010, (5). P. 92–102.
20. Ruchay A.N., Kuznetsov V.V., Melnikov A.V., Vokhmintsev A.V. Razrabotka tsentralizovannoy sistemy

РУЧАЙ Алексей Николаевич, кандидат физико-математических наук, доцент, заведующий кафедрой компьютерной безопасности и прикладной алгебры, Челябинский государственный университет. 454001, Челябинск, ул. Братьев Кашириных, 129.; доцент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: ran@csu.ru.

RUCHAY Alexey Nikolaevich, PhD in Physics and Mathematics, Associate Professor, Head of the Department of Computer Security and Applied Algebra, Chelyabinsk State University. 454001, Chelyabinsk, st. Kashirin Brothers, 129.; Associate Professor, Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, etc. them. IN AND. Lenin, 76. E-mail: ran@csu.ru.



МЕТОДИКА ОБУЧЕНИЯ НЕЙРОННЫХ СЕТЕЙ, ИСПОЛЬЗУЕМЫХ В БЛОКЕ ПРИНЯТИЯ РЕШЕНИЯ СИГНАЛИЗАЦИОННЫХ СРЕДСТВ ОБНАРУЖЕНИЯ

В статье рассматривается вопрос обучения нейронной сети при построении алгоритмов обнаружения нарушителей в блоке принятия решения современных средств обнаружения. Особенность обучения нейронных сетей в средствах обнаружения заключается в использовании модифицированной функции потерь, учитывающей различный ущерб от реализации ошибок первого и второго рода в системах охранной сигнализации. Исходя из критерия минимума среднего риска, в средствах обнаружения целесообразно минимизировать вероятность ложной тревоги (ошибка первого рода) при фиксированном значении вероятности пропуска цели (ошибка второго рода). Получено новое выражение для обновления весов нейронной сети при обучении, исходя из минимизации новой функции потерь. На примере магнитометрических средств обнаружений распределенного типа показан процесс обучения нейронной сети на представительном банке данных расчетных реализаций информационного сигнала и моделирования помех. Показано, что рекуррентная нейронная сеть имеет высокие характеристики обнаружения нарушителей: при заданном значении правильного обнаружения 0,95 вероятность ложной тревоги составила 5,9·10⁻⁴.

Ключевые слова: магнитометрические средства обнаружения, система охранной сигнализации, нейронные сети, функция потерь, блок принятия решения, вероятность обнаружения.

TRAINING METHODS FOR NEURAL NETWORKS USED IN THE DECISIONMAKING BLOCK OF SIGNALING DETECTION TOOLS

The article deals with the issue of training a neural network when building algorithms for detecting violators in the decision-making block of modern detection tools. The feature of training neural networks in modern detection tools is to change the loss function under consideration, which takes into account the possible damage from the implementation of errors of the first and second kind in alarm systems. Based on the criterion of minimum average risk, it is advisable to minimize the probability of a false alarm (error of the first kind) with a fixed value of the probability of missing the target (error of the second kind). A new expression is obtained for updating the weights of the neural network during training, based on minimizing the new loss function. The process of training a neural network on a representative dataset of calculated information signal realizations and interference modeling is shown on the example of distributed magnetometric systems. It is proved that the recurrent neural network has high characteristics of detecting violators: for a given value of correct detection of 0,95, the probability of a false alarm was 5,9·10⁻⁴.

Keywords: detection tools, magnetometric security alarm system, neural network, loss function, decision block, detection probability.

Сигнализационные средства обнаружения (СО) являются сложными техническими системами, состоящими из взаимодействующих составных частей, важнейшими из которых являются чувствительный элемент (ЧЭ), тракт выделения и усиления сигналов, блок принятия решений об обнаружении (БПР). Современный подход к исследованию и разработке СО, представленный в [1], предусматривает разработку математической модели процессов формирования информационного сигнала (ИС), обусловленного воздействием человека-нарушителя (ЧН) на ЧЭ (полезного сигнала), а также проведение натурных экспериментов в объеме, достаточном для подтверждения адекватности разработанной математической модели. Кроме того, при анализе предметной области проводятся оценка влияния шумов на качественные показатели работы СО, натурное измерение шумовых сигналов на выходе ЧЭ в отсутствии нарушителя, составление их адекватной статистической модели. Дальнейшие оптимизация параметров чувствительного элемента и аналогового тракта, выбор и тестирование алгорит-

мов функционирования БПР средства осуществляются путем всестороннего компьютерного моделирования.

Для автоматизации натурных и теоретических исследований СО, анализа их потенциальных характеристик в [1] рекомендовано разрабатывать и реализовать многофункциональный программно-аппаратный комплекс. На рис. 1 представлен пример такого комплекса для исследования магнитометрических СО с протяженным винтовым ЧЭ [2]. Структура комплекса основывается на анализе его требуемой функциональности и включает в себя блоки:

- расчета реализаций полезных сигналов с учетом типа нарушителя;
- моделирования шума и получение аддитивной смеси с ИС;
- формирования представительных баз данных (БД) сигналов и помех, а также частных выборок реализаций аддитивной смеси ИС с шумом;
- навигации по БД;
- синтеза и тестирования алгоритмов принятия решения.

Наличие математических моделей полезных сигналов и шумов, адекватность которых подтверждена экспериментально, позволяет формировать исчерпывающую базу данных расчетных реализаций ИС с обоснованной дискретностью вариации входных параметров моделей, таких, как скорость движения ЧН, параметры его траектории, модуль и ориентация эквивалентного магнитного момента (для магнитометрических СО) и т.д. Вычислительная мощность современных компьютеров позволяет создавать и обрабатывать БД расчетных сигналов весьма подробно, с дискретностью, при которой «соседние» реализации отличаются друг от друга на уровне шума. Функциональные возможности комплекса позволяют на основе исходной базы данных для каждого этапа исследований создавать обучающие выборки смесей расчетных реализаций полезных сигналов (с учетом типа нарушителя) и шума, а также только шумовых воздействий.

денту выбранной функции потерь. Обычно в практике построения ИНС в качестве минимизируемой функции потерь применяется среднеквадратическая ошибка:

$$E_n = \frac{1}{2} \sum_{j=1}^K e_j^2 = \frac{1}{2} \sum_{j=1}^K (d_i - y_i)^2, \quad (1)$$

где d_i – ожидаемое выходное значение на выходе сети; y_i – реально полученное значение на j -м нейроне выходного слоя ИНС; K – количество нейронов в выходном слое сети.

Такой подход оправдан при одинаковом влиянии на качество работы технической системы в целом ошибок первого и второго рода. Стоимость ошибок типа «пропуск цели» и «ложная тревога» в системах охранной сигнализации существенно различны. В [5] показана целесообразность учета возможного ущерба от реализации ошибок при обучении нейронных сетей БПР средств обнаружения. В сигнализационных системах применяется так называемый «обратный критерий Нейма-

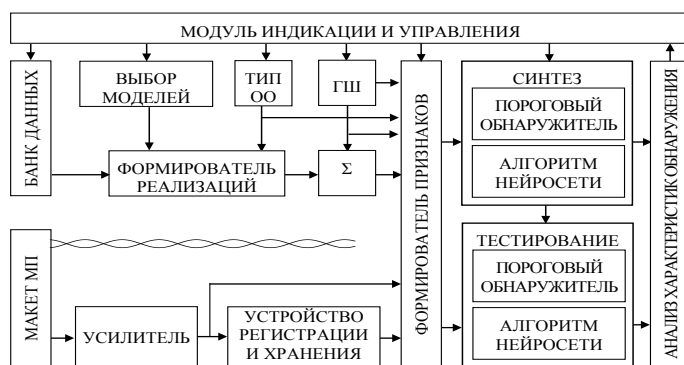


Рис. 1. Структурная схема программно-аппаратного комплекса для исследования потенциальных характеристик СО с распределенным магнитометрическим ЧЭ

Основные тенденции развития устройств, средств и систем охранной сигнализации связаны с совершенствованием алгоритмов обработки информационных сигналов [3]. На сегодняшний день для построения блоков принятия решения об обнаружении СО все чаще используются алгоритмы машинного обучения, в том числе искусственные нейронные сети (ИНС). При этом процесс обучения ИНС при построении блоков принятия решений в средствах обнаружения имеет ряд особенностей.

Проведенные исследования показывают эффективность применения рекуррентной нейронной сети при построении алгоритма принятия решения в магнитометрических СО [4]. В процессе обучения ИНС происходит пересчет весовых коэффициентов по антигра-

на-Пирсона» (как частый случай критерия минимума среднего риска), при котором минимизируется вероятность ложной тревоги (ошибка первого рода) при фиксированном (минимально допустимом) значении вероятности пропуска цели (ошибка второго рода).

Функция потерь (1) в [5] представляется в виде двух слагаемых, каждое из которых соответствует ошибкам первого и второго рода соответственно. Модифицированная функция потерь имеет вид:

$$\sum_{j=1}^K e_j^2 = \sum_{j \in Y} (\alpha_1 \cdot f_1(y_i))^2 + \sum_{j \in N} (\alpha_2 \cdot f_2(y_i))^2,$$

где α_1 и α_2 – линейные коэффициенты; f_1 и f_2 – некоторые функции от выходного значения сети y_j ; Y – подмножество нейронов, для которых ожидаемое значение равно 1; N – под-

множество нейронов, для которых ожидаемое значение равно 0; $K=N+Y$.

В простейшем случае функции f_1 и f_2 могут быть линейными, а коэффициенты α_1 и α_2 равны единице и разнице между желаемым значением правильного обнаружения и выходным значением сети соответственно:

$$\sum_{j=1}^K e_j^2 = \sum_{j \in Y} (\alpha_1 \cdot (1 - y_j))^2 + \sum_{j \in N} (-\alpha_2 \cdot y_j)^2, \quad (2)$$

Тогда функция потерь по всей обучающей выборке для пакетного режима обучения с учетом того, что выходной слой сети имеет только один нейрон, принимает вид:

$$E_{av}(n) = \frac{1}{L} \cdot \sum_{n=1}^L E_n = \frac{1}{2 \cdot L} \cdot \sum_{n=1}^L \sum_{j=1}^K e_j^2 = \frac{1}{2 \cdot L} \cdot \sum_{n=1}^L \left(\sum_{j \in Y} (\alpha_1 \cdot (1 - y_j))^2 + \sum_{j \in N} (-\alpha_2 \cdot y_j)^2 \right), \quad (3)$$

где E_{av} – средняя ошибка по выборке; e_j – сигнал ошибки j -го нейрона в слое;

Y – подмножество объектов обучающей выборки, для которых ожидаемое значение равно 1; N – подмножество объектов, для которых ожидаемое значение равно 0; $L=N+Y$ – мощность обучающей выборки.

Обновление весов происходит по следующей формуле:

$$\Delta w_{j,i} = -\eta \cdot \frac{\partial E_{av}}{\partial w_{j,i}} = \frac{-\eta}{N} \cdot \sum_{n=1}^N e_j(n) \frac{\partial e_j(n)}{\partial w_{j,i}}, \quad (4)$$

где η – норма обучения.

Поскольку ошибка известна на каждом шаге, то $\frac{\partial e_j(n)}{\partial w_{j,i}}$ можно просто вычислить для выходного слоя:

$$\frac{\partial e_j(n)}{\partial w_{j,i}} = -\alpha \cdot q'(\text{net}_j(n)) \cdot y_j, \quad (5)$$

где net_j – взвешенная сумма нейрона; q – функция активации нейрона; коэффициент α принимает значения α_1 или α_2 в зависимости от класса ожидаемого ответа.

Проведенные для магнитометрических средств обнаружения компьютерные эксперименты показали, что учет различия стоимости ошибок первого и второго рода на одних и тех же выборках позволяет снизить вероятность формирования ложной тревоги более, чем на порядок при неснижаемом значении вероятности правильного обнаружения.

Одним из ключевых этапов обучения ИНС, является оценка ее качества на данных, которые не использовались при обучении. Популярным методом оценки обобщающей способности нейронных сетей является двух-

блочная перекрестная проверка, при которой часть данных «откладывается» для тестирования и оценки качества ИНС и не принимает участия в ее обучении. Для улучшения качества модели требуется итерационная настройка гиперпараметров сети или отбор модели. Однако, если тот же самый тестовый набор данных использовать во время отбора модели неоднократно, то он станет частью тренировочных (обучающих) данных, что приведет к переобучению ИНС [6].

Более эффективный способ заключается в разделении исходных данных на три части: тренировочный, проверочный и тестовый наборы. Тренировочный набор используется для выполнения настройки разных моделей, а полученная на проверочном наборе оценка качества используется для отбора модели. Таким образом, тестовый набор не участвует в тренировке и настройке модели сети, а служит только для формирования итоговой оценки. Чтобы оценка модели была менее чувствительна к способу деления на тренировочный и проверочный наборы, применяют k -блочную перекрестную проверку. При k -блочной перекрестной проверке тренировочные данные случайным образом делятся на k блоков, где $k-1$ блоков используются для тренировки модели, а один блок – для проверки. Эта процедура повторяется k раз, в результате чего формируется k моделей (с одинаковыми гиперпараметрами ИНС) и оценок их качества [7]. Чаще всего на практике используют $k=5$ или $k=10$ (для небольших наборов данных).

В результате k -блочной перекрестной проверки формируется предварительная оценка работы ИНС при определенной настройке параметров конфигурации сети (гиперпараметров). Для получения окончательной оценки необходимо обучить ИНС на всем тренировочном наборе данных при параметрах сети, которые демонстрируют наилучшие результаты при предварительной оценке на этапе k -блочной перекрестной проверки. Данный процесс представлен схематично на рис. 2.

Для реализации алгоритмов k -блочной перекрестной проверки требуется предварительная обучающая выборка. С учетом большого разнообразия форм и параметров информационных сигналов в сигнализационных средствах обнаружения каждая из частных выборок должна содержать аддитивные смеси шума и всех информационных сигнала-

лов из БД, сформированной с обоснованной дискретностью входных параметров модели для конкретного типа нарушителя. Тестовую выборку для итоговой оценки качества работы синтезируемого алгоритма принятия решения следует формировать также путем аддитивного смешивания всех реализаций ИС из исходной БД и сгенерированных на основе статистической модели шумов вариативных шумовых воздействий.

сировки классов. После разбиения в каждом блоке находилось примерно равное число обоих классов.

Исходя из данных, представленных в табл. 1, можно сделать вывод о том, что предварительная оценка качества модели показывает низкое значение вероятности ложной тревоги при фиксировании вероятности пропуска цели и использовании модифицированной функции потерь.

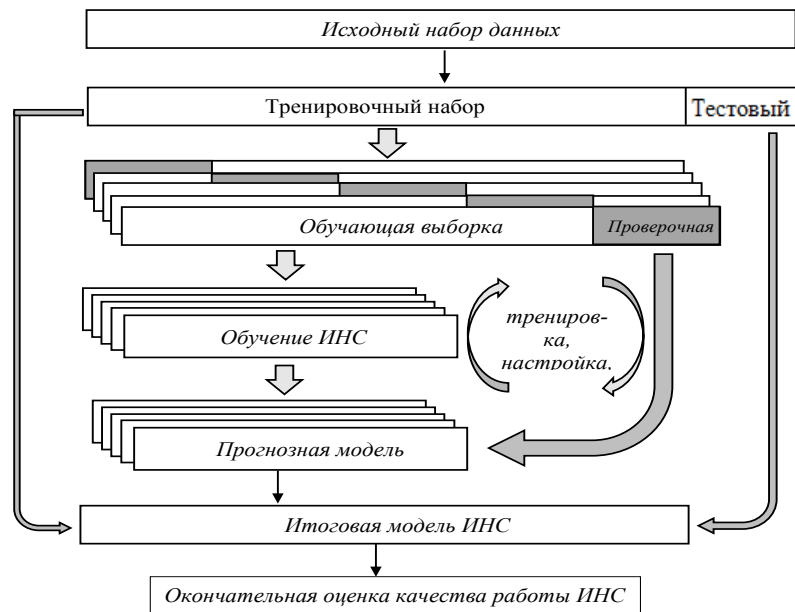


Рис. 2. Схема процесса обучения, проверки и тестирования ИНС

С использованием выражений (2) – (5) была проведена 5-блочная перекрестная проверка модели ИНС для магнитометрического средства обнаружения с протяженным чувствительным элементом на основе винтового преобразователя. Полученные результаты представлены в таблице 1 в виде матриц ошибок. Обучающая выборка содержала

Итоговое тестирование разработанной модели происходило после обучения ИНС по всей обучающей выборке и тестировании на отложенной. Отложенная выборка для тестирования представляла собой весь набор расчетных реализаций аддитивной смеси ИС с шумом на основании БД и реализации моделированного шума (с балансировкой клас-

Таблица 1

Матрица ошибок при проверке ИНС

	Реальное значение класса									
	k=1		k=2		k=3		k=4		k=5	
Прогноз класса	1	0	1	0	1	0	1	0	1	0
1 (есть объект)	21012	13	21008	12	21013	14	21015	14	21017	13
0 (нет объекта)	1106	22105	1110	22106	1105	22104	1104	22105	1102	22106

110592 расчетные реализации аддитивной смеси ИС с шумом (класс 1) и столько же просто шумовых реализаций (класс 0) для балан-

сов). При этом реализации шума при тестировании отличались от реализаций шума в тренировочных данных, что обеспечивало пред-

ставительность этих выборок в отношении всех возможных форм, уровней и длительностей сигналов. Результаты окончательной оценки качества модели представлены в таблице 2 в виде матрицы ошибок.

Проведенные исследования показывают, что с учетом особенностей обучения и фор-

дают основания говорить о высоких характеристиках обнаружения магнитометрических СО распределенного типа, БПР которых построен на основе ИНС: при заданном значении правильного обнаружения 0,95 вероятность ложной тревоги составила $5,9 \cdot 10^{-4}$. Полученное значение вероятности ложной тре-

Таблица 2

Матрица ошибок итогового тестирования ИНС

Прогноз класса	Реальное значение класса	
	1	0
1	105062	130
0	5530	221054

мирования обучающих выборок искусственные нейронные сети целесообразно использовать при синтезе блоков принятия решений в сигнализационных средствах обнаружения. Так полученные авторами данные

воги существенно ниже, чем соответствующее значение, наблюдаемое при простом пороговом алгоритме принятия решений ($6,3 \cdot 10^{-3}$) [4].

Литература

1. Духан, Е.И. Методология научного исследования средств обнаружения / Радиотехника: территориально распределенные системы охраны. – 2015. – № 13. – С. 31–33.

2. Духан Е.И., Захаркин Г.Ф., Звездинский С.С. Специализированный комплекс для исследования характеристик магнитометрического средства обнаружения нарушителей / Сборник трудов XI Международной отраслевой научно-технической конференции «Технологии информационного общества», 15–16 марта 2017 г. Москва, МТУСИ. – С. 299–300.

3. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: учебное пособие для вузов – М.: Горячая линия-Телеком, 2004. – 367с.

4. Духан Е.И., Захаркин Г.Ф., Духан А.Е., Звездинский С.С. Алгоритмы обработки информации магнитометрического средства обнаружения на основе нейросети / Спецтехника и связь, 2015. – № 5. – С. 29–32.

5. Звездинский С.С., Духан А.Е., Духан Е.И., Парфенцев И.В. Интеллектуализация принятия решений в системах физической защиты объектов / Т Comm: Телекоммуникации и транспорт. 2018. Том 12. №1. С. 40–43.

6. Рашка С., Python и машинное обучение / пер. с англ. А.В. Логунова. – М.: ДМК Пресс, 2017. – 418 с.: ил.

7. Жерон О. Прикладное машинное обучение с помощью Scikit-Learn и TensorFlow: концепции, инструменты и техники для создания интеллектуальных систем.: Пер. с англ. – СПб.: ООО «Альфа-книга», 2018. – 688 с.: ил.

References

1. Dukhan, E.I. Metodologiya nauchnogo issledovaniya sredstv obnaruzheniya / Radiotekhnika: territorial'no raspredelennye sistemy okhrany. – 2015. – №13. – С. 31–33.

2. Dukhan E.I., Zakharkin G.F., Zvezhinskiy S.S. Spetsializirovanny kompleks dlya issledovaniya kharakteristik magnitometricheskogo sredstva obnaruzheniya narushiteley / Sbornik trudov XI Mezhdunarodnoy otraslevoy nauchno-tekhnicheskoy konferentsii «Tekhnologii informatsionnogo obshchestva», 15–16 marta 2017 g. Moskva, MTUSI. – S. 299-300.

3. Magauenov R.G. Sistemy okhrannoy signalizatsii: osnovy teorii i printsipy postroeniya: uchebnoe posobie dlya vuzov – M.: Goryachaya liniya-Telekom, 2004. – 367s.

4. Dukhan E.I., Zakharkin G.F., Dukhan A.E., Zvezhinskiy S.S. Algoritmy obrabotki informatsii magnitometricheskogo sredstva obnaruzheniya na osnove neyroseti / Spetsstekhnika i svyaz, 2015. – № 5. – S. 29 –32.

5. Zvezhinskiy S.S., Dukhan A.E., Dukhan E.I., Parfentsev I.V. Intellectualizatsiya prinyatiya resheniy v sistemakh fizicheskoy zashchity ob"ektov / T Comm: Telekommunikatsii i transport. 2018. Tom 12. №1. S. 40-43.

6. Rashka S., Python i mashinnoe obuchenie / per. s angl. A.V. Logunova. – M.: DMK Press, 2017. – 418 s.: il.

7. Zheron O. Prikladnoe mashinnoe obuchenie s pomoshch'yu Scikit-Learn i TensorFlow: kontseptsii, instrumenty i tekhniki dlya sozdaniya intellektual'nykh sistem.: Per. s angl. – SpB.: ООО «Al'fa-kniga», 2018. – 688 s.: il.

ДУХАН Евгений Изович, доктор технических наук, доцент, профессор Учебно-научного центра «Информационная безопасность» ИРИТ-РТФ ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина». 620002, Россия, г. Екатеринбург, ул. Мира, 19. Email: Evgeny.Duchan@urfu.ru

ЗАХАРКИН Григорий Федорович, инженер департамента радиоэлектроники и связи ИРИТ-РТФ ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина». 620002, Россия, г. Екатеринбург, ул. Мира, 19. Email: zakharkin88@gmail.com

ДУХАН Андрей Евгеньевич, аспирант ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина». 620002, Россия, г. Екатеринбург, ул. Мира, 19. Email: andmo901@gmail.com

DUKHAN Evgeny Izovich, doctor of technical Sciences, associate Professor, Professor Of the educational and scientific center "Information security" of the URAL Federal University named after the first President of Russia B. N. Yeltsin. 19 Mira str., Yekaterinburg, 620002, Russia. Email: Evgeny.Duchan@urfu.ru

ZAKHARKIN Grigoriy Fedorovich, engineer of the Department of Radioelectronics and communications, URAL Federal University named after the first President of Russia B. N. Yeltsin. 19 Mira str., Yekaterinburg, 620002, Russia. Email: zakharkin88@gmail.com

DUKHAN Andrey Evgenyevich, graduate student of Ural Federal University named after first President of Russia B. N. Yeltsin. 19 Mira str., Yekaterinburg, 620002, Russia. Email: andmo901@gmail.com

ЧИСЛЕННЫЙ МЕТОД ОПРЕДЕЛЕНИЯ ТЕМПЕРАТУРНОГО ПОЛЯ ЛИНЕЙНОГО ОБЪЕКТА ПРИ ВНЕШНЕМ ТЕПЛОВОМ ВОЗДЕЙСТВИИ

Использование технологий анализа данных для обработки результатов температурных измерений направлена на решение задач контроля параметров управляющих тепловых режимов, мониторинга теплового состояния основного промышленного оборудования, а также вопросы обеспечения целостности и доступности данных, циркулирующих в автоматизированных системах управления технологическими процессами (АСУ ТП).

В статье рассмотрена задача определения нестационарных температурных полей внутри объекта по зашумленным результатам поверхностных температурных измерений и параметрам внешнего теплового воздействия на его поверхность. Математически процесс теплопереноса представлен параболическим уравнением, включает начальные условия, а также граничные условия, определенные по результатам измерений температуры на поверхности объекта и в соответствии с характеристиками внешнего теплового режима.

Точность и устойчивость представленного в работе метода решения задачи теплопереноса исследованы посредством вычислительного эксперимента. В эксперименте найденные температурные значения во внутренних точках объекта сравнивались с тестовыми функциями, сформированными на основе имитационного моделирования. Результаты вычислительного эксперимента свидетельствуют о надежности и устойчивости используемого метода определения внутренних нестационарных температурных полей из измеренных граничных значений. Предложенный алгоритм определения температуры используется для обеспечения целостности данных при обработке измеренной информации, так как направлен на уменьшение негативного влияния шумов на точность конечного результата. Алгоритм определяет внутренние нестационарные температурные поля по результатам косвенных измерений, тем самым обеспечивая доступность информации о внутреннем тепловом состоянии объекта.

Ключевые слова: нестационарный процесс, уравнение теплопроводности, операционный метод, численное решение, обратная задача, теплоперенос, автоматизированная система управления технологическим процессом (АСУ ТП), целостность информации, доступность информации.

NUMERICAL METHOD FOR DETERMINING TEMPERATURE FIELD OF A LINEAR OBJECT UNDER EXTERNAL THERMAL INFLUENCE

The use of data analysis technologies for processing the temperature measurement results is aimed at solving the problems of controlling the parameters of controlling thermal modes, monitoring the thermal state of the main industrial equipment, as well as issues of integrity and availability of data circulating in automated control systems for technological processes.

The article is devoted to the problem of determining non-stationary temperature fields inside an object from the noisy results of surface temperature measurements and the parameters of external thermal effect on its surface. Mathematically, the heat transfer process is represented by a parabolic equation, includes initial conditions, as well as boundary conditions formed from temperature measurements on the object's surface and in accordance with the characteristics of the external thermal regime.

The accuracy and stability of the presented method were investigated by means of a computational experiment. In the experiment, the found temperature values were compared with simulate test functions. The computational results indicate the reliability of the proposed method for determining the temperature at the internal points of the object from the measured boundary values. This method can be aim to ensuring the reliability and integrity of data when processing the measured information, reducing the negative effect of initial data noise. The algorithm determines the internal non-stationary temperature fields based on the results of indirect measurements, thereby ensuring the availability of information about the internal thermal state of the object.

Keywords: *non-stationary process, heat conduction equation, operational method, numerical solution, inverse problem, heat transfer, automated control system of technological process, the integrity of information, accessibility of information.*

Введение

Цифровизация технологических процессов, связанных с теплопереносом, направлена на повышение эффективности и оптимизацию современного производства. Обработка результатов измерений, полученных от датчиков АСУ ТП, расположенных вблизи поверхности объекта, позволяет определять внутреннее тепловое состояние объектов, подвергаемых внешнему тепловому воздействию в технологических процессах, связанных с теплопереносом.

Задачи, в которых неизвестные температурные поля внутри объекта находят по ис-

ходным данным, сформированным из результатов граничных измерений и характеристик внешнего теплового воздействия, относятся к классу обратных граничных задач. Сложность решения обратных задач заключается в том, что, с одной стороны, результаты измерений неизбежно содержат отклонения от действительных значений, а с другой стороны, использование общепринятых методов для обработки зашумленных исходных данных дает искаженную информацию о внутреннем тепловом состоянии объекта, что порождает проблему обеспечения целостности и доступности информации о теплофизи-

ческих свойствах объекта. Таким образом, возникает необходимость разрабатывать вычислительные методы, устойчивые относительно погрешности исходных данных, позволяющие уменьшить негативное влияние шумов на точность результата.

Основы теории обратных задач положены в работах А.Н. Тихонова [1], М.М. Лаврентьева [2]. Дальнейшим исследованиям в этой области посвящены работы О.М. Алифанова [3], А.А. Самарского [4], С.И. Кабанихина, М.А. Шишленина [5], А.Г. Яголы [6]. Разработке вычислительных схем и численных алгоритмов для решения рассматриваемых задач посвящены труды П.Н. Вабищевича [7], Ю.М. Мацевитого [8], Г.И. Марчука [9], В.И. Васильева [10] и других исследователей [11–17].

В данной статье обобщены результаты работы [18] для неоднородной обратной задачи тепломассопереноса. Исходная задача с помощью прямого и обратного преобразования Лапласа сводится к интегральному уравнению. В статье также предложен численный алгоритм его решения, основанный на регуляризирующем подходе, заключающемся в выборе количества слагаемых в ядре полученного уравнения. Для проверки надежности построенного алгоритма был проведен вычислительный эксперимент на основе имитационного моделирования. Результаты эксперимента представлены в работе.

Постановка задачи нестационарного теплопереноса

Предпосылки математической модели нестационарного теплового процесса состоят в следующем. Теплоперенос в объекте при вторичной и комплексной термообработке сопровождается эндотермическими и экзотермическими химическими реакциями между внутренними включениями, размеры которых пренебрежительно малы по сравнению с размерами объекта. При химических реакциях происходит выделение или поглощение тепла, влияние которых на температуру внутри объекта характеризуется функцией внутреннего теплового источника. Объект подвергается внешнему тепловому воздействию, при этом в каждой точке поверхности температурные значения одинаковы, что позволяет представить процесс теплопереноса как проблему определения температуры в стержне, одному концу которого соответствует точка на поверхности, а другому – точка внутри объекта, в которой требуется определить температуру.

В соответствии с требованиями технического регламента для выравнивания внутренних температурных полей объекта перед началом технологического процесса, связанного с тепловым воздействием, предусмотрена выдержка при постоянной температуре. Полагаем, что в начальный момент времени температура во внутренних точках объекта была одинаковой. Теплофизические характеристики объекта не претерпевают существенных изменений, что позволяет считать коэффициент температуропроводности постоянной величиной.

Введем следующие обозначения: точка P соответствует началу координат; точке B соответствует точка с координатой L ; x – текущая точка линейного объекта PB , $x \in [0, L]$; T – продолжительность технологического процесса, t – текущее время, $t \in [0, T]$.

Измерения температуры проводятся в точках P и x_0 . Результатам измерения температуры в точке P соответствует функция $\varphi(t)$, а результатам измерения в точке x_0 – функция $q(t)$. Схема измерения температуры изображена на рис. 1.

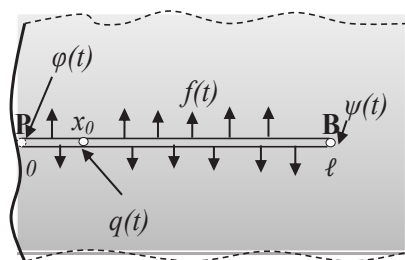


Рис. 1. Схема измерения

В этой задаче требуется найти значения температуры $\psi(t)$ в точке B . Математическую модель процесса, согласно [4], можно представить уравнением теплопроводности

$$u_t = au_{xx} + f(t), \quad x \in (0, L), \quad t \geq 0. \quad (1)$$

где функция $f(t)$ характеризует мощность внутреннего теплового источника,

a – коэффициент температуропроводности. Из результатов измерений формируются условия

$$u(0, t) = \varphi(t), \quad u(x_0, t) = q(t), \quad t \geq 0. \quad (2)$$

Так как температура в начальный момент одинакова во всем линейном объекте, то этому условию соответствует соотношение:

$$u(x, 0) = 0, \quad x \in [0, L]. \quad (3)$$

Искомым является значение температуры в точке B , а математически требуется найти функцию

$$u(L, t) = \psi(t). \quad (4)$$

Существование единственного решения обратной граничной задачи (1)–(4) обосновано в работах [3] и [9].

Согласно требованиям, предъявляемым к технологическому процессу, при его реализации недопустимы резкие изменения температурных градиентов на поверхности и внутри объекта. Математически эту ситуацию представим в следующем виде: полагаем, что существуют постоянные $M_0 \geq 0$, $M_1 \geq 0$, $M_2 \geq 0$, $M_3 \geq 0$, $M_4 \geq 0$ и $s_0 \geq 0$, $s_1 \geq 0$, $s_2 \geq 0$, $s_3 \geq 0$, $s_4 \geq 0$ такие, что $|\mu(x, t)| \leq M_0 e^{s_0 t}$, $x \in [0, L]$, $|\varphi(t)| \leq M_1 e^{s_1 t}$, $|q(t)| \leq M_2 e^{s_2 t}$, $|\psi(t)| \leq M_3 e^{s_3 t}$ и $|f(t)| \leq M_4 e^{s_4 t}$ для всех $t > 0$. При этом для любого $t \in [0, T]$ при всех $T > 0$ функции $\varphi(t)$, $q(t)$, $\psi(t)$ и $f(t)$ отвечают условиям теоремы Дирихле.

Неизбежно возникающие отклонения измеренных величин от действительных приводят к тому, что вместо действительных значений q_0 и φ_0 получены q_δ и φ_δ , удовлетворяющие условию $\max \{\|q_\delta - q_0\|_C, \|\varphi_\delta - \varphi_0\|_C\} \leq \delta$, где δ – уровень точности средства измерения температуры.

Таким образом, по измеренным величинам необходимо определить температурное поле $u_\delta(L, t) = \psi_\delta(t)$ в точке В.

Редукция обратной граничной задачи теплопереноса к интегральному уравнению

На первом этапе редукции исходной задачи к интегральному уравнению используем идею, предложенную в [13]. Согласно этому подходу, находим решение прямой задачи теплопереноса, полагая, что функция внешнего теплового режима $\psi(t)$ известна. Математическая модель прямой задачи имеет вид:

$$u_t = au_{xx} + f(t), \quad x \in (0, L), \quad t \geq 0. \quad (5)$$

$$u(0, t) = \varphi(t), \quad u(L, t) = \psi(t), \quad t \geq 0. \quad (6)$$

$$u(x, 0) = 0, \quad x \in [0, L]. \quad (7)$$

Основываясь на свойствах функций $\varphi(t)$, $\psi(t)$, $f(t)$, $u(x, t)$ и применяя прямое преобразование Лапласа [19], получим следующее операторное изображение прямой задачи теплопереноса:

$$\bar{u}_{xx} - \frac{p}{a} \bar{u} = -\frac{\bar{f}}{a},$$

$$\bar{u}(0, p) = \bar{\varphi}(p), \quad \bar{u}(L, p) = \bar{\psi}(p),$$

где $\bar{u}(x, p)$, $\bar{\varphi}(p)$, $\bar{\psi}(p)$ и $\bar{f}(p)$ – образы функций $u(x, t)$, $\varphi(t)$, $\psi(t)$ и $f(t)$ при прямом преобразовании Лапласа.

Изображение аналитического решения

$\bar{u}(x, p)$ прямой задачи имеет следующий

вид:

$$\bar{u}(x, p) = \bar{\varphi}(p) \frac{\operatorname{sh}\left(\sqrt{\frac{p}{a}}(L-x)\right)}{\operatorname{sh}\sqrt{\frac{p}{a}}L} + \bar{\psi}(p) \frac{\operatorname{sh}\left(\sqrt{\frac{p}{a}}x\right)}{\operatorname{sh}\sqrt{\frac{p}{a}}L} - \frac{\bar{f}}{p} \left(\frac{\operatorname{sh}\left(\sqrt{\frac{p}{a}}(L-x)\right)}{\operatorname{sh}\sqrt{\frac{p}{a}}L} + \frac{\operatorname{sh}\left(\sqrt{\frac{p}{a}}x\right)}{\operatorname{sh}\sqrt{\frac{p}{a}}L} \right) + \frac{\bar{f}}{p}. \quad (8)$$

Из результатов, доказанных в [13], получаем:

$$\frac{\operatorname{sh}\left(\sqrt{\frac{p}{a}}(L-x)\right)}{\operatorname{sh}\sqrt{\frac{p}{a}}L} = \frac{L-x}{L} + \frac{2}{\pi} \sum_{n=1}^{\infty} \frac{(-1)^n}{n} \sin\left(\frac{\pi n(L-x)}{L}\right) \frac{p}{p + \frac{n^2 \pi^2 a}{L^2}} \quad (9)$$

$$\frac{\operatorname{sh}\left(\sqrt{\frac{p}{a}}x\right)}{\operatorname{sh}\sqrt{\frac{p}{a}}L} = \frac{x}{L} + \frac{2}{\pi} \sum_{n=1}^{\infty} \frac{(-1)^n}{n} \sin\left(\frac{\pi nx}{L}\right) \frac{p}{p + \frac{n^2 \pi^2 a}{L^2}} \quad (10)$$

Перегруппировав слагаемые в (8), и принимая во внимание сходимость рядов (9) и (10), получим:

$$\begin{aligned} \bar{u}(x, p) = & \bar{\varphi}(p) \frac{L-x}{L} + \frac{2}{\pi} \bar{\varphi}(p) \sum_{n=1}^{\infty} \frac{(-1)^n}{n} \sin\left(\frac{\pi n(L-x)}{L}\right) \frac{p}{p + \frac{n^2 \pi^2 a}{L^2}} + \\ & + \bar{\psi}(p) \frac{x}{L} + \frac{2}{\pi} \bar{\psi}(p) \sum_{n=1}^{\infty} \frac{(-1)^n}{n} \sin\left(\frac{\pi nx}{L}\right) \frac{p}{p + \frac{n^2 \pi^2 a}{L^2}} + \\ & + \frac{4}{\pi} \cdot \frac{\bar{f}}{p} \sum_{n=1}^{\infty} \frac{1}{2n-1} \sin\left(\frac{(2n-1)\pi x}{L}\right) \frac{p}{p + \frac{(2n-1)^2 \pi^2 a}{L^2}}. \quad (11) \end{aligned}$$

Учитывая свойства функций $\varphi(t)$, $f(t)$, $\psi(t)$, найдем решение $u(x, t)$ прямой задачи (5)–(7), применив обратное преобразование Лапласа и теорему о свертке [19]. Получим:

$$\begin{aligned} u(x, t) = & \varphi(t) \frac{L-x}{L} + \frac{2}{\pi} \frac{d}{dt} \sum_{n=1}^{\infty} \frac{(-1)^n}{n} \sin\left(\frac{\pi n(L-x)}{L}\right) e^{-\frac{n^2 \pi^2 a}{L^2} t} \int_0^t \varphi(\tau) e^{\frac{n^2 \pi^2 a}{L^2} \tau} d\tau + \\ & + \psi(t) \frac{x}{L} + \frac{2}{\pi} \frac{d}{dt} \sum_{n=1}^{\infty} \frac{(-1)^n}{n} \sin\left(\frac{\pi nx}{L}\right) e^{-\frac{n^2 \pi^2 a}{L^2} t} \int_0^t \psi(\tau) e^{\frac{n^2 \pi^2 a}{L^2} \tau} d\tau + \\ & + \frac{4}{\pi} \sum_{n=1}^{\infty} \frac{1}{2n-1} \sin\left(\frac{(2n-1)\pi x}{L}\right) e^{-\frac{(2n-1)^2 \pi^2 a}{L^2} t} \int_0^t f(\tau) e^{\frac{n^2 \pi^2 a}{L^2} \tau} d\tau. \quad (12) \end{aligned}$$

Исследуем сходимость ряда, содержащего функцию $\varphi(t)$, используя теорему Вейерштрасса и следующие оценки:

$$\left| \int_0^t \varphi(\tau) e^{\frac{n^2 \pi^2 a}{L^2} \tau} d\tau \right| \leq M_1 \int_0^t e^{\left(\frac{n^2 \pi^2 a}{L^2} + s_1\right) \tau} d\tau = \frac{M_1 L^2}{(n^2 \pi^2 a + L^2 s_1)} \left(e^{\left(\frac{n^2 \pi^2 a}{L^2} + s_1\right) t} - 1 \right) \leq \frac{M_1 L^2 e^{\left(\frac{n^2 \pi^2 a}{L^2} + s_1\right) t}}{(n^2 \pi^2 a + L^2 s_1)}.$$

Имеем

$$\frac{1}{n} \left| \sin \left(\frac{\pi n(L-x)}{L} \right) \right| e^{\frac{-n^2 \pi^2 a}{L^2} t} \left| \int_0^t \varphi(\tau) e^{\frac{n^2 \pi^2 a}{L^2} \tau} d\tau \right| \leq \quad (13)$$

$$\leq \frac{1}{n} \left| \sin \left(\frac{\pi n(L-x)}{L} \right) \right| e^{\frac{-n^2 \pi^2 a}{L^2} t} \cdot \frac{M_1 L^2 e^{\left(\frac{n^2 \pi^2 a}{L^2} t \right)}}{(n^2 \pi^2 a + L^2 s_1)} \leq \frac{M_1 L^2 e^{s_1}}{n(n^2 \pi^2 a + L^2 s_1)} \leq \frac{M_1 L^2 e^{s_1}}{n^3 \pi^2 a}$$

Проводя аналогичные рассуждения, получаем сходимость ряда, содержащего функцию $\psi(t)$.

В силу того, что функциональная последовательность $\left\{ n \sin \left(\frac{\pi n x}{L} \right) \right\}_{n=1}^{\infty}$ не является ограниченной для всех $x \in [0, L]$, то по теореме Абеля ряды в (12), содержащие функции $\varphi(t)$ и $\psi(t)$, не являются сходящимися.

На втором этапе редукции, обобщая результат [18], осуществляем регуляризацию, аппроксимируя каждый из рядов в (12) конечным рядом. Решение $u(x, t)$ прямой задачи (5)–(7) примет вид:

$$u(x, t) = \varphi(t) \frac{L-x}{L} + \frac{2}{\pi} \frac{d}{dt} \sum_{n=1}^{N_1} \frac{(-1)^n}{n} \sin \left(\frac{\pi n(L-x)}{L} \right) e^{\frac{-n^2 \pi^2 a}{L^2} t} \int_0^t \varphi(\tau) e^{\frac{n^2 \pi^2 a}{L^2} \tau} d\tau +$$

$$+ \psi(t) \frac{x}{L} + \frac{2}{\pi} \frac{d}{dt} \sum_{n=1}^{N_2} \frac{(-1)^n}{n} \sin \left(\frac{\pi n x}{L} \right) e^{\frac{-n^2 \pi^2 a}{L^2} t} \int_0^t \psi(\tau) e^{\frac{n^2 \pi^2 a}{L^2} \tau} d\tau +$$

$$+ \frac{4}{\pi} \sum_{n=1}^{N_3} \frac{1}{2n-1} \sin \left(\frac{(2n-1)\pi x}{L} \right) e^{\frac{-(2n-1)^2 \pi^2 a}{L^2} t} \int_0^t f(\tau) e^{\frac{n^2 \pi^2 a}{L^2} \tau} d\tau \quad (14)$$

На третьем этапе редукции продифференцируем конечные ряды в (14). Имеем:

$$u(x, t) = \frac{2\pi a}{L^2} \sum_{n=1}^{N_1} (-1)^{n+1} n \sin \left(\frac{\pi n x}{L} \right) \int_0^t \psi(\tau) e^{\frac{-n^2 \pi^2 a}{L^2} (t-\tau)} d\tau +$$

$$+ \frac{2\pi a}{L^2} \sum_{n=1}^{N_2} n \sin \left(\frac{\pi n x}{L} \right) \int_0^t \varphi(\tau) e^{\frac{-n^2 \pi^2 a}{L^2} (t-\tau)} d\tau +$$

$$+ \frac{4}{\pi} \sum_{n=1}^{N_3} \frac{1}{2n-1} \sin \left(\frac{\pi(2n-1)x}{L} \right) \int_0^t f(\tau) e^{\frac{-n^2 \pi^2 a}{L^2} (t-\tau)} d\tau. \quad (15)$$

Отсюда и граничных условий (2), имеем:

$$q(t) = \frac{2\pi a}{L^2} \sum_{n=1}^{N_1} (-1)^{n+1} n \sin \left(\frac{\pi n x_0}{L} \right) \int_0^t \psi(\tau) e^{\frac{-n^2 \pi^2 a}{L^2} (t-\tau)} d\tau +$$

$$+ \frac{2\pi a}{L^2} \sum_{n=1}^{N_2} n \sin \left(\frac{\pi n x_0}{L} \right) \int_0^t \varphi(\tau) e^{\frac{-n^2 \pi^2 a}{L^2} (t-\tau)} d\tau +$$

$$+ \frac{4}{\pi} \sum_{n=1}^{N_3} \frac{1}{2n-1} \sin \left(\frac{\pi(2n-1)x_0}{L} \right) \int_0^t f(\tau) e^{\frac{-n^2 \pi^2 a}{L^2} (t-\tau)} d\tau \quad (16)$$

Введем следующие обозначения:

$$K_N(t-\tau) = \frac{2\pi a}{L^2} \sum_{n=1}^{N_1} (-1)^{n+1} n \sin \left(\frac{\pi n x_0}{L} \right) e^{\frac{-n^2 \pi^2 a}{L^2} (t-\tau)},$$

$$Q_N(t-\tau) = \frac{2\pi a}{L^2} \sum_{n=1}^{N_2} n \sin \left(\frac{\pi n x_0}{L} \right) e^{\frac{-n^2 \pi^2 a}{L^2} (t-\tau)},$$

$$R_N(t-\tau) = \frac{4}{\pi} \sum_{n=1}^{N_3} \frac{1}{2n-1} \sin \left(\frac{\pi(2n-1)x_0}{L} \right) e^{\frac{-(2n-1)^2 \pi^2 a}{L^2} (t-\tau)}$$

при всех $t \in [0, T]$.

Тогда уравнение (16) примет вид:

$$\int_0^t K_N(t-\tau) \psi(\tau) d\tau = g(t) - \left(\int_0^t Q_N(t-\tau) \varphi(\tau) d\tau + \int_0^t R_N(t-\tau) f(\tau) d\tau \right). \quad (17)$$

Учитывая, что вместо действительных значений φ_0 и q_0 известны приближенные φ_δ и q_δ , необходимо найти решение уравнения (17) при условии $\max \{ \|q_\delta - q_0\|_C, \|\varphi_\delta - \varphi_0\|_C \} \leq \delta$. Для построения решения $u_\delta(x, t)$ уравнения (17) предлагается метод, основанный на конечных интегральных представлениях.

Вычислительная схема метода решения

Основные этапы метода решения уравнения (17) заключаются в следующем. Сначала выбираем начальные значения параметров регуляризации: шага дискретизации по времени h и величин N_1, N_2 и N_3 .

Затем вводим сетку с узлами t_i , где $t_i = ih$, $i = 0, s$, $s = \frac{T}{h}$. В результате дискретизации уравнения (17) получим следующую систему уравнений:

$$\sum_{j=1}^s h K_N(t_i - \tau_j) \psi(\tau_j) = q(t_i) - \left(\sum_{j=1}^s h Q_N(t_i - \tau_j) \varphi(\tau_j) + \sum_{j=1}^s h R_N(t_i - \tau_j) f(\tau_j) \right), \quad (18)$$

где $i = \overline{1, s}$. Далее переходим к итерационному процессу. На каждом шаге процесса находим решение системы (18) и оцениваем величину погрешности Δ , определяемую формулой:

$$\Delta = \frac{\max_{t_i \in [0, T]} |\psi_\delta(t_i) - \psi(t_i)|}{\max_{t_i \in [0, T]} |\psi(t_i)|}.$$

На следующем шаге выбираем новые значения N_1, N_2, N_3 и шага дискретизации h и решаем систему (18). По завершению решения находим новое значение Δ и сравниваем его с величиной, найденной на предыдущем шаге. Итерационный процесс останавливаем при достижении минимального значения величины Δ .

С целью проверки устойчивости построенного численного алгоритма относительно погрешности исходных данных и получения экспериментальных оценок погрешностей

был осуществлен вычислительный эксперимент на основе имитационного моделирования.

Вычислительный эксперимент

Эксперимент проводился при следующих теплофизических характеристиках процесса теплопереноса: длина линейного объекта $L = 10$, коэффициент температуропроводности $a = 1$, точка $x_0 = 0,1 \cdot L$. Для проведения вычислений в области $[0, L] \times [0, T]$ вводим сетку с узлами (x_i, t_j) , где $x_i = ih_x$, $i = 0, \dots, r + 1$, $r = L/h_x$; $t_j = jh_t$, $j = 0, \dots, m + 1$, $m = T/h_t$. Эксперимент осуществлялся для следующих тестовых моделей:

1. Функции, соответствующие первоначальному росту и последующему убыванию влияния внешнего теплового источника, при этом влияние функции внутреннего теплового постоянно уменьшается. Представителями данного типа являются функции $\varphi_1(t) = 15te^{-t/10}$, $\psi_1(t) = 20te^{-t/9}$ и $f_1(t) = 20e^{-t/10}(1 - 0,1t)$.

2. Функции, соответствующие росту влияния внешнего и внутреннего тепловых источников. Представителями данного типа являются функции $\varphi_2(t) = e^{t/9} - 1$, $\psi_2(t) = e^{2t/15} - 1$ и $f_2(t) = e^{t/20}$.

Основные этапы вычислительного эксперимента:

Этап 1. Моделирование температурных полей $u(x, t)$ в линейном объекте и тестовых функций. С этой целью для тестовых функций $\varphi_k(t)$, $f_k(t)$ и $\psi_k(t)$ находим решение $u(x, t)$ прямой задачи (5)–(7). Для этого используем метод конечно-разностной аппроксимации. Для определения температурной функции $q(t_i) = u(x_0, t_i)$ используем значения температурного поля $u(x, t)$ объекта в соответствующей точке x_0 .

Этап 2. Моделирование возмущенных исходных данных. Для этого формируем тестовые значения $q_\delta(t_i)$ и $\varphi_\delta(t_j)$ по формулам: $q_\delta(t_i) = q(t_i) + \mu_\delta(t_i)$, $\varphi_\delta(t_j) = \varphi(t_j) + \eta_\delta(t_j)$, где функции $\mu_\delta(t)$ и $\eta_\delta(t)$ распределены равномерно на отрезке $[-\delta, \delta]$.

Этап 3. Построение решения интегрального уравнения (17). Для этого используем предложенную вычислительную схему. Получаем $\psi_\delta(t)$.

Этап 4. Оценка температурных погрешностей. С этой целью используем функции $\Delta(t)$ и величины Δ_ψ , θ_ψ : $\Delta(t) = |\psi_\delta(t) - \psi(t)|$, $\Delta_\psi = \max_{t \in [0, T]} \Delta(t)$, $\theta_\psi = \frac{\Delta_\psi}{\max_{t \in [0, T]} |\psi(t)|}$.

Если величины $\Delta(t)$, Δ_ψ , θ_ψ достигли ми-

нимального значения, то останавливаем итерационный процесс.

Этап 5. Построение температурных полей $u_\delta(x, t)$ в линейном объекте. По завершении итерационного процесса найденную функцию $\psi_\delta(t)$, соответствующую минимальному значению Δ , подставляем в прямую задачу (5)–(7) и находим температурное поле $u_\delta(x, t)$. Далее сравниваем функции $u_\delta(x, t)$ и $u(x, t)$, находя наибольшие отклонения температурных полей линейного объекта по формулам:

$$\Delta_u = \max_{(x, t) \in [0, \ell] \times [0, T]} |u_\delta(x, t) - u(x, t)|,$$

$$\theta_u = \frac{\Delta_u}{\max_{(x, t) \in [0, \ell] \times [0, T]} |u(x, t)|}.$$

На основании этих величин получаем оценки точности определения нестационарных температурных полей в линейном объекте.

Результаты вычислительного эксперимента

В работе представлены результаты вычислительного эксперимента, проведенного для тестовых функций, сформированных посредством имитационного моделирования. Результаты эксперимента приведены в таблице 1 для различных значений погрешностей исходных данных.

На рис. 2 и рис. 4 представлены результаты сравнительного анализа температурных полей $\psi_\delta(t)$, полученных в точке В и тестовых функций $\psi(t)$. Обозначения: линия 1 соответствует температурному полю $\psi_\delta(t)$, найденному с помощью предложенного метода; линия 2 соответствует тестовым значениям функции $\psi(t)$. На рис. 2б и рис. 4б показаны графики погрешностей $\Delta(t)$. Двумерные поверхности на рис. 3 и рис. 5 соответствуют температурным полям линейного объекта. Поверхности, озаглавленные «Температурное поле $u(x, t)$ », соответствуют тестовым значениям, сформированным на первом этапе вычислительного эксперимента. Поверхности, озаглавленные «Расчетное температурное поле $u_\delta(x, t)$ », соответствуют температурным полям, вычисленным с помощью предложенного метода.

Результаты имитационного моделирования свидетельствуют о достаточной точности и устойчивости относительно погрешности исходных данных предложенного алгоритма определения нестационарных температурных полей внутри объекта.

Экспериментальные оценки погрешностей температурных функций

Тестовые функции	Погрешность исходных данных, δ	Погрешности вычислений			
		Δ_ψ	θ_ψ	Δ_u	θ_u
Тест 1					
$\varphi_1(t)=15te^{-t/10}$ $\psi_1(t)=20te^{-t/9}$ $f_1(t)=20e^{-t/10}(1-0,1t)$	0,01	5,4949	0,0830	3,3633	0,0464
	0,03	5,5045	0,0831	3,5447	0,0458
	0,05	5,5742	0,0842	3,4099	0,0471
	0,1	5,6359	0,0851	3,4863	0,0481
Тест 2					
$\varphi_2(t)=e^{t/9}-1$ $\psi_2(t)=e^{2t/15}-1$ $f_2(t)=e^{t/20}$	0,01	2,4712	0,0461	2,4712	0,0461
	0,03	2,5380	0,0474	2,5380	0,0474
	0,05	2,6221	0,0489	2,6221	0,0489
	0,1	2,7008	0,0504	2,7008	0,0504

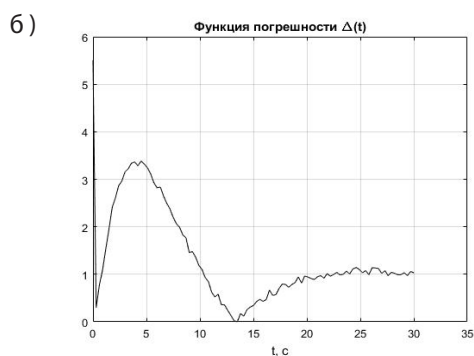
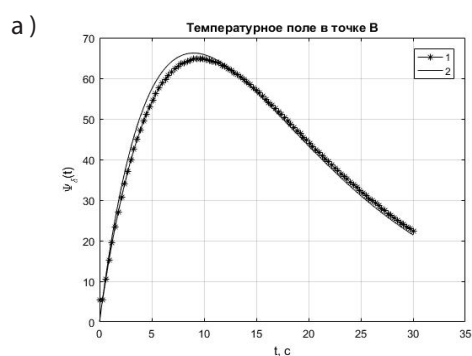


Рис. 2 а. Температурное поле в точке В для теста 1: 1 - температурное поле $\psi_\delta(t)$ в точке В; 2 - тестовая функция $\psi_1(t)$;
Рис. 2 б. График функции температурной погрешности $\Delta(t)$.

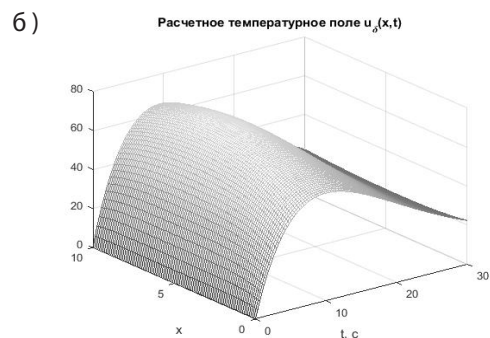
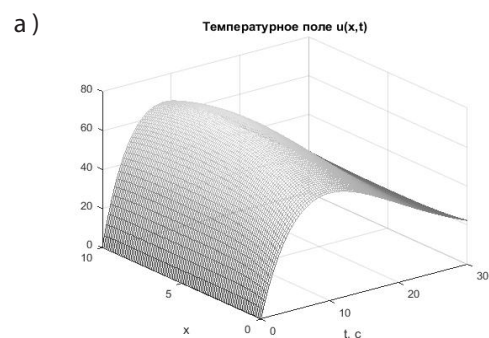


Рис. 3. Температурные поля в линейном объекте для теста 1. а – тестовое температурное поле $u(x,t)$;
б – расчетное температурное поле $u_\delta(x,t)$.

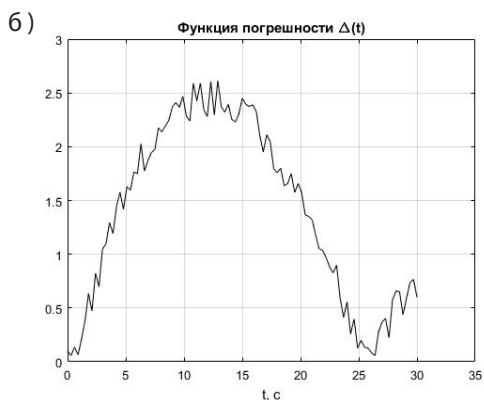
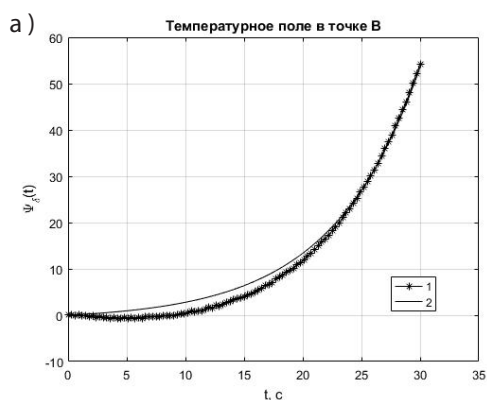


Рис. 4а. Температурное поле в точке В для теста 2: 1 -температурное поле $\psi_{\delta}(t)$ в точке В; 2 - тестовая функция $\psi_1(t)$;
Рис. 4б. График функции температурной погрешности $\Delta(t)$.

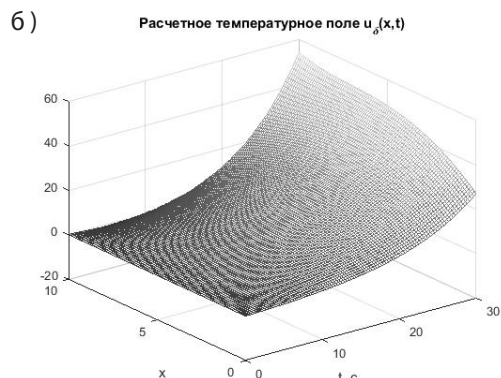
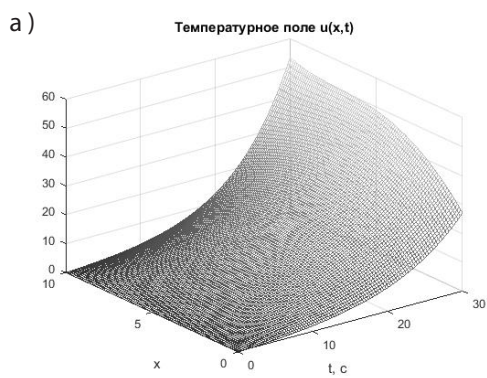


Рис. 5. Температурные поля в линейном объекте для теста 2. а – тестовое температурное поле $u(x,t)$; б – расчетное температурное поле $u_{\delta}(x,t)$.

Заключение

В данной статье предложен метод определения нестационарного температурного поля внутри неоднородного объекта, подвергаемого тепловому воздействию. Математическая модель учитывает теплообменные процессы внутри объекта, представленные в виде функции внутреннего теплового источника, и включает неоднородное уравнение параболического типа, начальные, а также граничные условия, формируемые из результатов измерений температуры вблизи границы.

В работе предложен метод редуцирования задачи (1)–(4) к интегральному уравнению и численный метод его решения. Результаты вычислительного эксперимента, включающего сравнительный анализ вычисленных значений температуры в контрольной

точке и тестовых значений, подтверждают эффективность, а также устойчивость относительно погрешности исходных данных предложенного метода решения задачи теплопереноса. Результаты эксперимента выявили, что предложенный метод решения интегрального уравнения обладает свойством саморегуляризации, когда возможно найти шаг дискретизации, обеспечивающий устойчивость вычислительной схемы.

Предложенный метод определения температуры позволяет обеспечить доступность информации о внутреннем тепловом состоянии объекта, а также целостность данных в процессе обработки зашумленной исходной измеренной информации путем уменьшения негативного влияния шумов на точность результатов ее обработки.

Литература

1. Тихонов А.Н., Самарский А.А. Уравнения математической физики: учеб. пособие. 6-ое изд., испр. и доп. Москва: Изд. МГУ, 1999. – 735 с.

2. Лаврентьев М.М. Условно-корректные задачи для дифференциальных уравнений / Лаврентьев М.М. – Новосибирск: НГУ, 1973. – 71 с.
3. Алифанов О.М. Обратные задачи теплообмена. Москва: Машиностроение, 1988. – 280 с.
4. Самарский А.А., Вабищевич П.Н. Вычислительная теплопередача. Москва: Едиториал УРСС, 2009. – 784 с.
5. Кабанikhин С.И., Шишленин М.А. Прямые и интегральные методы решения обратных и некорректных задач // Сибирские электронные математические известия. 2008. Т.5, № 2. – С. 595-608.
6. Королев Ю.М., Ягола А.Г. Оценка погрешности в линейных обратных задачах при наличии априорной информации // Выч. методы и программирование: новые выч. технологии. 2012. Т.13. №1(25). – С.14–18.
7. Вабищевич П.Н., Васильев В.И. Выбор шага при численном решении краевых задач для параболических уравнений // Журнал вычислительной математики и математической физики. 2017. Т. 57. № 5. – С. 842–853.
8. Мацевитый Ю.М. Обратные задачи теплопроводности. Методология. Киев: Наукова думка, 2002. – 408 с.
9. Марчук Г.И. Методы вычислительной математики. СПб: Лань, 2009. – 608 с.
10. Вабищевич П.Н., Васильев В.И. Вычислительная идентификация младшего коэффициента параболического уравнения // Доклады Академии наук. 2014. Т. 455. № 3. – С. 258.
11. Самарский А.А. Введение в теорию разностных схем. Москва: Наука, 1971. – 736 с.
12. Табаринцева Е.В., Менихес Л.Д., Дрозин А.Д. О решении граничной обратной задачи для параболического уравнения методом квазиобращения // Вестник Южно-Уральского университета. Серия: Математика, Механика, Физика. 2012, № 6. – С. 8–13.
13. Yaparova N. Numerical Methods for Solving a Boundary Value Inverse Heat Conduction Problem // Inverse Problems in Science and Engineering. 2014. Vol.22, no 5. – P. 832–847.
14. Прилепко А.И. Корректность обратной задачи об источнике для параболических систем // Дифференциальные уравнения. 2004. т. 40. № 11. – С. 1540–1547.
15. Diligenskaya A. N., Rapoport E. Y. Method of minimax optimization in the coefficient inverse heat-conduction problem // Journal of Engineering Physics and Thermophysics. 2016. Vol. 89, Issue 4. – P. 1008–1013.
16. Cialkowski M., Grysa K. A sequential and global method of solving an inverse problem of heat conduction equation // Journal of Theoretical and Applied Mechanics. 2010. Vol. 48, no.1. – P. 111-134.
17. Якимов А.С. Аналитический метод решения краевых задач. Томск: Изд-во Том. ун-та, 2011. – 199 с.
18. Япарова Н.М., Гаврилова Т.П. Интегральная модель и численный метод определения температуры при линейном теплопереносе // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2019. Т.19, №4. С.60-71. DOI: 10.14529/ctcr190406.
19. Деч Г. Руководство к практическому применению преобразований Лапласа и Z-преобразования. Москва: Наука, 1971. – 288 с.

References

1. Tihonov A.N. Samarskij A.A. Uravneniya matematicheskoy fiziki [Equations of Mathematical Physics], Moscow: Publishing of the Moscow State University, 1999. – 799 p.
2. Lavrentiev M.M. Uslovno korrektnye zadachi dlya diferentsialnykh uravneniy [Conditionally Correct Problems for Differential Equations], Novosibirsk: Publishing of Novosibirsk Government University, 1973, – 71 p.
3. Alifanov O.M. Obratnye zadachi teploobmena [Inverse Heat Transfer Problems]. Moscow: Mashinostroenie, 1988. – 280 p.
4. Samarskij A.A., Vabishchevich P.N. Vychislitelnaya teploperedacha [Computational Heat Transfer]. Moscow: Editorial URSS, 2009. – 784 p.
5. Kabanikhin S.I., Shishlenin M.A. Direct and Integral Methods for Solving Inverse and Ill-posed Problems [Prямые i integralnyye metody resheniya obratnykh i nekorrektnykh zadach]. Sibirskie elektronnyye matematicheskiye izvestiya. 2008, vol. 5, no. 2. – P. 595–608.
6. Korolev Yu.M., Yagola A.G. Error Estimation in Linear Inverse Problems in the Presence of a Priori Information [Otsenka pogreshnosti v lineynykh obratnykh zadachakh pri nalichii apriornoy informatsii]. Vych. metody i programmirovaniye: novyye vych.tekhnologii. 2012, vol. 13, no. 1(25). – P. 14–18.
7. Vabishchevich P.N., Vasilyev V.I. Step Selection for Numerical Solution of Boundary Value Problems for Parabolic Equations [Vybor shaga pri chislennom reshenii krayevykh zadach dlya parabolicheskikh uravneniy]. Zhurnal vychislitelnoy matematiki i matematicheskoy fiziki. 2017, vol. 57, no. 5. – P. 842–853.

8. Matsevityy Yu.M. Obratnyye zadachi teploprovodnosti. Metodologiya [Inverse Problems of Thermal Conductivity. Methodology] Kiyev: Naukova dumka, 2002. – 408 p.
9. Marchuk G.I. Metody vychislitelnoy matematiki [Methods of Computational Mathematics]. SPb: Lan, 2009. – 608 p.
10. Vabishchevich P.N., Vasilyev V.I. Computational Identification of the Lowest Coefficient of a Parabolic Equation [Vychislitelnaya identifikatsiya mladshogo ko-effitsiyenta parabolicheskogo uravneniya]. Doklady Akademii nauk, 2014, vol. 455, no. 3. – P. 258.
11. Samarskiy A.A. Vvedeniye v teoriyu raznostnykh skhem [Introduction to the Theory of Difference Schemes] Moskva: Nauka, 1971. – 736 p.
12. Tabarintseva E.V., Menikhes L.D., Drozin A.D. On Solving the Boundary Inverse Problem for a Parabolic Equation by the Quasi-Inversion Method [O reshenii granichnoy obratnoy zadachi dlya parabolicheskogo uravneniya metodom kvaziobrashcheniya]. Vestnik Yuzhno-Uralskogo universiteta. Seriya: Matematika. Mekhanika. Fizika, 2012, no. 6. – P. 8–13.
13. Yaparova N. Numerical Methods for Solving a Boundary Value Inverse Heat Conduction Problem. Inverse Problems in Science and Engineering, 2014, vol.22, no 5, pp. 832-847. DOI: 10.1080/17415977.2013.830614.
14. Prilepko A.I. Correctness of the Inverse Source Problem for Parabolic Systems [Korrektnost obratnoy zadachi ob istochnike dlya parabolicheskikh]. Differentsialnyye uravneniya, 2004, vol. 40, no. 11. – P. 1540–1547.
15. Diligenskaya A. N., Rapoport E. Y. Method of minimax optimization in the coefficient inverse heat-conduction problem. Journal of Engineering Physics and Thermophysics, 2016, vol. 89, Issue 4. – P. 1008–1013.
16. Cialkowski M., Grysa K. [A sequential and global method of solving an inverse problem of heat conduction equation]. Journal of Theoretical and Applied Mechanics, 2010, vol. 48, no.1. – P. 111–134.
17. Yakimov A.S. Analiticheskiy metod resheniya krayevykh zadach [Analytical Method for Solving Boundary Value Problems]. Tomsk: Publishing of the Tomsk State University, 2011. – 199 p.
18. Yaparova N.M., Gavrilova T.P. Integral Model and Numerical Method for Determining Temperature in Linear Heat Transfer [Integralnaya model i chislennyy metod opredeleniya temperatury pri lineynom teploperenose]. Vestnik YuUrGU. Seriya «Kompyuternyye tekhnologii. upravleniye. radioelektronika», 2019, vol. 19, no. 4, pp. 60-71. DOI: 10.14529/ctcr190406.
19. Dech G. Rukovodstvo k prakticheskomu primeneniyu preobrazovaniy Laplasy i Z-preobrazovaniya [Guide to the Practical Application of Laplace Transforms and Z-transforms]. Moscow: Nauka. 1971. – 288 s.

ЯПАРОВА Наталья Михайловна, кандидат физико-математических наук, доцент, заведующий кафедрой вычислительной математики и высокопроизводительных вычислений ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080 Челябинск, проспект Ленина, 76. E-mail: iaparovam@susu.ru.

ГАВРИЛОВА Татьяна Петровна, старший преподаватель кафедры вычислительной математики и высокопроизводительных вычислений ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080 Челябинск, проспект Ленина, 76. E-mail: gavrilovatp@susu.ru.

YAPAROVA Natalia Mikhailovna, Ph.D. in math, Associate Professor, Head of Department of Computational Mathematics and High-Performance Computing, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: iaparovam@susu.ru.

GAVRILOVA Tatiana Petrovna, Senior Lecturer of Department of Computational Mathematics and High-Performance Computing, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: gavrilovatp@susu.ru.



ЭВОЛЮЦИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ВИДЕОИГРАХ

В статье рассмотрены видеоигры как уникальное явление в информационной среде, развитие технологий защиты и методов несанкционированного доступа в видеоигровой индустрии со времен появления первой видеоигры и начала становления индустрии до настоящего времени. Представлены поэтапное изменение систем взаимодействия с видеоиграми, технические особенности как аппаратной, так и программной защиты, которые использовали разработчики видеоигр и компании, производящие платформы для них. Изучены приёмы и методы взлома этих систем защиты, инциденты мировых масштабов. Показано, как ошибки и недочёты в безопасности предыдущих поколений видеоигровых приставок повлияли на становление и развитие систем безопасности в последующих поколениях. Рассмотрен процесс централизации и обобщенности систем обеспечения сохранности данных пользователей в современном мире.

Ключевые слова: система защиты информации, видеоигра, программная защита информации, аппаратная защита информации, система безопасности, нелегальное программное обеспечение.

Anfinogenov M. V., Antyasov I. S.

EVOLUTION OF INFORMATION SECURITY SYSTEMS IN VIDEO GAMES

This article covers the video games as a unique phenomenon in the information environment, the development of security technologies and unauthorized access methods since the first video game release until the position of the video game industry in our time. Represented a step change in the interaction systems, the technical features of both hardware and software security which were used by video game developers and companies producing platforms. The analysis of the hacking techniques and methods intended for these protection systems and related global incidents is made. Illustrated the formation and development of security systems of the video game consoles of subsequent generations under the influence of the mistakes and shortcomings in the data security of the prior console generations. The process of centralization and generalization of the user data integrity systems in the modern world is considered.

Keywords: information security system, video game, software information security, hardware information security, safety system, unlicensed software.

Видеоигровая индустрия на данный момент является крупнейшей медиаиндустрией в мире с годовым оборотом в \$148.8 млрд, а системы защиты в видеоиграх очень комплексны и разнообразны, но так было далеко не всегда. Первая видеоигра возникла в 1940 году. Это был игровой автомат Nimatron, который представлял собой электронно-релейную машину для игры в «Ним», где игрок гасит лампы в определенном порядке по очереди с компьютером (рис. 1). Кто погасит последнюю лампу – выигрывает. Данный автомат не был коммерческим, а был скорее демонстрационным. Устройство работало на релейной схеме, и создатель Эдвард Кондон продемонстрировал его на всемирной выставке «Мир Завтрашнего дня» в Нью-Йорке. Он рассчитывал на то, что его аппаратом заинтересуются технологические компании, но хотя аппарат не был коммерческим, в него сыграли более ста тысяч человек, 90% из которых не смогли обыграть компьютер. Так как Эдвард никак не монетизировал свое изобретение, а предложений о сотрудничестве он не получил – его идея стала финансовым провалом компании Westinghouse Electric, а дальнейшее развитие стало невозможным. Несмотря на финансовую несостоятельность Nimatron стал отправной точкой в игровой индустрии. Этот автомат не имел никаких потребностей в обеспечении безопасности.

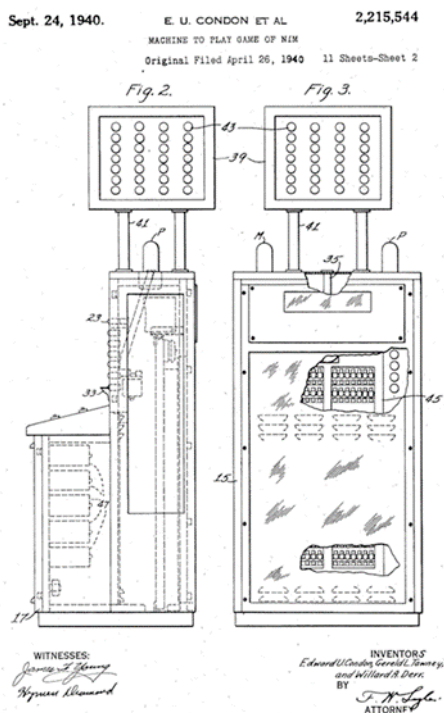


Рис. 1. Схема игрового автомата Nimatron

В последующие 20 лет хоть и создавались прототипы таких игровых автоматов как крестики-нолики, теннис, шахматы, но они были невероятно дорогими, громоздкими и чаще всего существовали в одном экземпляре в университетах, где и были созданы. Основное развитие технологий видеоигр произошло благодаря государственным заказам на обучающие симуляторы для военных.

После массового распространения компьютеров IBM серии 700, которые стали революционными в начале 1960-х годов, множество программистов стали пробовать свои силы в создании простых игр на этой платформе. Игра spasewar (рис. 2), созданная Стивом Расселом стала настоящим прорывом в игровой индустрии, так как была увлекательной и простой в освоении. Игра была примитивной в своей графике и механиках, но увлекательность процесса вместе с ощущением того, что ты участвуешь в космической битве, вызывала фурор у пользователей. Никаких систем защиты эта игра не имела, поэтому она очень быстро распространилась на множество других компьютеров серии IBM 700. Стив Рассел не патентовал свою разработку и в результате не получил со своей игры никаких дивидендов. Популярность spasewar и других игр показала, что видеоигры должны иметь защиту от взлома и копирования, так как могут пользоваться большой популярностью, несмотря на маленький процент населения, у которого на тот момент был доступ к компьютерам IBM 700.



Рис. 2. Spacewar на компьютере PDP-1

Это дало толчок к развитию аркадных автоматов. Несмотря на дороговизну производства, их начали выпускать крупнейшие компании развлекательной индустрии, начиная с конца 1960-х годов, так как увидели возможность для освоения нового рынка. Первые

аркадные автоматы приносили большие убытки, но компании стремились осваивать технологии раньше остальных, чтобы первыми закрепиться в новой отрасли. Многие компании позже полностью переключились на производство видеоигр: такие компании, как Konami, Nintendo и Namco (в данный момент Bandai Namco) до сих пор являются крупными представителями видеоигровой индустрии. У первых аркадных автоматов также была цель приобщить общество к новому виду развлечений, ведь стоимость за одну игру едва покрывала затраты на электроэнергию и износ деталей. Основой для первых аркадных автоматов служили слот-машины из казино (также из-за того, что первые производители аркадных автоматов занимались в том числе производством слот-машин для залов азартных игр), как следствие – все системы защиты казино-автоматов сводились к особому строению корпуса и системы вброса монет с защитой от взлома, в том числе «монет на верёвочках». Эти аркадные автоматы были изолированными от любых вмешательств, потому что каждый автомат имел специализированное аппаратное обеспечение, которое было невозможно или чрезвычайно трудоёмко модифицировать на любых компьютерах того времени. Единственной возможностью несанкционированного доступа была кража самих автоматов, что было крайне затруднительно, учитывая их габариты. Так появились первые системы обеспечения безопасности в видеоиграх. Замкнутость таких систем делала нецелесообразными все попытки взлома и несанкционированного доступа.

В то же время стали выпускаться более универсальные персональные игровые системы. В 1972 году появилась домашняя приставка Magnavox Odyssey, с которой началось первое поколение игровых приставок. Она работала на диодно-транзисторной логике с использованием диодов и дискретных транзисторов. Такая приставка могла выводить на экран три квадратных точки и вертикальную линию, двумя точками можно было управлять с помощью контроллеров, а третья управлялась системой. С играми шли полупрозрачные пленки с цветными пластиковыми накладками на экран телевизора, и со сменой игрового картриджа необходимо было менять эту пленку. Данная приставка была скорее рекламой самих телевизоров компании Magnavox (подразделение компании Philips),

чем полноценным коммерческим продуктом, поэтому все доступные игры шли сразу с приставкой. Из-за этого потребности в обеспечении безопасности попросту не было. Сами же картриджи представляли собой переключки между разными контактами, запускающими одну из игр, которые уже были в Magnavox Odyssey.

В этом же году вышел легендарный аркадный автомат PONG (рис. 3), который стал первым коммерчески успешным игровым автоматом. Высокая популярность стала причиной его портирования на домашние игровые приставки и привела к бурному развитию домашних игровых приставок. Приставка PONG имела всего одну игру и была уменьшенной версией аркадного автомата. Все приставки первого поколения были узкоспециализированы и дороги в производстве. Они не имели никаких причин для взлома, и по причине своей «узконаправленности» стали довольно быстро уходить с рынка. Единственной распространенной возможностью несанкционированного доступа была модификация схем сломанных приставок, так как вскрывать рабочую приставку было попросту нецелесообразно. Но таких модификаций было настолько мало, что никакого значительного финансового вреда они не наносили, поэтому производители не обращали на это внимания.



Рис. 3. Аркадный автомат PONG

В 1976 году началось второе поколение домашних приставок, начавшееся с выходом первой микропроцессорной приставки Fairchild VES. В новых системах устройство уже было восьмиразрядным компьютером. И если примитивные картриджи первого поколения были набором соединений между контактами самой приставки, то второе поколе-

ние перешло на сменяемые микрочипы, которые кодировались с помощью дискретной логики. Так называемые «восьмибитные» системы позволили расширить возможности в

но было появиться на экране. И если в тайминге при этом возникала ошибка, то на экране появлялись множественные артефакты, которые называли «гонка за лучом».



Рис. 4. Игровая приставка Atari 2600 и процессор MOS Technology 6507

разы, так как у новых приставок появилась полноценная графика и даже своя звуковая система. И за то, и за другое отвечал отдельный телевизионный чип, встроенный в архитектуру. Со второго поколения приставок началось активное развитие несанкционированного взлома видеоигр, которое в основном было завязано на копировании микросхем. По современным меркам строение картриджей выглядело примитивным. Главным элементом был микрочип, подделка которого стала главной задачей пиратских объединений, впервые появившихся именно в это время. Несанкционированное производство картриджей позволило пользователям гораздо дешевле опробовать новинки игрового рынка.

Впервые в истории игровое пиратство существенно повлияло на прибыль официального производителя. Больше всего пострадала приставка Atari 2600, которая была лидирующей на рынке. В качестве процессора использовался MOS Technology 6507 (рис. 4) с частотой 1.19 МГц, который был урезанной версией MOS Technology 6502, стоявших на персональных компьютерах Apple I и Apple II. Оперативной памяти было всего 128 байт, в которую включался и стек вызовов, и полное состояние игрового мира. Примечательно, что в данной системе попросту не хватало памяти для экранного буфера, который бы загружал кадр перед отправкой его на экран. Буфер сохранял только пиксель последующего положения луча на экране, при этом после прохождения последней активной строки был кадровый гасящий импульс. В этот промежуток игра обрабатывала входные данные для обновления информации о том, что долж-

Для удешевления самой консоли был выбран самый недорогой интерфейс картриджей. Он имел 12 адресных линий, благодаря чему использовалось только 4 Кб памяти картриджа. Это делало невозможным создать программную защиту, но компания Atari и не рассчитывала на то, что будут выпускаться нелегальные картриджи, так как массовых инцидентов до этого не было. На волне успеха даже крупные компании стали делать свои видеоигры на эту систему, так как отношение к игровой приставке было как к обычному проигрывателю. Если компания выпускает DVD-диски, она не обязана платить отчисления всем DVD-проигрывателям, которые могут запустить их диск. Такие отношения к лицензиям на Atari 2600 привели к большим убыткам и множеству судебных разбирательств, а рынок видеоигр был переполнен настолько плохими по качеству играми, что доверие к Atari 2600 стало стремительно падать. Более того, злоумышленники создали клон данной приставки со встроенной внутренней памятью, в которой уже было заложено несколько десятков игр. Atari 2600 продавалась в США, Франции, Германии и Японии, а клон RAMBO распространялся во всем остальном мире. На упаковке этой приставки был актер Сильвестр Сталлоне в образе персонажа из одноименного фильма Рэмбо, которого также разместили незаконно. Поэтому на последующих приставках этого поколения, таких как Emerson Arcadia 2001, Vectrex и ColecoVision была сделана особая форма картриджа и слота под него, которую сложно воспроизвести без особого оборудования, хотя и это вряд ли спасло их от подделки. Малая популярность других приставок по срав-

нению с Atari 2600 свела на нет попытки следующего взлома этого поколения приставок.

В 1983 году после кризиса игровой индустрии стали выходить игровые устройства третьего поколения. Восьмиразрядные игровые системы ознаменовали новую эпоху видеоигр, когда они стали очень массовым явлением в обществе. В этом же году появляется понятие «платформодержатель», означающее, что производители программного обеспечения для специализированных платформ должны соблюдать лицензионные условия и быть юридически оформлены с компанией, выпускающей систему для легального выпуска своей продукции. Самыми знаковыми игровыми системами в этом поколении были японские приставки Famicom и Sega Master System, которых было продано суммарно более восьмидесяти миллионов экземпляров. Такая большая популярность привела к огромному развитию нелегальных копий. Нарушение авторских прав в игровой индустрии достигло своего пика именно в третьем поколении. Были целые официально-оформленные компании, которые в огромных масштабах выпускали копии, как картриджей, так и целых приставок. Более того, многие разработчики сами создавали и продавали нелегальные игры, чтобы не отчислять процент от продаж компаниям Sega и Nintendo. Началось настоящее противостояние систем защиты и взлома.

Famicom (сокращение от Family Computer), выпускавшаяся в Северной Америке и Европе под названием Nintendo Entertainment System (NES) была лидирующей на рынке (рис. 5) и имела выдающиеся технические характеристики. В особенности, систему выделял восьмибитный процессор Ricoh, также совмещающий в одном кристалле звуковой процессор и контроллер DMA,



Рис. 5. Версия NES для Северной Америки

ещё сильнее выделялся видеоконтроллер Ricoh, поддерживающий сорок восемь цветов и «спрайты» на аппаратном уровне.

Встроенная комплексная lock-out аппаратная система защиты 10NES состояла из двух частей комплекса Checking Integrated Circuit (CIC). И чип блокировки внутри NES, и чип на картридже являлись частями одной схемы (рис. 6). Чип внутри NES, действовал как замок, а чип в картридже – как ключ. Разница была лишь в том, как они подключены. Система составлена таким образом, что выход одного CIC подключен к входу другого, и наоборот. Замок и ключ повышают напряжение до +5 В внутри NES и заземляются на картридже. Оба имеют одни и те же тактовые импульсы 4 МГц, передавая их на контакт 6. Контакт RESET на ключе подключен к SLAVE CIC RESET на замке. Вывод RESET замка подключен к шине сброса системы. Это можно продемонстрировать, вставив игру в приставку с уже включенной системой. NES не будет работать, пока не будет нажата кнопка Reset, сбросив блокировку CIC, которая в свою очередь сбрасывает ключ. CPU & PPU RESET не подключен на ключе, а на замке он подключен к контактам сброса CPU и PPU. Контакты 11 – 15 заземлены на оба CIC в NES; они фактически используются в многопользовательских системах, так что в одной системе могут быть адресованы несколько CIC. Таким образом, вся цепь переходит на + 5 В и запускает игру.

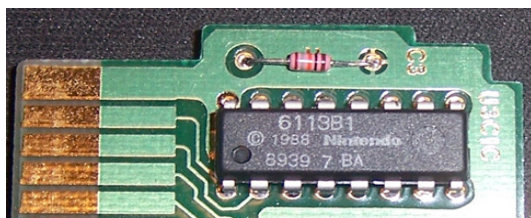


Рис. 6. Чип безопасности 10NES для Famicom

Как только система выходит из режима загрузки, замок посылает соответствующие сигналы сброса и инициализации на ключ. Затем ключ должен вернуть правильный ответ, в противном случае блокировка будет удерживать CPU & PPU RESET в режиме ожидания с импульсами прямоугольной волны частоты 1 Гц. После прохождения проверки замок может сбросить ключ, оба CIC синхронизируются друг с другом, а система запускается.

Комплекс состоит из четырехбитного микроконтроллера SM590, находящегося в са-

мой приставке, который проверял вставленный картридж на предмет аутентификации. Если ключ не проходил проверку, то Famicom просто перезагружалась до тех пор, пока чип не пройдет проверку. Такая система стала довольно эффективной и обеспечивала не только предотвращение запуска нелегального программного обеспечения, но и полный контроль над выпускаемой продукцией, включая возможность региональной блокировки игр, не предназначенных для выхода в определенных странах. Региональная блокировка никак не считывала геопозицию, поэтому для разных стран выпускали разные версии Famicom, которые отличались в том числе и региональными данными в микроконтроллере. Производители нелегальной продукции из-за невозможности создать чипы с подходящими ключами стали обходить систему безопасности как на уровне выше, так и на уровне ниже этого чипа. В картриджах стали встраивать системы подключения через оригинальный картридж, таким образом владелец NES мог подключить пиратский картридж к любому лицензионному, и система защиты распознавала чип именно с лицензионного, но запускала при этом нелегальный. Помимо этого, появилось множество аппаратных клонов самой приставки. Они имели множество модификаций печатных плат с интегральными схемами, объединенными чипами и другими методами удешевления производства. Как и в случае с Atari 2600 клоны приставки были распространены в тех странах, где Famicom официально не выпускалась. Более того, почти в каждой стране от стран СНГ и Южной Америки до Южной Африки и даже Северной Кореи были свои аппаратные клоны NES. В одной только России «скопированной» приставки Dendy было продано более двух миллионов экземпляров. Общество того времени настолько не привыкло к лицензированию, что отдельные магазины для клонов, реклама по телевизору и даже отдельные телепередачи, посвященные этим приставкам, были абсолютно нормальным явлением, тем более, что аппаратные клоны не имели системы защиты и запускали любые картриджи. По неофициальным данным количество аппаратных клонов было примерно равно количеству проданных приставок Famicom. Несмотря на это, финансовые потери компании из-за пиратства были довольно малы, так как нелегальных картриджей было довольно мало, а клоны в ос-

новом продавались в странах, где Nintendo Entertainment System никогда официально не выпускались.

Остальные приставки третьего поколения, включая Sega Master System и Atari 7800 имели очень схожую архитектуру и системы защиты. А в силу подавляющей популярности Famicom практически не подвергались несанкционированному взлому.

Четвертое поколение игровых приставок появилось в 1987 году с выпуском PC EngineTurboGrafx-16 от компании NEC, которая стала первой шестнадцатиразрядной игровой системой. Популярностью данная игра не пользовалась, поэтому новое поколение вышло в массы в 1988 – 1990 годах с выходом приставок Super Nintendo Entertainment System и Sega Mega Drive (рис. 7). В это же самое время появились портативные игровые консоли, такие как Nintendo Gameboy, Sega Game Gear и Atari Links. Игры окончательно перестали быть нишевым продуктом, одними только портативными Gameboy в поездках и перелётах пользовались многие публичные люди, такие как группа Metallica, актёр Робин Уильямс, политик Хиллари Клинтон и множество других. В домашних приставках этого поколения системы защиты немного изменились. Рассмотрим систему защиты в двух основных системах этого поколения.



Рис. 7. Японская версия Sega Mega Drive

Sega Mega Drive уже имела в своем составе 16/32-разрядный процессор Motorola 68000 и дополнительный 8-битный процессор Zilog Z80, отвечающий за управление звуковыми устройствами. 72 Кб оперативной памяти и 64 Кб видеопамати значительно расширили возможности консоли. Она уже могла отображать на экране 64 цвета из палитры в 512-оттенков. Для обеспечения безопасности система использовала встроенную в материнскую плату TradeMark Security System. Использовался двухбитный чип, который имел две стадии проверки. При запуске игры

TradeMark Security System проверяет память ПЗУ картриджа по адресу \$100, есть ли по этому адресу слово «SEGA» в кодировке ASCII. За этот шаг отвечала программная часть системы защиты, и после прохождения этой части на экран выводилось сообщение «Produced By License From Sega Enterprises Ltd.». Система проверки держалась в строгой секретности, что сработало очень хорошо, так как взломать эту систему удалось только после основного периода продаж приставки. Далее шла уже привычная система проверки с помощью контроллера ввода-вывода, который ограничивал доступ к порту данных VDP, если в чипе картриджа не содержалось слова «SEGA» по адресу \$A14000. Новые картриджи имели структуру, которая не позволяла подключить через них нелегальный картридж для обхода второй стадии, но они появились намного позже из-за утечек информации от официального издателя Absolute Entertainment и не сильно повлияли на прибыль компании Sega.

Приставка Super Nintendo Entertainment System (SNES) в свою очередь использует незначительно модифицированную Checking Integrated Circuit, а форма картриджей также была изменена таким образом, чтобы подключить через них нелегализованный картридж было практически невозможно, не испортив оригинальный картридж. Но в это же время появилось такое понятие как «прошивка» игровой приставки, которая заключалась в удалении чипа проверки безопасности и запаивания контактов на месте этого чипа. Этот способ позволял запускать на ней любое нелегализованное программное обеспечение, что сильно развязало руки производителям пиратских копий видеоигр.

Примечательно, что именно в этом поколении появились в продаже отдельные подключаемые устройства, читающие компакт-диски, так как очень малого объема памяти картриджей явно не хватало для реализации новых амбиций видеоигровых разработчиков.

Пятое поколение берет свое начало в 1993 году. После очередного кризиса игровой индустрии произошел невероятный рост как количества компаний, выпускающих свои платформы, так и количества видеоигровых студий. Игры совершили огромный скачок, потому что появилась трехмерная графика, возможности расширились в сотни раз за счет использования компакт-дисков, которые вмещали куда больше памяти и были бо-

лее износостойкими, а увеличенные мощности позволили создать полноценную операционную систему в игровых приставках.

В тот момент игровая индустрия разрослась настолько, что рассмотреть системы защиты всех игровых консолей и самих игр в рамках этой работы попросту невозможно, поэтому рассмотрим только игровую консоль Sony PlayStation (рис. 8) и Персональный Компьютер, которые были двумя самыми популярными игровыми системами во время пятого поколения игровых приставок.



Рис. 8. Sony Playstation

Сначала рассмотрим средства защиты на консоли PlayStation, которой было продано более ста миллионов экземпляров. Sony PlayStation имела центральный процессор MIPS R3000A и 32-разрядный RISC-микропроцессор, работающий на частоте 33,9 МГц с производительностью в 30 MIPS. Чип содержал контроллер для работы с трехмерной графикой (Geometry Transformation Engine) с производительностью в 66 MIPS, который находился на одном кристалле с центральным процессором. Память основного ОЗУ была 2 Мб, видео ОЗУ – 1 Мб, а звукового ОЗУ – 512 Кб. У этой приставки была региональная блокировка, подобная тем, которые рассматривались ранее. Данная блокировка, как и раньше, одновременно служила для проверки лицензии диска. Лицензионные игры PlayStation имели отмеченную зону в крайней области диска, которая содержала информацию о регионе, эта информация состояла из букв SCEX, где X – область диска: A – для Америки (SCEA); E – для Европы (SCEE); Я – для Японии (SCEI); W – для тестирования разработчиками (SCEW).

В случае если консоль определенного региона не обнаружит в своей области нужной кодировки, то система не запустится. Нелицензионные диски не имеют такой метки, так как обычные дисководы не могут прочесть эту часть диска, поэтому система также откажется загружать игру.

Как и в Sega Mega Drive текст на экране «Лицензировано Sony Computer Entertainment America SCEA TM» находится не в самой системе, а на диске в области проверки лицензионности. Система читает этот текст с диска и помещает его в логотип загрузки, что позволило делать каждой игре собственные загрузочные экраны.

Злоумышленники использовали два способа обойти эти ограничения. Первый – с помощью специального диска Import Player. На этом диске использовался «эксплойт», который представляет собой использование способности системы играть в многодисковые игры. Некоторые игры не помещались на один носитель и в какой-то момент выводили сообщение о необходимости сменить игровой диск. Когда пользователь меняет диски, система не выходит в режим загрузки, поэтому вторая проверка вставленного диска не выполняется. Но происходит первичное считывание, которое решает модифицированный чип безопасности. Модификация чипа была схожа с «прошивкой» Super Nintendo Entertainment System с единственным отличием, что чип не вынимался с запаиванием контакта, а к нему припаивался элемент, имитирующий региональный код, и благодаря этому региональную блокировку была возможность обойти. Второй метод был гораздо более надежный, но схожий с добавлением пользовательской загрузки, только в этом случае правильный загрузочный текст был введен в компакт-диск, что позволяло загружать его напрямую.

Другая мера, которая была реализована – обнаружение модифицированных чипов. Она потребовала внедрения нового аппаратного обеспечения, поэтому она была доступна только в более поздних версиях устройства. Кроме того, это мера исполнялась не кодом системы, а кодом игры, поэтому код должен был быть внедрен в саму видеоигру, то есть компакт-диски старых ревизий не могли использовать данную функцию.

Обнаружение модифицированного чипа происходит следующим образом: обычный чип проверяет региональный код компакт-диска (SCEX, как мы видели выше), но новые диски также в ответ проверяют успешность региональной проверки, поэтому если в системе есть модифицированный чип, то официальные игры просто не будут на ней запускаться.

Обойти эту защиту можно было с помо-

щью еще одного внедряемого чипа (у которого есть патч для обнаружения «антимодчипа») или путем исправления кода игры перед нелегальной записью. Эти способы уже были куда менее популярны, так как были очень трудозатратны.

Несмотря на то, что у этой игровой консоли уже были модули подключения к интернету, закрытость системы и провальные попытки взлома не дают возможности узнать о системах интернет-защиты на этой приставке.

Если обратить внимание на игровой рынок персональных компьютеров, то системы взлома были куда более разнообразны из-за большей открытости операционной системы, а отсутствие специализированной системы, такой как игровая консоль попросту не давали играм централизованной защиты. Так как в это время даже не было специализированного программного обеспечения по защите видеоигр, каждая игровая студия была вынуждена самостоятельно создавать программное обеспечение для защиты своей игры от взлома.

Игровое пиратство и несанкционированный доступ к данным в компьютерных играх девяностых годов были настоящей катастрофой, масштабы которой удалось оценить только спустя несколько лет. Тот факт, что пиратских копий было в разы больше лицензионных дисков, стал наименьшей проблемой безопасности, например, в России официальными были всего пять процентов от всех продаваемых компьютерных видеоигр. Но если огромное количество уязвимостей в однопользовательских играх вело к их взлому для незаконного распространения копий, то взлом аккаунтов набирающих популярность онлайн-игр вел к несанкционированному доступу к персональным данным пользователей, банковским реквизитам и даже контролю над компьютерами пользователей. Из-за слабого развития интернет-культуры и онлайн-гейминга в период с 1990 до 2000 года были похищены данные более чем трех миллионов пользователей по всему миру с помощью фишинговых сайтов, взлома игровых серверов с данными и использования уязвимостей игрового кода. С такими последствиями сталкивались онлайн-игры всех размеров и жанров, ведь даже такие «мастодонты онлайн» как Ultima Online, Lineage, Neverwinter Nights и The Realm Online испытывали на себе многочисленные взломы через использование найденных уязвимостей. В последующее

время шло развитие, как аппаратных средств защиты, так и программных. Но аппаратные средства, по сути, являлись улучшенными модификациями старых версий, а разбирать все этапы улучшения программной защиты было бы просто нецелесообразно в рамках одной статьи по причине большого объема информации, поэтому далее рассмотрим современные средства защиты видеоигр.

В настоящее время все видеоигровые платформы содержат куда больше информации о пользователе, чем когда бы то ни было. Это могут быть данные банковских карт, электронная почта, адрес проживания и даже паспортные данные (как например в Китае). В Российском законодательстве видеоигры должны рассматриваться как информационные системы персональных данных (ИСПДн) и никак не отделяются. В мировой практике практически нет специализированных нормативных документов, регулирующих видеоигры. Но такие документы как общий регламент по защите данных (GDPR), действующий на территории Европейского Союза, были отредактированы с учётом того, что под их регламент попадают видеоигры. При этом данный регламент покрывает требования к ИСПДн большинства стран, поэтому чаще всего игровые студии опираются именно на него.

В данный момент игры имеют куда больше средств защиты, чем раньше, так как основную часть обеспечения безопасности берут на себя компании, производящие игровые консоли и компании-владельцы игровых «лаунчеров», которые представляют собой агрегатор по продаже и запуску видеоигр. Для персональных компьютеров их довольно много: Steam, Epic Games Store, UPlay (рис. 9) и множество других, в то время как на мобильных платформах такие «лаунчеры» создаются самими разработчиками операционных систем, такими как Apple и Google.

Рассмотрим систему защиты «лаунчера» Google Play Market. Система Android имеет средство защиты Google Play Protect, которая сканирует каждое приложение, попадающее в Play Market. Эта система для улучшения функционала использует машинное обучение. Она проверяет все пакеты данных приложения, все файлы и все данные. Не смотря на то, что эта система является одной из передовых, она имеет большое количество уязвимостей и не позволяет разработчикам узнать об этих уязвимостях из документаций. Систе-

ма работает как на уровне принятия приложения в свой магазин, так и на уровне сканирования данных, используемых пользователем.



Рис. 9. Крупнейшие современные лаунчеры

В основе большинства систем защиты, таких как StarForce, которая является одним из крупнейших российских представителей в обеспечении безопасности в видеоиграх, используется преобразование кода в .Net код виртуальной машины, шифрование строк и массивов, преобразование кода в цифровую форму, введение ложных связей, объединение участков кода и другие. Многие системы защиты используют собственный язык программирования для усложнения взлома. В процессе защиты исполняемый файл разбирается на составные части. Составные части исполняемого файла преобразуются с использованием различных технологий защиты. Помимо этого, существует множество методов защищенной «контейнеризации» данных, методов проверки целостности и внешней привязки видеоигры. Из этих инструментов чаще всего и выстраивается комплексная защита. В силу специфики видеоигр, системы защиты, не встроенные в игровую среду разработки или платформу, не могут быть универсальными и вынуждены подстраиваться под каждый проект.

Несмотря на кажущуюся полноценную безопасность, инциденты, связанные с современными игровыми системами, не исчезают. Постоянно находятся новые уязвимости, порождающие новые преступления с хищениями денежных средств, пользовательских данных и целых аккаунтов.

На данный момент одним из наиболее популярных методов взлома является метод reverse engineering, при котором злоумышленник с помощью декомпиляторов «разбирает» код игры для поиска мест потенциальных уязвимостей. После нахождения таких мест нарушитель запускает ботов, которые

проверяют каждое место на непосредственное наличие уязвимостей. Далее создаются уже специализированные боты, которые проверяют каждую найденную уязвимость и используют её. Также зачастую используют запуск видеоигры на виртуальной машине для просмотра кода операционной системы во время работы видеоигры.

Представленное исследование систем защиты в видеоиграх подчеркнуло комплексность развития всех систем и стратегий действий злоумышленников и противодействия им. Возможности систем нарушителей растут, поэтому для правильного выстраивания стратегии обеспечения безопасности необходимо изучать предыдущие системы и опыт

их развития. Потому как в современных продуктах игровой индустрии выяснить реализованные меры практически невозможно из-за того, что системы являются конфиденциальными для поддержания требуемого уровня сохранности данных.

Таким образом, инструменты защиты платформодержателей и разработчиков постоянно совершенствуются для обеспечения приемлемого уровня сохранности информации. Быстрое реагирование на инциденты со стороны видеоигровых разработчиков и соблюдение простых мер информационной безопасности со стороны игроков уменьшает шанс несанкционированного доступа к данным пользователя.

Литература

1. Стивен Л. Кент «The Ultimate History of Video Games» - Three Rivers Press : 2001 – С. 10–624 с.
2. Blake J. Harris «Console Wars» : 2014 – С. 7–244 с.
3. Peter Leigh «The Nostalgia Nerd's Retro Tech: Computer, Consoles & Games.» : 2018 – С. 5–186.
4. Brian J. Wardyga «The Video Games Textbook: History • Business • Technology» : 2018 – С. 6–252.
5. Тристан Донован, Ричард Гэрриот «Replay: The History of Video Games» : 2010 – С. 8–373.
6. Bill Loguidice, Matt Barton "Vintage Game Consoles: An Inside Look at Apple, Atari, Commodore, Nintendo, and the Greatest Gaming Platforms of All Time" : 2014 – С. 5–315.
7. Andy Bossom, Ben Dunning - "Video Games: An Introduction to the Industry" : 2015 – С. 23–30.

References

1. Steven L. Kent «The Ultimate History of Video Games» - Three Rivers Press : 2001 – S. 10–624.
2. Blake J. Harris «Console Wars» : 2014 – S. 7–244 с.
3. Peter Leigh «The Nostalgia Nerd's Retro Tech: Computer, Consoles & Games.» : 2018 – S. 5–186.
4. Brian J. Wardyga «The Video Games Textbook: History • Business • Technology» : 2018 – S. 6–252.
5. Tristan Donovan, Richard Garriott «Replay: The History of Video Games» : 2010 – S. 8–373.
6. Bill Loguidice, Matt Barton "Vintage Game Consoles: An Inside Look at Apple, Atari, Commodore, Nintendo, and the Greatest Gaming Platforms of All Time" : 2014 – S. 5–315.
7. Andy Bossom, Ben Dunning - "Video Games: An Introduction to the Industry" : 2015 – S. 23–30.

АНФИНОГЕНОВ Максим Викторович, студент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080 Челябинск, проспект Ленина, 76. E-mail: anfinogenov.max1997@yandex.ru.

АНТЯСОВ Иван Сергеевич, старший преподаватель кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080 Челябинск, проспект Ленина, 76. E-mail: antiasovis@susu.ru.

ANFINOGENOV Maksim Viktorovich, Student of Department of Information Security, South Ural State University (National Research University). 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: anfinogenov.max1997@yandex.ru.

ANTYASOV Ivan Sergeevich, Senior Lecturer of Department of Information Security, South Ural State University (National Research University). 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: antiasovis@susu.ru.



ФОРМИРОВАНИЕ ВЫСОКОИНФОРМАТИВНОГО ЦИФРОВОГО ОБРАЗА СИГНАЛА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ВРЕМЯ- ЧАСТОТНОГО ПРЕДСТАВЛЕНИЯ И ДВУМЕРНОЙ ЦИФРОВОЙ ФИЛЬТРАЦИИ

В исследовании рассматривается технология формирования высокоинформативного цифрового образа наблюдаемого временного сигнала автоматизированной системы управления (АСУ). Формирование образа сигнала включает этап отображения сигнала на время-частотную плоскость, получение время-частотного изображения сигнала, этап двумерной цифровой фильтрации, этап формирования высокоинформативных компонентов изображения сигнала. Полученный цифровой образ наблюдаемого сигнала АСУ представляет собой сформированные высокоинформативные входные данные для дальнейшего решения широкого круга различных задач с использованием технологий машинного обучения и глубоких нейронных сетей в АСУ промышленных систем. Широкий круг задач с использованием сформированного цифрового образа сигнала предполагает, например, анализ поведения процессов и выявление аномалий в процессах АСУ, реализацию алгоритмов диагностики технического оборудования в составе АСУ, обнаружение изменения в динамике процессов АСУ под воздействием информационных атак.

Ключевые слова: Цифровой сигнал, частотно-временное преобразование, двумерный цифровой фильтр, цифровая свертка, цифровой образ сигнала, АСУ.

FORMATION OF A HIGHLY INFORMATIVE DIGITAL SIGNAL IMAGE OF AN AUTOMATED CONTROL SYSTEM USING TIME-FREQUENCY REPRESENTATION AND TWO-DIMENSIONAL DIGITAL FILTERING TECHNOLOGIES

The study examines the technology of forming a high-informative digital image of the observed time signal of an automated control system (ACS). Formation of the signal image includes the stage of displaying the signal on the time-frequency representation, obtaining the time-frequency image of the signal, the stage of two-dimensional digital filtering, the stage of formation of high-informative components of the signal image. The resulting digital image of the observed ACS signal represents the generated high-informative input data for further solving a wide range of different problems using machine learning technologies and deep neural networks in the ACS of industrial systems. A wide range of tasks using the generated digital image of the signal implies, for example, the analysis of process behavior and identification of anomalies in the process of ACS, the implementation of diagnostic algorithms of technical equipment in the ACS, the detection of changes in the dynamics of the process of ACS under the influence of information attacks.

Keywords: *Digital signal, time-frequency representation, two-dimensional digital filter, digital convolution, digital image of the signal, ACS.*

Введение

В настоящее время актуальным является широкий круг задач в области промышленных систем, связанный с технологией цифровой обработки сигналов, предполагающий, например, анализ поведения процессов и выявление аномалий в процессах АСУ, реализацию алгоритмов диагностики технического оборудования в составе АСУ, обнаружение изменения в динамике процессов АСУ под воздействием информационных атак, цифровая обработка сигналов в системах биометрического контроля доступа на критически важных объектах, находящихся под управлением АСУ, цифровая обра-

ботка сигналов в различных системах человеко-машинного интерфейса, входящих в состав АСУ, в задачах диагностики электронных систем и комплексов, в задачах управления различным техническим оборудованием и процессами в современных промышленных системах [1–11].

Важным этапом в подготовке входных данных для решения широкого круга задач в АСУ промышленных систем с последующим использованием технологий машинного обучения и нейронных сетей является получение цифрового образа исследуемого сигнала технической системы, представляющего собой сформированные высо-

коинформативные входные данные. Именно качество (информативность) подготовленных входных данных влияет на эффективность решаемых задач и принимаемых решений [12–15].

В работе рассматривается модульный алгоритм, реализующий получение высокоинформативного цифрового образа сигнала исследуемой технической системы. Сформированный высокоинформативный цифровой образ наблюдаемого сигнала представляет собой входные данные для дальнейшего применения при решении широкого круга задач в АСУ промышленных промышленных систем с последующим использованием технологии искусственных нейронных сетей и машинного обучения.

1. Этапы предварительной цифровой обработки при формировании цифрового образа сигналов

Для обработки данных в АСУ с использованием технологий искусственных нейронных сетей и машинного обучения требуется качественная подготовка входных данных. Задача подготовки качественных высокоинформативных данных в исследовании реализуется с использованием технологии цифровой обработки сигналов [7–9,11].

Задача преобразования сигнала в изображение актуальна, так как в настоящее время достигнут существенный прогресс в обработке изображений (образов) с использованием технологий с использованием глубоких нейронных сетей и машинного обучения. [1,10,15].

В работе исследуется предлагаемый к применению в АСУ модульный алгоритм, реа-

лизующий преобразование входного (наблюдаемого) сигнала технической системы в подготовленные выходные данные в виде высокоинформативного цифрового образа входного сигнала для дальнейшего применения в АСУ с использованием технологии машинного обучения.

Модули алгоритма реализуют следующие этапы преобразований наблюдаемого входного сигнала: реализация алгоритма цифрового частотно-временного спектрального анализа входного сигнала, двумерная цифровая фильтрация результата частотно-временного преобразования (ЧВП) (формирование адаптивной поверхности ЧВП), выделение информативной части ЧВП, построение изображения скелетона сформированной информативной части ЧВП, реализация сжатия полученного изображения скелетона информативной части ЧВП. Полученное сжатое изображение скелетона является выходным результатом подготовленных выходных данных. Сформированные выходные данные представляют собой высокоинформативный цифровой образ входного исследуемого (наблюдаемого) сигнала.

2. Частотно-временное представление наблюдаемого сигнала

В качестве примера сигнала в исследовании рассматривается аудио сигнал, например, наблюдаемый в системах биометрического контроля доступа или в системах человеко-машинного интерфейса, входящих в состав АСУ.

На рис.1 изображен наблюдаемый аудио сигнал.

Частотно-временное представление (ЧВП)

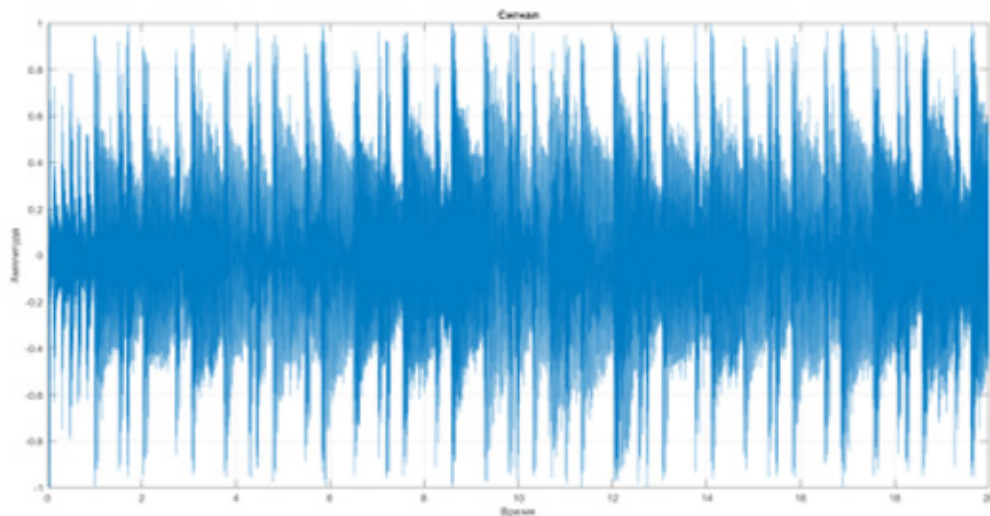


Рис. 1. Временное представление наблюдаемого аудио сигнала

аудио сигнала, представленного на рис. 1, осуществляется в координатах «частота – время – амплитуда», что позволяет получить значительное количество информации о аудио сигнале в частотно-временной области и сформировать его информационные признаки.

Для реализации ЧВП используется технология цифрового спектрального анализа [16–18].

Частотно-временное представление сигнала представляет собой поверхность, где по оси абсцисс располагается время или нормированное время, а по оси ординат – частота или нормированная частота.

ЧВП показывает изменение частотного спектра сигнала в зависимости от времени [16–18].

Результат ЧВП аудио сигнала (рис. 1) представлен на рис. 2.

При формировании ЧВП наблюдаемого сигнала весь анализируемый сигнал (рис. 1)

аудио сигнала имеет избыточную информативность (множество мелких деталей), а также занимает большой объем данных. То есть, результат ЧВП анализируемого сигнала (рис. 1), представленного на рис. 2, 3 в виде изображения, в силу большой избыточности не может использоваться в виде входных данных для решения последующих различных задач с использованием искусственных нейронных сетей и машинного обучения. Необходимо удалить из изображения (рис. 3) несущественные (избыточные данные), занимающие большой объем данных.

3. Двумерная цифровая фильтрация ЧВП сигнала

Для дальнейшей обработки сигнала требуется исключить избыточные данные из массива данных, представленных в виде изображения ЧВП (рис. 3). Для этого ЧВП как двумерный цифровой сигнал пропускается через двумерный цифровой усредняющий фильтр

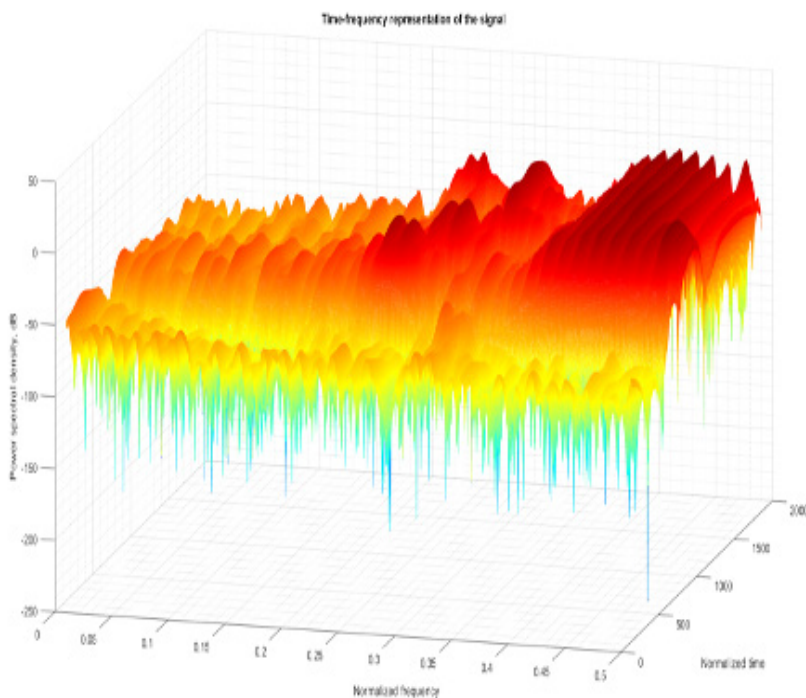


Рис. 2. ЧВП аудио сигнала, изображенного на рис. 1

подвергается разбиению на заданное число временных сегментов (оконный метод – реализуется с использованием временного окна Хемминга). последовательно к сформированным временным сегментам анализируемого сигнала применяется процедура быстрого преобразования Фурье (БПФ) [7–9, 11, 16–18].

На рис. 3 изображен вид сверху ЧВП аудио сигнала, изображенного на рис. 2.

На рис. 2 и 3 можно наблюдать, что ЧВП ау-

прямоугольного типа с конечной импульсной характеристикой (КИХ). Область определения конечной импульсной характеристики данного двумерного цифрового фильтра имеет вид прямоугольника.

При условии, что матрица A (конечная импульсная характеристика, ядро свертки) имеет размерность (M_a, N_a) , и матрица B (входное ЧВП) имеет размерность (M_b, N_b) , результат C преобразования ЧВП в двумер-

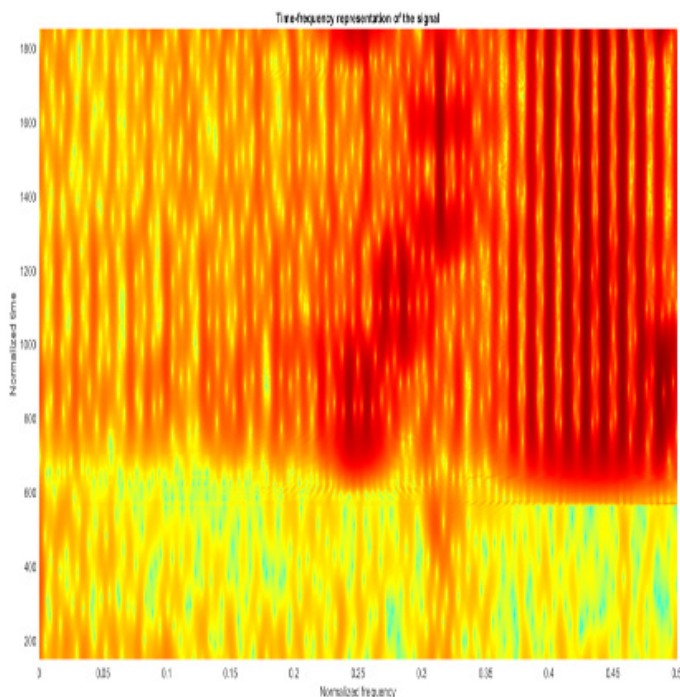


Рис. 3. Вид сверху ЧВП аудио сигнала, изображенного на рис. 2

ном цифровом фильтре описывается в виде двумерной цифровой свертки (формула 1):

$$C(i, j) = \sum_{m=0}^{(Ma-1)} \sum_{n=0}^{(Na-1)} A(m, n) * B(i - m, j - n), \quad (1)$$

где $0 \leq i < Ma + Mb - 1$ и $0 \leq j < Na + Nb - 1$,

$A(m, n)$ – ядро свертки,

$B(i - m, j - n)$ – соответственные входные точки ЧВП сигнала,

Размер ядра фильтра, то есть размер области определения импульсной характеристики (ИХ) двумерного цифрового фильтра, является одним из основных параметров данного фильтра. Используемый цифровой фильтр является цифровым фильтром нижних частот (ФНЧ).

В соответствии с выражением (1) на выходе двумерного цифрового ФНЧ получим результат свертки двумерного входного распределения ЧВП и двумерной ИХ фильтра в виде поверхности, отображенной на рис. 4.

На рис. 5 изображен результат совмещения ЧВП (рис. 2), и поверхности (синий цвет) (результата фильтрации ЧВП), отображенного на рис. 4.

На рис. 6 изображена только часть ЧВП, превышающая по уровню поверхность, отображенную на рис. 4 и показанную на рис. 5, то есть на рис. 6 отображена наиболее информативная часть ЧВП (рис. 2).

На рис. 7 изображен вид сверху для рис. 6.

На рис. 7 отображен конечный результат двумерной фильтрации – выделение наиболее информативной части ЧВП (рис. 2) сигнала.

Меняя значение параметров цифрового фильтра (изменяя параметры ядра фильтра), можно подобрать такие их значения, при которых будет удалено достаточное количество неинформативной (малозначимой) части данных ЧВП исследуемого технического сигнала, с сохранением существенной информативной части ЧВП.

Следующий этап обработки определяет выделение структурных параметров ЧВП (рис. 7), то есть формирование скелетона информативной части ЧВП исследуемого сигнала.

4. Построение скелетона (утончение линий) изображения информативной части ЧВП сигнала

Для наилучшего выделения информативных структурных признаков наблюдаемого сигнала (рис. 1) к полученной наиболее информативной части ЧВП (рис. 7) применяется операция скелетонизации (утончение линий). Функция, реализующая формирование скелетона в среде программирования MATLAB, задается операцией: $E = \text{bwmorph}(BW, 'skel', \text{Inf})$, где BW – входная двумерная цифровая матрица, E – двумерная цифровая бинарная матрица.

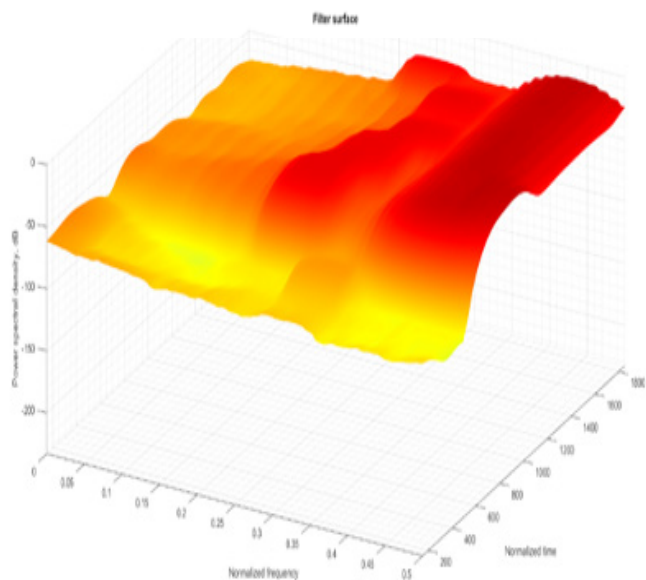


Рис. 4. Результат свертки двумерного входного распределения ЧВП (рис.3) и двумерной ИХ цифрового ФНЧ, отображаемый виде поверхности

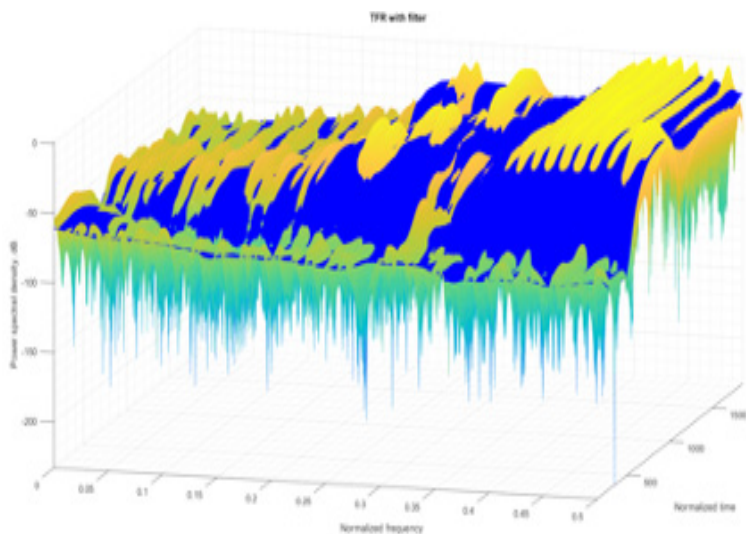


Рис. 5. ЧВП сигнала (рис. 2) с наложенным результатом двумерной цифровой фильтрации (рис. 4) ЧВП сигнала

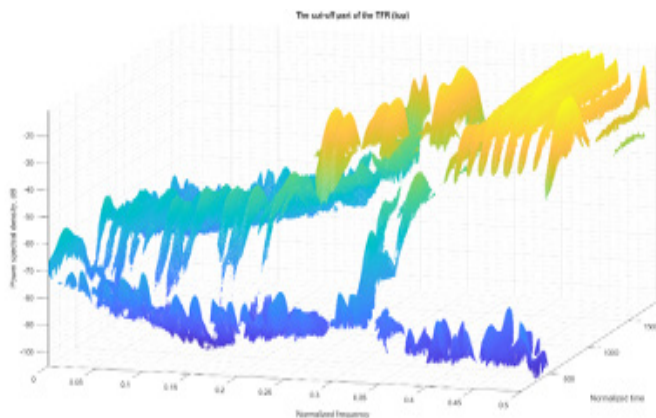


Рис. 6. Часть ЧВП (рис. 2), превышающая по уровню поверхность, отображенную на рис. 4

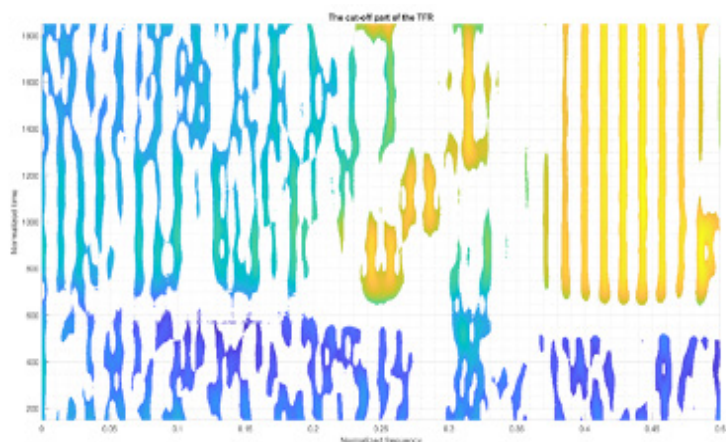


Рис. 7. Вид сверху для части ЧВП (рис. 2), превышающей по уровню поверхность, отображенную на рис. 4

Построение скелетона основано на уточнении областей изображения в результате анализа окрестности каждой информативной точки изображения.

Скелетон (рис. 8) информативной части ЧВП (рис. 7) в точности повторяет максимальные уровни информативной части ЧВП, располагаясь посередине выделенных линий.

На рис. 8 по оси абсцисс отображена нормированная частота, по оси ординат – нормированное время.

Скелетон изображения, представленный на рис. 8, построен с использованием алгоритма Зонга-Суня [19].

5. Подготовка высокоинформативного цифрового изображения наблюдаемого сигнала с использованием процедуры сжатия

Для еще большего (дополнительного) сжатия массива данных, отображающих скелетон информативной части ЧВП (рис. 8) наблюдаемого сигнала, применяется функция изменения размера изображений. Функция изменения размера изображений позволяет минимизировать объем данных, занимаемый «пустыми» областями на изображении.

Изменение размера происходит с использованием алгоритма бикубической ин-

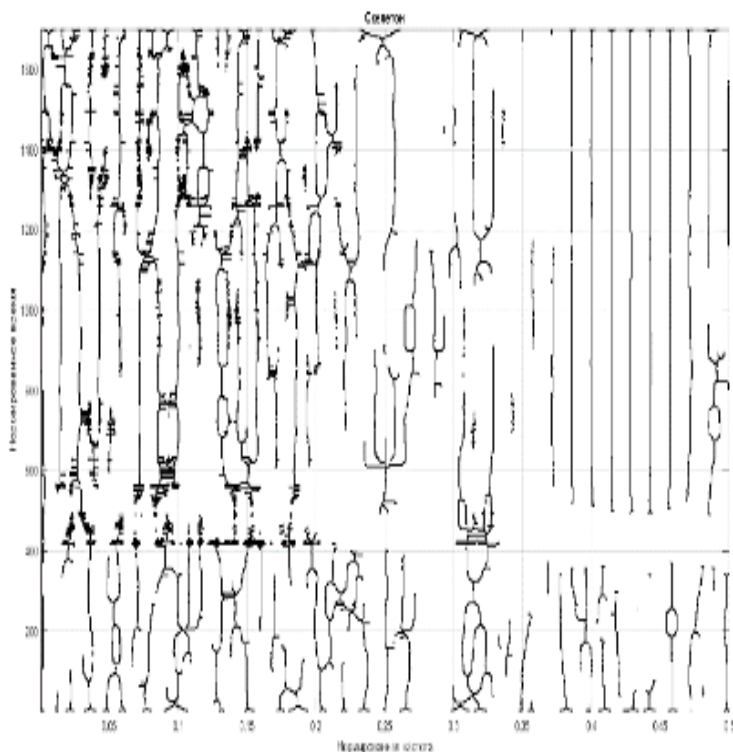


Рис. 8. Скелетон информативной части ЧВП сигнала (рис. 7)

терполяции [20]. При этом значение выходного пикселя представляет собой усредненное значение пикселей в ближайшей окрестности 4×4 . Значение функции в искомой точке вычисляется через ее значения в 16 соседних точках, расположенных в вершинах квадратов плоскости x, y .

Размер выходных данных может быть любым. В рассматриваемом примере выбран размер изображения: 227×227 точек (рис. 9). При этом, размер исходного изображения равен 1701×1049 точек (рис. 8).

При отображении сжатого изображения на рис. 9–11, по оси абсцисс откладывается нормированная частота, по оси ординат – нормированное время.

На рис. 9 отображен конечный результат преобразования, предложенным в работе модульным алгоритмом наблюдаемого аудио сигнала (рис. 1), то есть отображено сжатое изображение скелетона изображения ЧВП сигнала размером 227×227 точек, при этом размер области определения ИХ двумерного ЦФ равен $(50, 50)$.

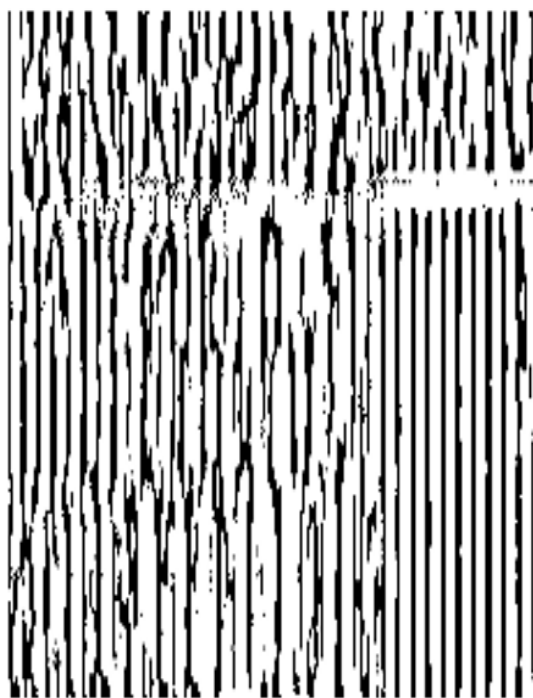


Рис. 9. Сжатое изображение скелетона ЧВП размером 227×227 точек (Sizeofthefilter 50)

Таким образом, результат работы рассматриваемого в работе модульного алгоритма – это, преобразование исходного сигнала (рис. 1) в информативное сжатое изображение, представленное на рис. 9. Используемый в рассматриваемом модульном алгоритме дву-

мерный ЦФ позволяет управлять степенью детализации выходного сжатого изображения (рис. 9).

На рис. 9 приведено конечное (результатирующее) сжатое изображение аудио сигнала (рис. 1) с использованием цифрового двумерного ФНЧ с размером области определения ИХ ЦФ равном $(50, 50)$.



Рис. 10. Сжатое изображение скелетона ЧВП размером 227×227 точек (Sizeofthefilter 150)



Рис. 11. Сжатое изображение скелета ЧВП размером 227×227 точек (Sizeofthefilter 270)

По результатам анализа изображений, представленных на рис. 9–11, видно, что изменение области определения ИХ двумерного ЦФ позволяет эффективно управлять степенью детализации выходного сжатого изображения. В данном случае последовательное увеличение области определения ИХ ЦФ (рис. 9–11 соответственно) приводит к постепенному снижению степени детализации отображения выходного сжатого изображения, наблюдаемого исходного технического сигнала.

В рассмотренном в работе модульном алгоритме преобразования входного наблюдаемого технического сигнала в выходное сжатое изображение, каждый модуль имеет свои параметры настройки, что позволяет приме-

нять модульный алгоритм для обработки широкого класса технических сигналов различного уровня сложности и для подготовки входных данных для решения разнообразных технологических задач, возникающих в АСУ промышленных систем.

6. Заключение

В работе рассматривается модульный алгоритм предварительной обработки (подготовки) наблюдаемых технических сигналов АСУ, реализующий преобразование исследуемого технического сигнала в высокоинформативное изображение на основе использования технологий цифровой обработки сигналов. Сформированное с использованием модульного алгоритма высокоинформативное изображение является подготовленными входными данными для последующей обработки в АСУ, например, с использованием технологии глубокого машинного обучения и искусственных нейронных сетей.

Разработанный и предложенный в работе модульный алгоритм предварительной подготовки данных, является универсальным и применимым для решения широкого круга задач решаемых в АСУ цифровых промышленных систем: при распознавании и обработки речи в системах человеко-машинного интерфейса, диагностики состояния технического оборудования в составе системы АСУ, идентификации человека по его биометрическим данным в биометрических системах контроля доступа, выявлении вредоносных информационных воздействий и обнаруже-

нии аномалий в наблюдаемых сигналах АСУ, что приводит соответственно, к снижению рисков в информационных системах АСУ [21].

Основные предлагаемые в проведенном исследовании этапы подготовки данных, реализуются с использованием технологии цифровой обработки сигналов: частотно-временного спектрального анализа сигналов, применение двумерной цифровой фильтрации с использованием двумерного КИХ-фильтра, получение скелетона двумерного сигнала с выхода двумерного КИХ-фильтра, конечное сжатие выходных данных.

Показано, что применение двумерной цифровой фильтрации позволяет выделить наиболее информативную составляющую изображения ЧВП сложного нестационарного анализируемого технического сигнала.

Совместное применение частотно-временного спектрального анализа и двумерной цифровой фильтрации позволяет сформировать информативные данные для решения широкого круга задач по дальнейшей обработке сложных нестационарных технических сигналов, наблюдаемых в АСУ промышленных систем.

Путем подбора параметров отдельных модулей, предлагаемый и рассмотренный в работе алгоритм возможно адаптировать для предварительной обработки (то есть, предварительной подготовки данных в виде высокоинформативного цифрового изображения) широкого класса технических сигналов АСУ, обладающих различным уровнем сложности.

Литература

1. Домингос, П. Верховный алгоритм: как машинное обучение изменит наш мир: учеб. пособие / П. Домингос. – М.: Гостехиздат, 2015. – 989 с.
2. Коллакот Р. А. Диагностирование механического оборудования. Пер. с англ. Л.: Судостроение, 1980. – 296 с.
3. Алексеев А.А. Идентификация и диагностика систем / А.А. Алексеев, Ю.А. Кораблев, М.Ю. Шестопалов. М.: Издательский центр «Академия», 2009. – 352 с.
4. Артоболевский И.И., Бобровницкий Ю.И., Генкин М.Д. Введение в акустическую динамику машин. М.: Наука, 1979. – 296 с.
5. Горелик А.Л. Методы технической диагностики машин и механизмов / А.Л. Горелик, Ф.Я. Балицкий, А.Н. Требунский.- М.: НТЦ «Информатика», 1990. – 204 с.
6. Ширман А. Р., Соловьев А. Б. Практическая вибродиагностика и мониторинг состояния механического оборудования. Энергомашиностроение, 1996. – 276 с.
7. Марпл-мл. С.Л. Цифровой спектральный анализ и его приложения. М.: Мир, – 1990. – 584 с.
8. Шахтарин Б. В., Ковригин В. А. Методы спектрального оценивания случайных сигналов: учебное пособие. – М.: Гелиос АРВ, 2005. – 248 с.
9. Бендат Дж., Пирсол А. Измерение и анализ случайных процессов. – М.: Мир, 1983. – 312 с.
10. Веселов, О. В. Методы искусственного интеллекта в диагностике: учеб. пособие / О. В. Веселов, П. С. Сабуров; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2015. – 251 с.

11. Крнев, А.Н. Цифровой спектральный анализ: учеб. пособие / А.Н. Крнев, Т.К. Артемова. – Ярославль: Изд-во Яросл. гос. ун-т, 2002. – 114 с.
12. A. Ragozin, V. Telezhkin, P. Podkorytov, «Prediction of Aggregate Multicomponent Time Series in Industrial Automated Systems Using Neural Network», Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2019, 13-15 March, 2019, Hong Kong. – P. 17-19.
13. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov, «Forecasting Complex Multi-component Time Series within Systems Designed to Detect Anomalies in Dataflows of Industrial Automated Systems», SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks, September 2019, Article No.: 2. – P. 1–5.
14. Ragozin, A.N., Telezhkin, V.F., Podkorytov, P.S. State Prediction in Compound Control Systems via Time Series: Neural Network Approach, 2019 Conference Proceedings - IEEE SOUTHEASTCON 2019, 11-14 April, 2019, Huntsville, AL, USA. – P. 1–6.
15. Ragozin A. N. ; Osipov D. V. ; Tarasov I. S. ; Pletenkova A. D., Investigation of the Influence of the Preliminary Digital Filtering Method on the Accuracy of Signal Prediction in Anomaly Detection Systems in Industrial Automatic Control Systems (IACS), 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBREIT) 2020, 14-15 May, 2020, Yekaterinburg, Russia. – P. 1–4.
16. Cooley, J. An Algorithm for the Machine Calculation Complex Fourier Series / J. Cooley, J. Tukey. – New Jersey: Pub. by Princeton University, 1965. – 5 p.
17. Меркушева, А.В. Формирование время-частотных представлений (динамического спектра) нестационарного сигнала на основе преобразования представлений известного типа / А.В. Меркушева // Научное приборостроение. – 2005. – Т. 15, №1. – С. 87–93.
18. Цифровая обработка сигналов: учеб. пособие / Ю.Н. Матвеев, К.К. Симончик, А.Ю. Тропченко, М.В. Хитров. – СПб.: СПбНИУ ИТМО, 2013. – 166 с.
19. MaJun, Tsiviatkou V. Yu., Konopelko V. K. A new improved fast parallel skeletonize algorithm // Кодирование и цифровая обработка сигналов в инфо-коммуникациях: материалы междунар. науч.-практ. конф. (Республика Беларусь, Минск, 4 апреля 2019 года) / редкол.: В. К. Конопелько, В. Ю. Цветков, Л. А. Шичко – Минск : БГУИР, 2019. – 136 с.
20. Половко, А.М. Интерполяция. Методы и компьютерные технологии их реализации / А.М. Половко, П.Н. Бутусов. – М.: БХВ-Петербург, 2016. – 320 с.
21. Баринев А.Е., Скурлаев С.В., Соколов А.Н. «Методика оценки рисков, вызванных уязвимостями в программном обеспечении автоматизированных систем управления технологическими процессами», Вестник УрФО. Безопасность в информационной сфере., No 3 (25), 2017. – С. 34–42.

References

1. Domingos, P. Verhovnyj algoritm: kak mashinnoe obucheniye izmenit nash mir: Ucheb. posobie / P. Domingos. – M.: Gostekhizdat, 2015. – 989 с.
2. Kollakot R. A. Diagnostirovaniye mekhanicheskogo oborudovaniya. Per. s angl. L.: Sudostroeniye, 1980. – 296 s.
3. Alekseev A. A. Identifikatsiya diagnosticheskoy sistemy / A. A. Alekseev, Yu. A. Korablev, M. Yu. Shestopalov. M.: Izdatel'skiy tsentr «Akademiya», 2009. – 352 s.
4. Artobolevskiy I. I., Bobrovnickiy Yu. I., Genkin M. D. Vvedeniye v akusticheskuyu dinamiku mashin. M.: Nauka, 1979. – 296 s.
5. Gorelik A. L. Metody tekhnicheskoy diagnostiki mashin i mekhanizmov / A. L. Gorelik, F. Ya. Balitskiy, A. N. Trebunskiy. – M.: NTC «Informatika», 1990. – 204 s.
6. Shirman A. R., Solov'ev A. B. Prakticheskaya vibrodiagnostika i monitoring sostoyaniy mekhanicheskogo oborudovaniya. Energomashinostroyeniye, 1996. – 276 s.
7. Marpl-m. S. L. Cifrovoye spektral'nyy analiz ego prilozheniya. M.: Mir, 1990. – 584 s.
8. Shahtarin B. V., Kovrigin V. A. Metody spektral'nogo ocenivaniya sluchaynykh signalov: Uchebnoye posobie. – M.: Gelios ARV, 2005. – 248 s.
9. Bendat Dzh., Pirsol A. Izmereniya analiz sluchaynykh processov. – M.: Mir, 1983. – 312 s.
10. Veselov, O. V. Metody iskusstvennogo intellekta v diagnostike: ucheb. posobie / O. V. Veselov, P. S. Saburov; Vladim. gos. un-t im. A. G. i N. G. Stoletovyh. – Vladimir: Izd-vo VIGU, 2015. – 251 s.
11. Krenev, A. N. Cifrovoye spektral'nyy analiz: Ucheb. posobie / A. N. Krenev, T. K. Artemova. – Yaroslavl': Izd-vo Yarosl. gos. un-t, 2002. – 114 s.
12. A. Ragozin, V. Telezhkin, P. Podkorytov, «Prediction of Aggregate Multicomponent Time Series in Industrial Automated Systems Using Neural Network», Lecture Notes in Engineering and Computer Science:

Proceedings of The International MultiConference of Engineers and Computer Scientists 2019, 13-15 March, 2019, Hong Kong. – P. 17–19.

13. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov, «Forecasting Complex Multi-component Time Series within Systems Designed to Detect Anomalies in Dataflows of Industrial Automated Systems», SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks, September 2019, Article No.: 2. – P. 1–5.

14. Ragozin, A.N., Telezhkin, V.F., Podkorytov, P.S. State Prediction in Compound Control Systems via Time Series: Neural Network Approach, 2019 Conference Proceedings - IEEE SOUTHEASTCON 2019, 11-14 April, 2019, Huntsville, AL, USA. – P. 1–6.

15. Ragozin A. N. ; Osipov D. V. ; Tarasov I. S. ; Pletenkova A. D., Investigation of the Influence of the Preliminary Digital Filtering Method on the Accuracy of Signal Prediction in Anomaly Detection Systems in Industrial Automatic Control Systems (IACS), 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBREIT) 2020, 14-15 May, 2020, Yekaterinburg, Russia. – P. 1–4.

16. Cooley, J. An Algorithm for the Machine Calculation Complex Fourier Series / J. Cooley, J. Tukey. – New Jersey: Pub. by Princeton University, 1965. – 5 p.

17. Merkusheva, A.V. Formirovaniyevremya-chastotnyhpredstavlenij (dinamicheskogospektra) nestacionarnygosignalanaosnovepreobrazovaniyapredstavlenijizvestnogotipa/A.V.Merkusheva//NauchnoepriBORostroenie. – 2005. – T. 15, №1. – S. 87–93.

18. Cifrovayaobrabotkasignalov: ucheb. posobie / Yu.N. Matveev, K.K. Simonchik, A.Yu. Tropchenko, M.V. Hitrov. – SPb.: SPbNIU ITMO, 2013. – 166 s.

19. Ma Jun, Tsviatkou.V.Yu., Konopelko V.K. A new improved fast parallel skeletonize algorithm // Kodirovaniyecifrovayaobrabotkasignalov v info-kommunikatsiyah: materialymezhdunar. nauch.-prakt. konf. (Respublika Belarus', Minsk, 4 aprelya 2019 goda) / redkol.: V. K. Konopel'ko, V. Yu. Cvetkov, L. A. Shichko – Minsk : BGUIR, 2019. – 136 s.

20. Polovko, A.M. Interpolyaciya. Metodyikomp'yuternyetekhnologiiirealizacii / A.M. Polovko, P.N. Butusov. - M.: BHV-Peterburg, 2016. – 320 s.

21. Barinov A. E., Skurlaev S. V., Sokolov A. N., "Methodology for assessing the risks caused by vulnerabilities in the software of automated process control systems", Bulletin of the Urals Federal District. Security in the information field, vol. 3(25), 2017. – P. 34–42.

РАГОЗИН Андрей Николаевич, кандидат технических наук, доцент кафедры защиты информации, доцент кафедры инфокоммуникационных технологий высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: ragozinan@susu.ru

ПОРТНОВ Андрей Владимирович, студент кафедры инфокоммуникационных технологий высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: andr.leo00@mail.ru

ЛЫСОВ Станислав Сергеевич, студент кафедры инфокоммуникационных технологий высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: stas_13_1999q@icloud.com

ПРЫТКОВ Никита Сергеевич, студент кафедры инфокоммуникационных технологий высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: yb31rb10nf99@gmail.com

RAGOZIN Andrey Nikolaevich, Candidate of Sciences in Technology, Department of Information Security, Department of Information Technology Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)» Russia, 454080, Chelyabinsk, prsp. Lenina, 76. E-mail: ragozinan@susu.ru

PORTNOV Andrey Vladimirovich, student of the Department of Information Technology Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)» Russia, 454080, Chelyabinsk, prsp. Lenina, 76. E-mail: andr.leo00@mail.ru

LYSOV Stanislav Sergeevich, student of the Department of Information Technology Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)» Russia, 454080, Chelyabinsk, prsp. Lenina, 76. E-mail: stas_13_1999q@icloud.com

PRYTKOV Nikita Sergeevich, student of the Department of Information Technology Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)» Russia, 454080, Chelyabinsk, prsp. Lenina, 76. E-mail: yb31rb10nf99@gmail.com

ИССЛЕДОВАНИЕ ПРОБЛЕМ ЗАЩИТЫ ОБЪЕКТОВ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ ОТ УГРОЗ ХИЩЕНИЯ ИНФОРМАЦИИ

В статье отмечается, что чем быстрее происходит цифровизация транспортной отрасли, а, следовательно, возникновении новых уязвимостей и рисков, тем острее стоит вопрос о разработке новых и усовершенствовании уже используемых средств по обеспечению информационной безопасности транспортной инфраструктуры, защите информации ограниченного доступа. Автор приводит примеры инцидентов информационной безопасности на транспорте в России и мире с 2018 года. Статистический анализ позволил прийти к выводу, что основным мотивом злоумышленников при совершении информационных атак является хищение информации, в наибольшей степени персональные данные, в том числе из облачных хранилищ. Социальная инженерия и кибератаки с использованием вредоносного программного обеспечения, вероятнее всего, останутся самыми популярными и успешными методами проникновения в корпоративные информационные системы.

Ключевые слова: транспортная инфраструктура, информационная безопасность, защита информации, инцидент информационной безопасности, информационная атака, утечка конфиденциальной информации.

Gruzdeva L.M.

RESEARCH OF PROBLEMS OF PROTECTION OF TRANSPORT INFRASTRUCTURE OBJECTS FROM THREATS OF INFORMATION THEFT

The article notes that the faster the digitalization of the transport industry takes place, and, consequently, the emergence of new vulnerabilities and risks, the more acute is the question of developing new and improving the already used means to ensure information security of transport infrastructure, protect information of limited access. The author gives examples of infor-

information security incidents in transport in Russia and worldwide since 2018. Statistical analysis made it possible to conclude that the main motive of cybercriminals in carrying out information attacks is information theft, mostly personal data, including from cloud storage. Social engineering and cyber-attacks using malicious software are likely to remain the most popular and successful methods of infiltrating corporate information systems.

Keywords: transport infrastructure, information security, data protection, information security incident, information attack, leak of confidential information.

Внедрение технологических инноваций позволяет транспортному комплексу соответствовать запросам цифровой экономики. Развитие электротранспорта и высокоскоростного железнодорожного движения [1, 2], использование автономного транспорта (AVRI) на основе роботизированных технологий призвано повысить экономические показатели, уменьшить экологический вред [3], а также улучшить качество жизни человека. Специалисты признают, что беспилотные технологии [4] могут принести человечеству огромную пользу, привести к значительному сокращению числа жертв автомобильных аварий, которые ежегодно забирают жизни 1,3 млн. человек, а также повысить доступность такого транспорта для людей с ограниченными возможностями.

Но стоит отметить, что с появлением новых технологий появляются и новые риски в области безопасности. В частности, компания Tesla имеет не только широкий модельный ряд автомобилей, но, и не менее обширный перечень аварий, приведших даже к гибели водителей, использовавших функцию автопилота. GPS-навигатор также неоднократно

становился причиной дорожно-транспортных происшествий из-за помех в сигнале, получаемом от спутников по сети.

Транспортные информационные системы и сети, инфраструктура организаций построены по тем же принципам, что и в других отраслях. В связи с этим глобальные проблемы обеспечения информационной безопасности так же остро стоят перед компаниями транспортного комплекса [5, 6]. При этом транспортная инфраструктура, как правило, географически распределена, включает большое число объектов, что усложняет работу служб защиты информации.

Ежегодная доля информационных атак, совершаемых на объекты транспортной инфраструктуры, по данным компании Positive Technologies (PT) составляет 1%, но в III квартале 2019 г. было зафиксировано увеличение их числа до 3% [7]. В I квартале 2020 г. произошло увеличение доли атак, совершенных с использованием вредоносного программного обеспечения (ПО), способного обходить антивирусы, межсетевые экраны, IPS, почтовые и веб-шлюзы, в комбинации с методами социальной инженерией (рис. 1).

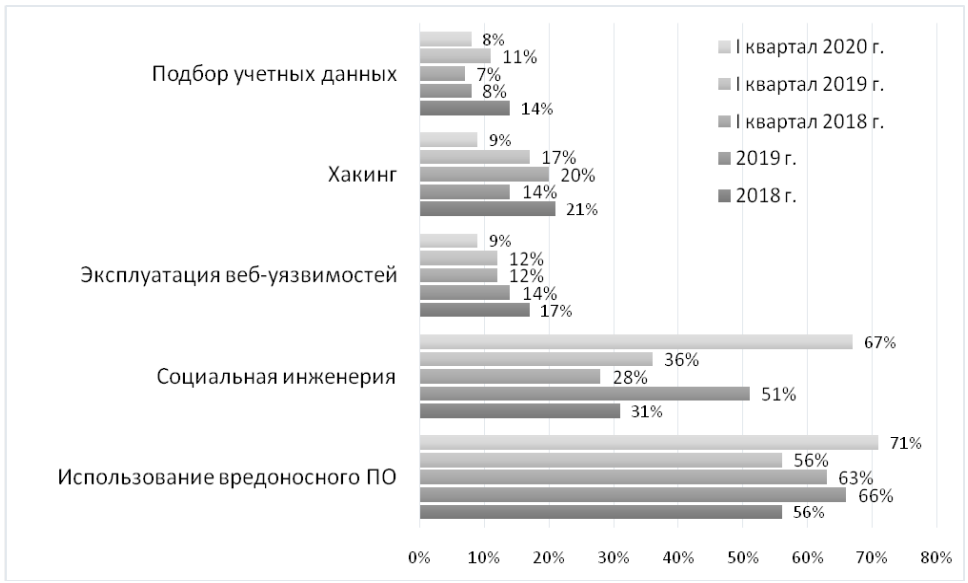


Рис. 1. Методы информационных атак (доля атак)

Так, например, на российские организации авиационно-космической отрасли была совершена АРТ-атака (advanced persistent threat - «развитая устойчивая угроза», целевая кибератака), в которой вредоносное ПО для удаленного управления (RAT) доставлялось путем рассылки писем с вредоносными документами в формате RTF [8].

Японский автопроизводитель Honda в июне 2020 г. заявил, что была совершена кибератака на сети промышленных систем управления, из-за которой возникли проблемы с доступом к внутренним серверам. Компания подтвердила, что работа на британском заводе была приостановлена наряду с приостановкой других операций в Северной Америке, Турции, Италии и Японии. Неизвестно, как злоумышленники проникли в компьютерную систему Honda, но исследования показывают, что все более распространенными становятся атаки с использованием информации о Covid-19, чтобы обманным путем заставить пользователей загружать на свои рабочие станции зараженные вредоносным ПО файлы.

В 2020 г. продолжился рост доли кибератак, совершаемых с целью хищения информации (рис. 2), при этом злоумышленников в 34% случаев интересовали персональные данные (ПДн), а в 19% - данные платежных карт.

меров кредитных карт клиентов, британский информационный регулятор (Commissioner's Office, ICO) заявил, что намерен оштрафовать компанию на рекордные 183 млн. фунтов стерлингов (230 млн. долларов).

В середине марта 2018 г. программист Владимир Серов раскрыл самую крупную уязвимость в сервисе бесплатного Wi-Fi московского метро. Минимум год уязвимость позволяла злоумышленникам получать номера телефонов всех подключенных пассажиров поезда, а затем прочитать в незашифрованном виде цифровой портрет каждого.

По данным экспертно-аналитического центра компании InfoWatch, число утечек конфиденциальной информации в транспортных и логистических компаниях в 2019 г. выросло на 67%. Скомпрометировано около 59 млн. записей персональных данных клиентов и сотрудников, что почти в 6 раз больше, чем в 2018 г. [9]. При этом по статистике за 2019 г. в России существенно чаще, чем в мире «утекали» телефонные номера и паспортные данные (более чем в 30% утечек).

Европейская аэрокосмическая корпорация Airbus 30 января 2019 г. сообщила об обнаружении инцидента информационной безопасности, который привел к несанкционированному доступу к данным в информаци-



Рис. 2. Мотивы злоумышленников

В 2018 г. злоумышленники похищали персональные данные в 30%, учетные данные в 24% и данные платежных карт в 14% случаев атак на информационные ресурсы. Например, из-за взлома системы бронирования British Airways в середине 2018 г., результатом которого стал доступ злоумышленников к тысячам но-

онных системах Airbus «Коммерческий авиационный бизнес». Нарушители получили доступ к личным данным, в основном, к профессиональным контактам и идентификационным данным некоторых сотрудников Airbus в Европе. Данный инцидент не повлиял на коммерческую деятельность корпорации.

Также в минувшем году крупную утечку персональных данных пассажиров пережила и китайская компания China Railway: из официальной системы бронирования могли быть похищены учетные записи до 5 млн. человек.

В России, как и в мире первое место по числу утечек ПДн занимает Интернет (браузер, cloud), на сеть приходится более 60% утечек. Бумажный документооборот в России продолжает функционировать наряду с электронным, поэтому злоумышленники в 22,7% случаев именно «бумагу» используют для хищения информации. Третье место в России занимают сервисы мгновенных сообщений (12,2%) [10].

С практической точки зрения для решения вопросов обеспечения информационной безопасности важно знать на сколько защищаемая информация подвержена деструктивному воздействию, т.е. «привлекательна» для злоумышленников. В России за 2018 г. было зафиксировано, что 60% утечек информации промышленных и транспортных компаний носило умышленный характер (рис. 3). В прошедшем году картина резко изменилась: было выявлено, что «привлекательность» для злоумышленников информации компаний данной отрасли являлась наименьшей, а доля умышленных утечек уменьшилась в 3 раза.

ции о путешествиях 9 млн. клиентов бюджетной британской авиакомпании EasyJet, но надо заметить, что при этом паспортные данные не были украдены. Интернет-издание Tom's Guide в июле 2020 г. сообщило об утечке персональных данных почти полумиллиона британских покупателей автомобилей BMW. Личные данные могут позволить злоумышленникам правдоподобно маскироваться под представителей автокомпании при реализации фишинговых атак на ее клиентов.

Из-за непрерывного роста спроса и предложений на рынке сервисов публичных облаков InfoWatch проявила интерес к проблеме обеспечения информационной безопасности от угроз хищения информации из баз данных. Согласно отчету Gartner, в 2019 г. объем данного рынка составил \$227,8 млрд. (около 86 млрд. руб. приходится на Россию), а 2020 г. он может вырасти на +17%.

Эксперты зарегистрировали за 2019 г. в 3,5 раза больше, чем в 2018 г. случаев утечек конфиденциальной информации с хранилищ на незащищенных (свободно доступных из-за неверной конфигурации) серверах в облачных сервисах. При этом более половины всех выявленных случаев утечек конфиденциальной информации пришлось на две страны – США (27,5%) и Россию (26,7%). На первом ме-

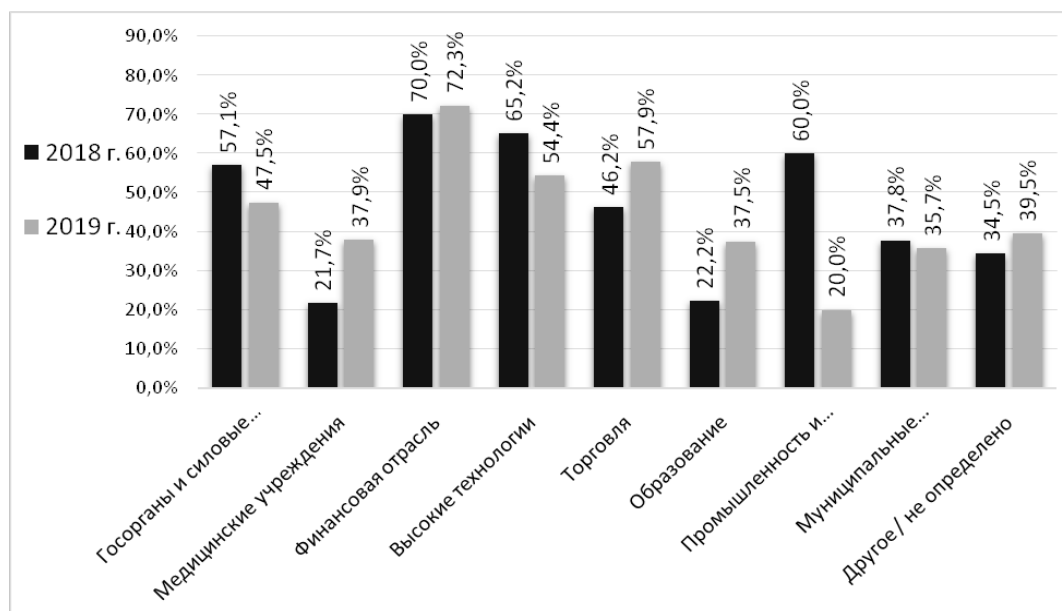


Рис. 3. Доля умышленных утечек ПДн и платежной информации по отраслям, Россия

В 2020 г. уже неоднократно фиксировались утечки ПДн из транспортных информационных систем. Например, в мае 2020 г. злоумышленники получили доступ к информа-

сте в мире и России по числу утечек находятся сервисы, на которых размещены данные высокотехнологичных компаний, например, телеком и электроника (рис. 4). При этом в

2019 г. в мире на +3,3% выросла доля утечек информации с промышленных и транспортных объектов, в России же зафиксировано число данных утечек на уровне 2018 г. - 7,2%.

Rivian Automotive Inc. в верховный суд штата Калифорнии, округ Санта-Клара (Сан-Хосе) о краже коммерческой тайны инсайдерами, которые перешли на работу к новому работода-

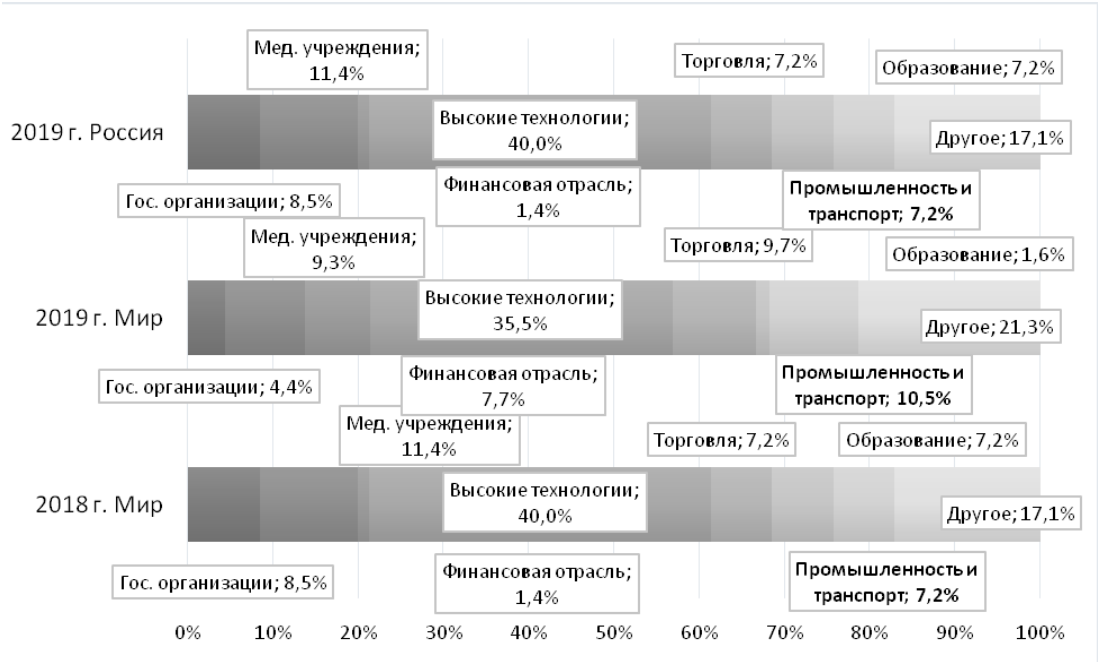


Рис. 4. Отраслевое распределение числа утечек из незащищенных хранилищ в облачных сервисах (Мир, 2018-2019 гг., Россия, 2019 г.)

В настоящее время на рынке облачных сервисов сохраняются многие проблемы в области информационной безопасности и защиты данных. Например, компьютерный справочный сайт Bleeping Computer сообщил, что на форумах распространяются базы (35 млн. записей персональных данных) участников программы лояльности и сведения из системы бронирования индонезийской авиакомпании Lion Air, при этом данные были скопированы с открытого облачного хранилища Amazon.

По мнению экспертов, International Data Corporation (IDC) к 2025 г. в облачных хранилищах будет обрабатываться почти половина всех мировых данных, в том числе и транспортной отрасли, в связи, с чем роль кибербезопасности будет только возрастать.

Около 10% утечек из транспортных и логистических компаний относятся к случаям компрометации информации категории «коммерческая тайна». Например, компания United Airlines была вынуждена принести извинения за утечку через Twitter внутренней информации, касающейся корпоративных расходов на авиабилеты среди крупнейших аккаунтов [9].

23 июля 2020 г. агентство Bloomberg сообщило об иске компании Tesla Inc. против

телю, что привело к внедрению интеллектуальной собственности Tesla в системы Rivian. Ранее Tesla уже подала в суд на бывших сотрудников за то, что они по сведениям компании передали ее коммерческие секреты китайскому производителю электромобилей Xpeng Motors и калифорнийскому разработчику беспилотного такси Zoox.

Издание The Register 10 апреля 2020 г. сообщило, что с помощью вируса-вымогателя DoppelPaymer для Windows был успешно атакован промышленный подрядчик Visser Precision. Конфиденциальные документы клиентов данной компании, в частности Tesla, Lockheed Martin, Boeing и SpaceX, были размещены злоумышленниками в открытом доступе в сети Интернет, так как Visser Precision не смогла выплатить выкуп за дешифратор зараженных файлов к сроку, установленному в марте.

Список инцидентов информационной безопасности на объектах транспортной инфраструктуры является далеко не полным, так как по мнению экспертов многие происшествия остаются не известны общественности. Компании стараются сохранить свою репутацию, стараются не подорвать доверие клиентов, поэтому не придают огласке случаи хищения инфор-

мации. Но каждая транспортная компания должна быть готова реагировать на информационные атаки и восстанавливаться путем создания киберустойчивости. Злоумышленники будут искать новые пути распространения вредоносного ПО и совершенствовать старые. Социальная инженерия, вероятно, останется основным путем распространения, однако в связи с ростом осведомленности о различных способах мошенничества преступники начнут разрабатывать более хитроумные схемы обмана пользователей. Стратегии защиты транспортных информационных систем должны быть сформулированы с учетом одного ключевого принципа: ни одна защита не является непреступной. Positive Technologies рекомендует заботиться не только об информационных ресурсах самих компаний, но и о безопасности их клиентов [7].

Анализ инцидентов информационной без-

опасности является одним из направлений оценки безопасности транспортных систем, которые в свою очередь являются объектами критической информационной инфраструктуры Российской Федерации [11]. Результаты проведенного исследования позволяют сделать вывод, что объекты транспортной инфраструктуры уязвимы и следует ожидать продолжение роста числа кибератак, совершаемых с целью хищения информации. В связи со сложностью и актуальностью задачи обеспечения информационной безопасности критической информационной инфраструктуры с 1 января 2018 г. на Федеральную службу безопасности Российской Федерации возложены функции по обеспечению функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ [12].

Литература

1. Розенберг Е. Н., Уманский В. И., Дзюба Ю. В. Цифровая экономика и цифровая железная дорога // Транспорт Российской Федерации. 2017. № 5 (72). – С. 45 – 49.
2. Уманский В. И., Павловский А. А., Дзюба Ю. В. Цифровая Железная Дорога. Технологический уровень // Перспективы Науки и Образования. 2018. № 1 (31). – С. 208 – 213.
3. Духно Н. А. Экологическая безопасность и транспорт // Транспортное право и безопасность. 2019. № 2(30). – С. 63 – 76.
4. Бойков В. Н., Скворцов А. В., Сарычев Д. С. Цифровая автомобильная дорога как отраслевой сегмент цифровой экономики // Транспорт Российской Федерации. 2018. № 2 (75) 2018. – С. 56 – 60.
5. Зворыкина Ю.В., Глуценко В.В. Обеспечение информационной безопасности на транспорте // Транспорт Российской Федерации. 2016. № 1 (62). – С. 6 – 9.
6. Груздева Л. М. Инциденты информационной безопасности на транспорте: виды, причины и негативные последствия // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. 2019. №6-2. – С. 57 – 60.
7. Актуальные киберугрозы. III квартал 2019 года [Электронный ресурс] ptsecurity.com. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q3/> (дата обращения 24.07.2020).
8. Актуальные киберугрозы. I квартал 2020 года [Электронный ресурс] ptsecurity.com. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/> (дата обращения 24.07.2020).
9. Транспорт: число утечек записей выросло в шесть раз [Электронный ресурс] infowatch.ru. – URL: <https://www.infowatch.ru/analytics/digest/21801> (дата обращения 24.07.2020).
10. Исследование структуры утечек персональных данных: мир и Россия, 2019 год [Электронный ресурс] infowatch.ru. – URL: <https://www.infowatch.ru/analytics/reports/26240> (дата обращения 24.07.2020).
11. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
12. Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

References

1. Rozenberg E. N., Umanskiy V. I., Dzjuba Ju. V. Cifrovaja jekonomika i cifrovaja zheleznaia doroga // Transport Rossijskoj Federacii. 2017. № 5 (72). – S. 45 – 49.

2. Umanskij V. I., Pavlovskij A. A., Dzjuba Ju. V. Cifrovaja Zhelez-naja Doroga. Tehnologicheskij uroven' // Perspektivy Nauki i Obrazovaniya. 2018. № 1 (31). – S. 208 – 213.
3. Duhno N. A. Jekologicheskaja bezopasnost' i transport // Transportnoe pravo i bezopasnost'. 2019. № 2(30). – S. 63 – 76.
4. Bojkov V. N., Skvorcov A. V., Sarychev D. S. Cifrovaja avtomo-bil'naja doroga kak otraslevoj segment cifrovoj jekonomiki // Transport Rossijskoj Federacii. 2018. № 2 (75) 2018. – S. 56 – 60.
5. Zvorykina Ju.V., Glushhenko V.V. Obespechenie informacionnoj bezopasnosti na transporte // Transport Rossijskoj Federacii. 2016. № 1 (62). – S. 6 – 9.
6. Gruzdeva L. M. Incidenty informacionnoj bezopasnosti na transporte: vidy, prichiny i negativnye posledstvija // Sovremennaja nauka: aktual'nye problemy teorii i praktiki. Serija: Estestvennye i Tehnicheskie Nauki. 2019. №6-2. – S. 57 – 60.
7. Aktual'nye kiberugrozy. III kvartal 2019 goda [Jelektronnyj resurs] ptsecurity.com. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q3/> (data obrashhenija 24.07.2020).
8. Aktual'nye kiberugrozy. I kvartal 2020 goda [Jelektronnyj resurs] ptsecurity.com. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/> (data obrashhenija 24.07.2020).
9. Transport: chislo utekshih zapisej vyroslo v shest' raz [Jelektronnyj resurs] infowatch.ru. – URL: <https://www.infowatch.ru/analytics/digest/21801> (data obrashhenija 24.07.2020).
10. Issledovanie struktury utechek personal'nyh dannyh: mir i Rossija, 2019 god [Jelektronnyj resurs] infowatch.ru. – URL: <https://www.infowatch.ru/analytics/reports/26240> (data obrashhenija 24.07.2020).
11. Federal'nyj zakon ot 26.07.2017 № 187-FZ «O bezopasnosti kriticheskoy informacionnoj infrastruktury Rossijskoj Federacii».
12. Ukaz Prezidenta RF ot 22.12.2017 № 620 «O sovershenstvovanii gosdarstvennoj sistemy obnaruzhenija, preduprezhdenija i likvidacii posledstvij komp'yuternyh atak na informacionnye resursy Rossijskoj Federacii».

ГРУЗДЕВА Людмила Михайловна, кандидат технических наук, доцент кафедры «Информационные технологии в юридической деятельности и документационное обеспечение управления», профессор Российской Академии Естествознания (РАЕ), Российский университет транспорта (МИИТ). 127994, г. Москва, ул. Образцова, д. 9, стр. 4. E-mail: docentglm@gmail.com

GRUZDEVA Liudmila Mikhailovna, Candidate of technical sciences, Associate professor of the department «Information Technologies in Legal Activity and Documentation Support of Management», Professor of the Russian Academy of natural Sciences (ANS), Russian University of Transport. 127994, Moscow, Obrastsova str., 9, bld. 9. E-mail: docentglm@gmail.com

***Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru
в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».***

***Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76,
ЮУрГУ, Издательский центр.***

**ВЕСТНИК УрФО
Безопасность в информационной сфере № 3(37) / 2020**

Подписано в печать 25.11.2020.

Дата выхода в свет 30.11.2020. Формат 70×108 1/16. Печать цифровая.

Усл.-печ. л. 7,7. Тираж 100 экз. Заказ 300/357.

Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

**Bulletin of the Ural Federal District
Security in the Sphere of Information No. 3(37) / 2020**

Signed to print November 25, 2020.

Date of publication of the 30.11.2020. Format 70×108 1/16. Screen printing.

Conventional printed sheet 7,7. Circulation – 100 issues. Order 300/357. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080